University of
Nottingham
UK | CHINA | MALAYSIA

Leveraging Web and Behavioural Data for Usable Adaptive Cybersecurity

A thesis submitted in fulfilment of the requirements
for the degree of Doctor of Philosophy

by

Joyce Hoese Addae

Advisors: *Xu Sun, Dave Towey and Milena Radenkovic*

in the

Faculty of Science and Engineering
School of Computer Science
International Doctoral Innovation Centre

May 2019

Declaration of Authorship

I, Joyce Hoese Addae , declare that this thesis titled, ”Leveraging Web and Behavioural Data for Usable Adaptive Cybersecurity” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: ____

Date: ____

Acknowledgements

First and foremost, all praise to the almighty God who shielded me and my family throughout this academic journey.

I would like to thank the International Doctoral Innovation Centre (IDIC), Ningbo Education Bureau, Ningbo Science and Technology Bureau, China's MoST and the Horizon Centre for Doctoral Training (CDT) here at Nottingham University, for all the financial and academic support to conduct the research presented in this thesis.

My sincere gratitude goes to my PhD advisors, Xu Sun, Dave Towey, and Milena Radenkovic, who have been an amazing team that offered professional support during my time at Nottingham University. I am most grateful to Dr Xu Sun for her unflinching support and her invaluable feedback and guidance throughout this project. Her interest in my ideas gave me the confidence to pursue them and her mentorship helped me grow as a researcher.

I would like to acknowledge my student collaborators Nan Li, Yi Ding, and Wenpeng Cheng in the School of Computer Science. They were very much involved in creating the initial implementation of SecAdapt by helping explore the source code for Google and Firefox for possible adaptation. They also contributed to the initial design concepts for the prototype.

I would also like to acknowledge my brother Victor Addae not just for his prayers and support, but his input in the design and development of the prototype produced in this thesis as well. He designed the initial interface for SecAdapt. Also, he was mostly that shoulder I leaned on when things got tough.

My heartfelt gratitude goes to my husband, Noble Kekeli Amegashie, for believing in me. His support and companionship have helped me stay true to my goal. My love goes to my two children Cassie and Caleb, who had to cope without me during this period.

Finally, my special thanks to all my family and friends for their care, prayers, and encouragement. I especially thank Joy, Jumoke, Michael and Elsie for their editorial and supportive efforts. I also appreciate all the stimulating discussions, the sleepless nights spent working hard before deadlines, and the precious moments shared with all my CDT/IDIC colleagues and office mates. Thanks to Felix, Francis, Aunty Bertha, Vicentia, Grace, Nana Kufuor and Antoinette for always listening to my frustrations and cheering me on. I could not have done it without all of you.

Abstract

Leveraging Web and Behavioural Data for Usable Adaptive Cybersecurity

There has been a general consensus in the computer security research community that the usability of cybersecurity is critical to maintaining and improving the security of information systems. However, the human element of cybersecurity is still not well understood hence the problem of designing security with unfriendly user interfaces persists. A major challenge in addressing the human component of cybersecurity is the lack of reliable behavioural data on users' online security actions. This thesis establishes an integrated view of online security-related attitudes and behaviours to facilitate the personalisation of cybersecurity tools. To do this, a design research approach involving behavioural science and machine learning techniques is adopted for an in-depth analysis of users' online security behaviour and implication for design of cybersecurity mechanisms.

As part of understanding users' attitude towards cybersecurity, studies were conducted to explore how users interact with web browser security features for their personal privacy and digital security online. Current interfaces designed for security in web browsers are plagued with several usability issues. This thesis proposes an improvement to these interfaces. The solution introduced here includes a user-centred design of personalized cybersecurity-related interfaces with minimalistic and modern aesthetics design that incorporates the concept of adaptive automation.

The study identified critical cybersecurity attributes that are susceptible to individual characteristics which provided a basis for the development of effective countermeasures for different user profiles. These findings were synthesised into two cybersecurity artefacts — SecAdapt versions 1 and 2 as proofs of concept for the proposed framework for personalised adaptive cybersecurity. The results of a usability study conducted to evaluate the prototype showed that SecAdapt was more efficient and effective when performing tasks to achieve specific cybersecurity goals compared to existing browser security controls. Most of the participants also found SecAdapt to be more user-friendly and clearly supported the proposed design concept for personalised adaptive cybersecurity and the benefits that it provides. Insights from this research can be useful in minimising the gap between people and cybersecurity in order to promote more frequent and correct usage of security tools and reduce human errors and dissatisfaction.

Contents

List of Figures

List of Tables

Abbreviations

AA Adaptive Automation

ACB Actual Cybersecurity Practiced and/or Behavior

APD Attitude to Personal Data

AVE Average Variance Extracted

AWA Awareness

BEH Protective Behavior/ Interest

BHO Browser Helper Objects

BN Bayesian-Network

CA Certification Authority

CFA Confirmatory Factor Analysis

CIA Confidentiality, Integrity, and Availability

COB Cost-Benefit

CPT Conditional Probability Table

CR Composite Reliability

DDoS Distributed Denial of Service

DK Domain Knowledge

DoS Denial of Service

DSL Digital Subscriber Line

DSR Design Science Research

DSS Decision Support Systems

DV Dependent Variable

EFA Exploratory Factor Analysis

FF Firefox

GC Google Chrome

GOMS Goals, Operators, Method and Selection

HCI Human-Computer Interaction

HCUs Home Computer Users

HTML HyperText Markup Language

HTTP HyperText Transfer Protocol

IC Interface Characteristics

IDS Intrusion Detection Systems

IE Internet Explorer

IoT Internet of Things

IPC Internet Privacy Concerns

IS Information Systems

ISO International Standards Organization

IT Information Technology

IV Independent Variables

LMID Limited Memory Influence Diagram

LV Latent Variables

MANOVA Multivariate Analysis of Variance

NCSA National Cyber Security Alliance

NIST National Institute of Standards and Technology

OS Operating system

OTG Omnibus Test of Group Differences

PAC Personalized Adaptive Cybersecurity

PEOU Perceived Ease of Use

PII Personal Identifiable Information

PKC Public Key Cryptography

PKI Public Key Infrastructure

PLS-MGA Partial Least Squares Multi-group Analysis

PLS-SEM Partial Least Squares Structural Equation Modelling

PMT Protection Motivation Theory

PR Perceived Risk

PRI Privacy/ Confidentiality Concerns

PU Perceived Usefulness

RES Responsibility

SBCL Security Breach Concern Level

SE Self-efficacy

SEC Security

SEM Structural Equation Modelling

SUS System Usability Scale

SUT Situated Usability Testing

SV1 SecAdapt Version 1

SV2 SecAdapt Version 2

TAM Technology Acceptance Model

TPB Theory of Planned Behaviour

TRA Theory of Reasoned Action

UI User Interface

USA United States of America

VFP Value for Personalization

VIF Variance Inflation Factor

WBSC Web Browser Security Controls

To God be the glory…

CHAPTER 1

Introduction

Contents

> "Many of the nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet... A cyber attack could be debilitating to our highly interdependent Critical Infrastructure and Key Resources (CIKR) and ultimately to our economy and national security."
>
> (**Homeland Security Council, 2007**).

1.1 Motivation

Modern society and economies rely on technological infrastructures for communication, finance, energy distribution, and transportation. These infrastructures depend increasingly on networked information systems and the web. The internet provides a network infrastructure for millions of networked computers to connect and communicate across the globe. With the growing popularity of cloud computing, more and more applications are being developed as web-based and with web interfaces. The interconnection between the web and internet-enabled devices built the cyberspace where people are able to create and share information and services. Thus, cyberspace refers to the virtual computer world that allows participants to create, interact, share and assess web-based products and services from almost anywhere in the world. Accordingly, the cyber ecosystem encompasses the interaction between the cyber devices (computers, software, etc.) and the diverse range of participants including individuals, organizations, and processes for a variety of virtual products and services [7]. Attacks against these systems can threaten the economic viability of organizations as well as the physical well-being of people. Several factors including the environment and other conditions influencing the interactions among the different entities, processes, data and the technologies are part of the security chain within cyberspace. This exposes the cyber ecosystems to different kinds of risks and threats. The current trend of ubiquitous computing whereby digital devices are increasingly becoming more context-aware is creating several opportunities as well as new and unique security and privacy challenges for the user population [8].

Cybersecurity generally refers to the technologies and processes that are used to protect computer networks, applications and data from attacks, destruction or exploitation. Cybersecurity breaches lead to numerous problems including destruction of operating systems, disruption of access to information, loss or theft of data, and privacy depreciation. Many cybersecurity breaches have been reported, sometimes with potentially quite severe consequences [9]. Incidents of cyber attacks are becoming more consequential. Attackers are exploiting the various vulnerabilities inherent in the cyberspace to commit all sorts of crimes on-line including identity theft and espionage [10]. Due to the widespread interconnection of these cyber devices, attacks can be waged anonymously and from a safe distance. Considering these numerous vulnerabilities, the necessity of an effective cybersecurity infrastructure is self-evident. Despite advances in cybersecurity technological solutions, most users are still unable to effectively access them for the protection of their digital assets. Ultimately, security technologies are effective only when they are correctly used. Unfriendly security mechanisms can hinder users from adopting them as well as from patronising web-based services. The need for web-based security functions to be usable are heightened, as these features are generally exposed to a broader cross-section of the society.

Nurse et al. [11] acknowledged that design of cybersecurity systems and interfaces must take into account psychological and social factors. Thus to address the challenges of building usable security mechanisms for web-based applications, developers/designers need user models that clearly capture the dynamics of user characteristics and contexts. User models are the representation of users' characteristics and preferences used to provide adaptivity [12]. Various methods (such as GOMS and Grammar-based models) have been proposed for the classification of different and changing characteristics of users based on their level of expertise. GOMS stands for Goals, Operators, Method and Selection which is a family of models which assumes the goals of users are determined before the execution of a task. Grammar-based models simulate interactions in the form of grammatical rules and are useful for comparing different interaction techniques [13].

There is, however, a gap in the literature in terms of models involving not just users' level of expertise but other socio-cultural characteristics in order to provide an integrated view of security-related behaviours. The acceleration in the creation of data along with technological advancements such as data mining and information extraction presents new opportunities to enhance user models with rich knowledge of users' experiences within the cyberspace. The massive datasets being generated has led to new technologies being developed to advance the field of data science and its applications. However, analysis of these massive datasets from a human factors perspective has received less attention as compared to the technical mechanisms facilitating their efficient storage and processing [14, 15].

1.2 Problem statement

Despite the fact that most computer security failures are triggered by user errors, security-related interfaces still tend to be very unclear and unfriendly. Consequently, many problems remain whereby the average user still fails to understand security and privacy settings for their systems applications (e.g. internet security settings provided for web browsers, privacy configurations on social networks etc.). Galitz [16] defined the user interface as "the part of a computer and its software that people can see, hear, touch or talk to or otherwise understand or direct." According to Galitz [16], because the user interface is what is presented to most users as the system, it is the most significant aspect of any computer application. Understanding how to configure cybersecurity is quite challenging for the majority of computer users mainly due to the complexity of user interfaces designed for security.

In spite of advances in Human-Computer Interaction (HCI) techniques and its wide adoption in evaluating commercial systems/applications, its application to the design and evaluation of security systems is relatively new and limited [17]. Despite the attempt to incorporate usability guidelines into security applications, most computer users still find it difficult to configure and interact with even the most fundamental cybersecurity settings necessary to ensure the safety of their data and other computing resources. This drawback in the application of generic usability guidelines to security has mainly been attributed to the inherent properties of security that call for a distinct set of design principles and strategies.

Empowering end-users to take charge of their own security controls was one of the main research challenges identified by the Computing Research Association et al. [18]. It has, therefore, become very crucial to understand the behaviour of security end-users and their impact on the usefulness of technical security solutions. This research hypothesises that an augmented user-model of cybersecurity can be developed from the analysis of multiple sourced security behavioural data on end-users. The study focuses on understanding people's security behaviours and actions on the web and how that knowledge can be leveraged towards improving the usability of cybersecurity mechanisms.

1.3 Research Scope and Objectives

This thesis aimed to investigate how a behavioural and data science approach can be adopted together with machine learning techniques in profiling user characteristics for adaptive cybersecurity. The main goal is to develop an integrated view of on-line security-related attitudes and behaviours to better understand the human aspect of cybersecurity and facilitate the design and development of more usable interactions with web browser security controls. The study, therefore, seeks to achieve the following objectives:

OBJ1. Identify, obtain, and filter behaviour and web data sources/ contents that represents real-world internet user experiences with different types of web browsers.

OBJ2. Explore data analytics for the extraction and visualisation of key user characteristics and security-related behaviour profiles.

OBJ3. Leverage knowledge acquired from the data analytics to develop a machine-learning framework for personalised adaptive cybersecurity to support the encoding of user behaviour and preferences into the design and development of digital security tools.

OBJ4. Develop and evaluate the usability and acceptability of alternative design concepts for web browser security controls based on the user behaviour profiles and personalised adaptive cybersecurity framework.

Research Questions

The main research question asked in this thesis is: *How can cybersecurity mechanisms be designed to increase the rate at which they are adopted and properly used by non-expert users?* The formulation of the main research question was based on the aims as well as the extant literature. The core enquiry for the thesis then directed the formulation of the following three sub-questions representing different aspects of the main question.

RQ1. What are the factors impacting on the adoption and use of cybersecurity mechanisms?

RQ2. What are the constructs and dimensions describing people's security-related behaviours on-line?

RQ3. How can augmented user models be developed for an adaptive cybersecurity framework based on behavioural and web data analytics?

The conceptual model presented in Chapter 3 highlights the relationships between the research questions. To support the aims and questions of this thesis, the research touches the field of Cybersecurity, HCI, Human Factors and Behavioural Science, and contribute mainly to the first two. Cybersecurity is the field concerned with the tools and systems employed to monitor, mitigate, and prevent cyber attacks. This thesis contributes to the cybersecurity literature by exploring the design space for personalised adaptive cybersecurity for non-expert users.

HCI is a field focused on studying the interaction between humans (the users) and computers. While originally concerned with understanding how people interact with computers and to what extent they are or are not developed for successful human interaction, the field has steadily expanded to encompass more areas of information technology design. Human Factors, on the other hand, has been defined as:
"the basic understanding of cognitive, physical, behavioural, physiological, social, developmental, affective, and motivational aspects of human performance—to yield design principles; enhance training, selection, and communication; and ultimately improve human-system interfaces and sociotechnical systems that lead to safer and more effective outcomes" [19].
As HCI expands to incorporate multiple disciplines, including computer science, cognitive science and human factors engineering, an overlap is formed between the two fields with various different viewpoints on what they entail. However, this research work sits in their intersection eventually adopting a mixed-methods approach to make contributions in these areas.

Behavioural science focuses on performance improvement in systems with behaviour and systems analytical principles and techniques. The field is primarily driven by rigorously obtained empirical data towards understanding and prediction of behaviour. As ergonomic principles are being applied to more and more product designs across diverse industries, researchers have identified the benefit of an integrated approach between behavioural science and the area of human factors [20]. The reactions, preferences and behaviour of internet users play a critical role in designing usable and acceptable cybersecurity mechanisms. By appropriately evaluating user behaviour, this thesis provides critical insights to better understand the human component of cybersecurity and how best to instil the habit of cybersecurity awareness and adoption of available countermeasures for secure interaction among cyber citizens.

The Web ecosystem represents one of the largest sources of information in today's society and is emerging as a logical area of study. Industrial practitioners from various fields have been successfully generating and using web data to achieve specific objectives for some time now. Areas, where web data is being adopted to enhance decision-making, includes politics (e.g. targeting political advertisements at likely supporters based on web searches) and search engines (e.g. Google's personalisation of searches based on previous web data). Both qualitative and quantitative approaches are being established as a way of investigating how the web influences human behaviour and shapes how users interact with related technologies. Since this research is focusing on web browser security interfaces, both web and data science techniques are adopted to study users' interactions with these security functionalities. The research consists of a mixed approach of both qualitative and quantitative data collection methods. The qualitative aspect is mainly targeted at seeking insights from individuals about their experiences in dealing with security-related interfaces. A quantitative data analysis approach involving attitude scale development and distribution online was carried out to measure and compare these experiences towards the development of personalised and/or adaptive models.

1.4 Thesis Overview

Figure 1.1 presents the structure of this thesis based on chapter contributions to the research questions and objectives. The purpose of chapter one was to introduce the thesis by identifying the research problem, scope, objectives, and questions. The remaining thesis is organised into 7 chapters using the traditional format that begins with a literature review followed by the research design. Next, the main research activities and discussion of findings are organised into four main experimental chapters. Specific aspects of background literature are provided to support the studies described in each of the four experimental chapters. The thesis ends with a summary of the main contributions, limitations and future works in Chapter 8. The following are brief overview of each of the chapters in the thesis.

Chapter 2 — Background and Related Work: this chapter presents a review of the literature supporting the research. The chapter covers cybersecurity implementation mechanisms and related usability and acceptability problems. The chapter also discusses inherent web browser vulnerabilities used to breach cybersecurity and the importance of usable security research.

Chapter 3 — Methodology: this chapter discusses the multidisciplinary research approach adopted to answer the research questions and the proposed research model.

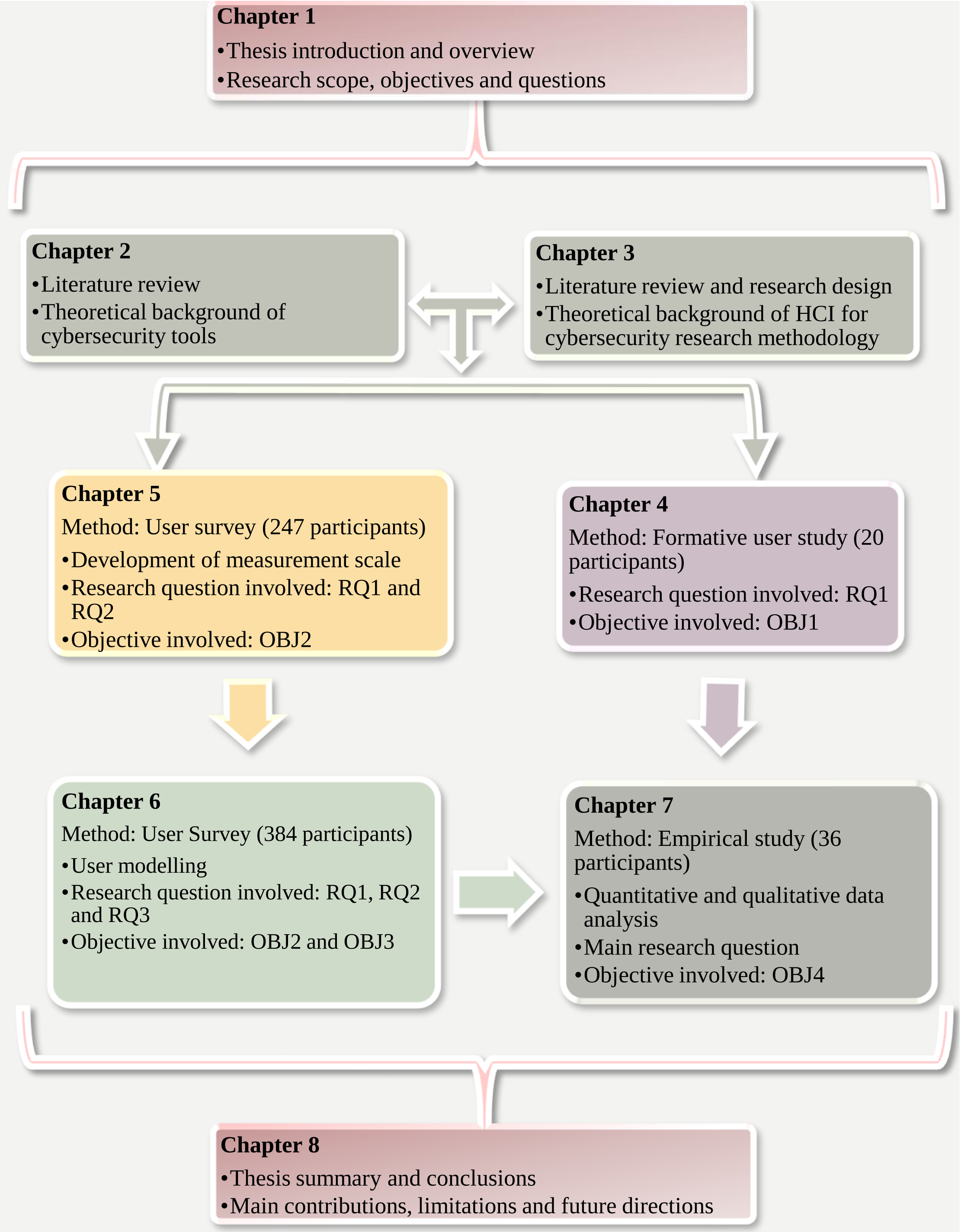

Chapter 1
•Thesis introduction and overview
•Research scope, objectives and questions
Chapter 2
•Literature review
•Theoretical background of cybersecurity tools
Chapter 3
•Literature review and research design
•Theoretical background of HCI for cybersecurity research methodology
Chapter 5
Method: User survey (247 participants)
•Development of measurement scale
•Research question involved: RQ1 and RQ2
•Objective involved: OBJ2
Chapter 4
Method: Formative user study (20 participants)
•Research question involved: RQ1
•Objective involved: OBJ1
Chapter 6
Method: User Survey (384 participants)
•User modelling
•Research question involved: RQ1, RQ2 and RQ3
•Objective involved: OBJ2 and OBJ3
Chapter 7
Method: Empirical study (36 participants)
•Quantitative and qualitative data analysis
•Main research question
•Objective involved: OBJ4
Chapter 8
•Thesis summary and conclusions
•Main contributions, limitations and future directions

FIGURE 1.1: A visual summary of research workflow and contributions

Chapter 4 — User Experience with Web Browser Security Settings: this chapter evaluates the user interface of web browser security controls and identifies usability problems.

Chapter 5 — Measuring Cybersecurity Behavioural Attitudes: this chapter presents results of the first part of user studies conducted towards the evaluation of the theoretical research model.

Chapter 6 — Modelling Behaviour for Adaptive Cybersecurity: this chapter presents the final part of the user study conducted to evaluate the proposed research model and explains how it would provide adaptivity to diverse user groups and personalization.

Chapter 7 — Prototype Development and Evaluation: this chapter covers adaptive cybersecurity design options and implementation in web browsers. It reviews the user-centred process followed to develop the prototype application (SecAdapt). The results of the evaluation of the data gathered from users who tested the proofs of concept designs implemented in SecAdapt versions 1 and 2 are also presented and discussed.

Chapter 8 — Conclusion: this final chapter concludes the research by giving an overview of how the research questions were addressed. It also summarizes the main achievements and discusses future research paths.

CHAPTER 2

Background and Literature Review

Contents

2.1 Introduction

Computer networks keep getting bigger, faster and ever evolving into a dynamic ubiquitous infrastructure for the digital economy. The internet underpins the interconnection of these networks further enhancing their capabilities in terms of communication and global access. Most governments and business corporations now rely on these computer networks to control their critical processes such as utility supplies, stock market monitoring, manufacturing etc. The web as an internet service offers online business owners a wider jurisdiction for commerce without the constraints of geographical boundaries. The result is a virtual marketplace where consumers now have more options and flexibility to make purchases from different suppliers around the world. The cyberspace as an interconnection of web technology makes the sharing of digital information, products and services available to a broader range of participants. Thus with the aid of their computing devices, cybercitizens can create, share and access various products and services across the globe. According to Internet Live Stats [21], there are currently more than 4 billion home internet users worldwide. Thus more than half of the world's population are now active participants in the cyber world with an average user spending approximately 6 hours online each day [22].

A number of research papers have identified security as the most important attribute of commerce on the internet [23–25]. For instance, Aliyu et al. [23] identified security and privacy as one of the important features that can affect the extent to which Islamic websites are used. Visible mechanisms such as encrypted data, status of protection by firewalls, and digital certificates influence how users perceive digital security in general. Cybersecurity mechanisms can, therefore, be designed in a way that will help build trust and improve users' security perceptions and attitude online. First, an extensive review of cybersecurity-related literature is necessary to determine established knowledge within the field and areas needing further investigation and improvement.

In this chapter, Section 2.2 explains the security and privacy exposures inherent in web browsers. Section 2.3 highlights the need for comprehensive cybersecurity by defining cybersecurity with a focus on its multidisciplinary requirements and global relevance. Section 2.4 then lists and discusses the major types of technical security mechanisms relevant for cybersecurity implementation and their related usability issues. Following the review of the extant literature examining the usability of different types of technical security controls, the specific security features commonly found in modern web browsers are discussed in Section 2.5. To conclude the chapter, best practices, and approaches that can be adopted and/or integrated by average computer users to protect themselves against different kinds of cyber threats are briefly discussed and then findings of the literature review are summarised.

2.2 Vulnerabilities in Web Browsers

Web browsers (often referred to as browsers) are one of the most common software applications used to actively participate in the virtual world of cyberspace. They have thus become an integral part of our daily lives. Browsers are used daily to search for academic publications, access emails, news articles, entertainment programs, and conduct various kinds of businesses online. This trend has turned browsers into one of the most common points of attack against information systems as shown in Figure 2.1. This is because browsers generally have inherent vulnerabilities that are easily exploitable by unauthorised users (attackers, hackers etc.). Despite their built-in security features, all browsers have design issues making them susceptible to exploitation and attacks [26, 27]. Consequently, attackers are able to use web browsers to take control of computers connected to the internet and steal or destroy sensitive electronic resources.

Security exposures are continually detected in top modern browsers each year of which cyber-criminals do not hesitate to exploit (Figure 2.2). Attacks like phishing and distributed denial of services (DDoS) are facilitated by users who assess malicious websites or legitimate websites that have been compromised. Attackers can focus on exploiting computer systems through various web browser vulnerabilities with the aim

[1] Source: https://securelist.com/kaspersky-security-bulletin-2015-overall-statistics-for-2015/73038/

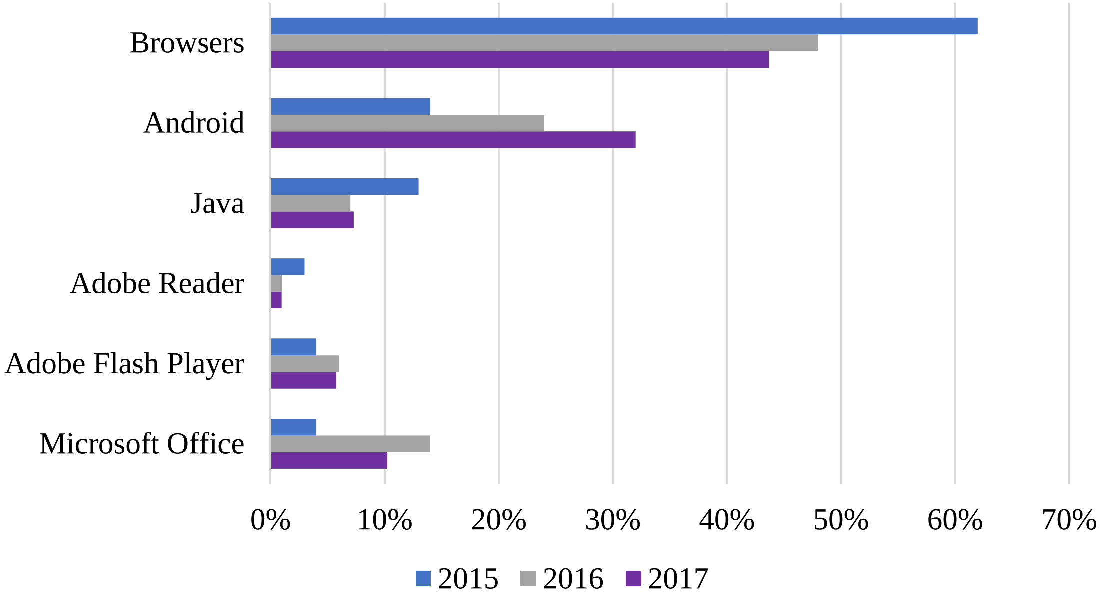


FIGURE 2.1: Distribution of exploits used in attacks by the type of application attacked 2015 - Q1 2017 [1]

of corrupting data files, stealing information and/or taking control of personal computers and using them to attack other information systems. For instance, malware can be installed on a system to bypass access controls and cause harm to the host computer just by visiting a malicious website unknowingly (drive-by download) or by clicking a link on a compromised web page. A 'drive-by download' occurs when malware is unintentionally downloaded and installed unto a computer without the user's consent by exploiting a vulnerability in the web browser [28]. Malware generally refers to a broad variety of malicious software such as spyware, viruses, worms, adware, bots, trojan horses etc. Most malware types deployed online may either act primarily as spyware or have spyware-like features [29]. For instance, a scan performed by America Online and the National Cyber Security Alliance (AOL/NCSA) [30] discovered spyware programs on 80% of 329 computers with an average of 93 spyware components on each infected computer.

The categories of people who normally use spyware to extract data from systems includes marketing organisations, trusted insiders (e.g. friends, family), organised crime groups and online attackers. The motivation for spyware perpetrators, therefore, ranges from simple curiosity like finding out about a spouse's shopping habit to more hideous crimes such as identity theft, credit card fraud etc. One can encounter different forms of cyber-attacks when browsing online especially if the security settings of the browser are not optimised. As shown in Figure 2.3, most cyber-attacks are facilitated by exploring certain features of web browsers. These features include Browser Helper Objects (BHO), Scripting Platforms, Cookies, Web Bugs, ActiveX, Java, and Plugins. The associated vulnerabilities of some of these web browser features are briefly described in this section.

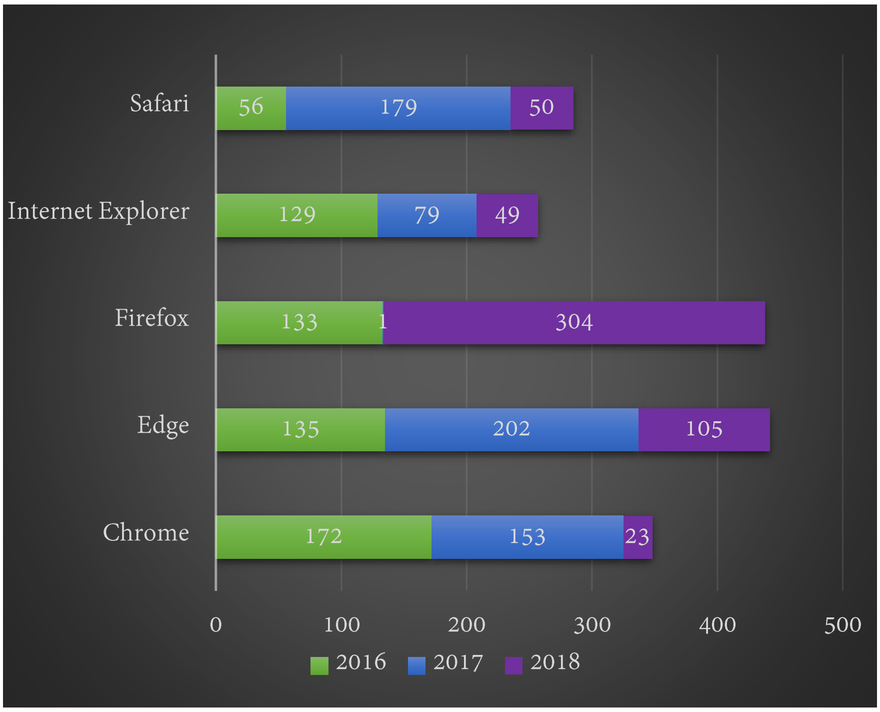


FIGURE 2.2: Vulnerabilities detected in popular modern browsers: 2016–2018(Source: CVEdetails.com)

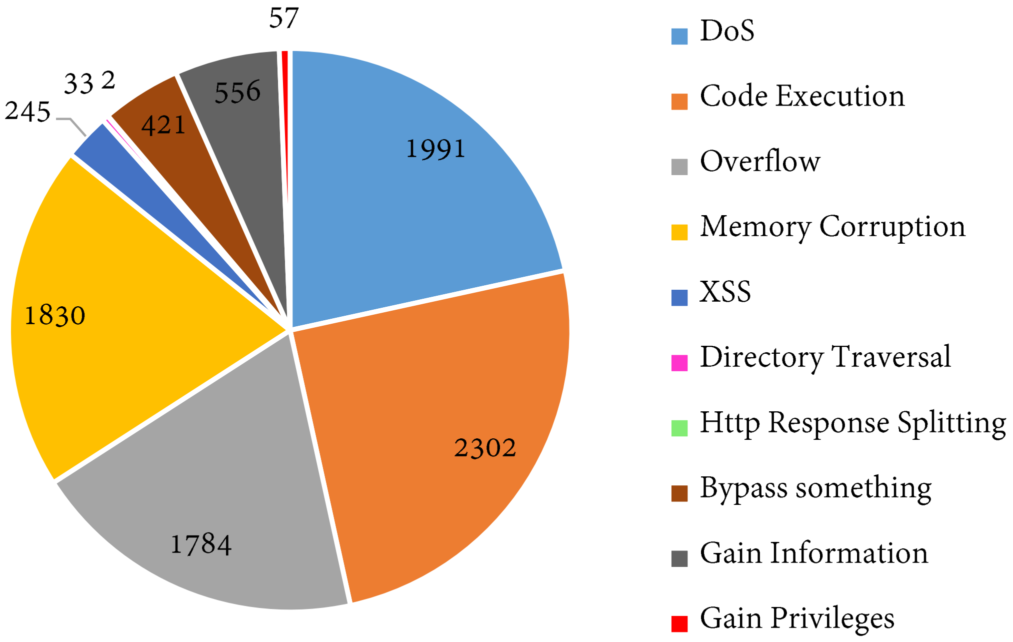


FIGURE 2.3: Types of browser vulnerabilities exploited by cybercriminals: 2016–2018 (Source: CVEdetails.com)

2.2.1 Browser Helper Objects/ Extensions

BHO which were designed by Microsoft to extend the functionalities of the web browser (Internet Explorer (IE)) are being severely exploited for malicious purposes such as the spread of spyware. This is because BHO are allowed easy access to data and system resources that the currently logged on user is authorised to access both within and outside the IE process space. Thus, once they are installed, BHO load automatically into the process space whenever IE is started and begin to operate independently. [29]. BHO can go unnoticed whiles carrying out its functions which can include access to user data or system files, modify browser settings or access network resources to download and install further malware. Extensions are like BHO for other web browsers such as Firefox and Chrome. Both of these web browser features use the same web technologies and are fairly easy to develop but work differently in each type of browser [31, 32]. Gühring [31] described special types of Trojans that use BHO and other browser manipulation techniques to by-pass any authentication system installed on a personal computer (PC) as the single channel for transactions between the server and clients. Accordingly, these Trojans can modify transactions being carried out by users with web browsers on the spot without being detected. Notable among their proposed solutions to such vulnerabilities is a hardened browser that fulfils specific security requirements to be compiled into one static binary which can be personalised for every user. Apart from Trojans, various types of spyware programs mostly employ BHO techniques to monitor users' behaviour and take-over browser actions. In a study to examine the Auto-Start Extensibility Points (ASEP) of spyware programs, Yi-Min Wang, et al. Wang et al. [33] found close to 90 out of 120 distinct spyware hooked to BHO for auto-starting and monitoring of user activities. Spyware programs that are implemented as BHO or browser toolbars are very difficult to detect using the traditional signature-based anti-spyware tools as they are not able to detect malware instances that are not previously seen/known [34].

2.2.2 Cross-Site Scripting (XSS) Vulnerabilities

Scripting languages such as JavaScript, JScript, VBScript, and ECMAScript are integrated with web browsers which allow diverse features and interactivity to be added to web pages. As these scripting tools share the same address space with the browser, attackers can take full advantage to inject malicious codes into memory for execution. Although XSS is usually not due to a failure in the web browser, XSS attacks are ultimately targeted at clients running specific web browsers. This is because XSS vulnerabilities results from sites that fail to validate user input being returned to the web browser of the client. XSS vulnerabilities can be exploited to disclose information stored in cookies, hijack user accounts, compromise private information, cause DoS attacks and execute codes for many other malicious purposes. Abgrall et al. [35] analysed six different families of web browsers (IE, Netscape, Firefox, Opera, Safari and Chrome) over a decade and found that their attack surface under XSS did not decrease or stabilise overtime. Thus, even though web browsers keep evolving with each new version release, it does not necessarily lead to an improvement in their degree of exposure to XSS attacks. Three main types of XSS have been identified and described in the cybersecurity literature namely Reflected, Stored and DOM-Based XSS. Reflected and Stored

XSS attacks are executed on the server side but in the case of DOM-Based XSS, the client (web browser) performs the injection of the XSS into the web-page. Hydara et al. [36] conducted a systematic review of XSS related studies and found that only one out of the 115 related research papers dealt specifically with DOM-Based XSS. They attributed the lack of research focuses on the DOM-Based XSS to the difficulty involved in accessing client-side scripts for empirical analysis.

Previous comparative analyses of popular web browsers have revealed the varying levels of protection they offer against security threats [27]. NSS Labs [27] however concur that browsers, in general, remain the primary starting point for cyber attacks. More recently, very dangerous vulnerabilities were discovered in current web browsers [37]. Accordingly, the security exposure which is termed CVE-2018-6177, exploit weaknesses in video or audio HTML tags allowing remote attackers to access people's social media messages or emails. In 2017, PwC UK [38] investigated a new threat actor against managed information technology (IT) service providers and discovered over 20 million individual's personal data was compromised between 2014 to 2015 in the USA alone. They also found out that about 5.4 million records in health information systems were accessed during a security breach in 2014. More recent data from Internet Live Stats [39] indicates over 30 million websites were hacked in 2018 alone. The need for cybersecurity has, therefore, become more apparent as more information systems and applications adopt web technology for the collection, transfer and storage of information which are mostly private/ sensitive.

2.3 The Need for A Systematic Cybersecurity Development

Security in computer science can be defined as the ability of a system to protect its resources including data with respect to three main goals, namely: confidentiality, integrity, and availability (CIA). A distinction can be made between general computer security and network security whereby the former focuses on preventing and/or detecting unauthorised actions by users on a computer system. Network security, on the other hand, includes controlling authorised and unauthorised access to computers across network connections. Cybersecurity is therefore concerned with the protection of devices, applications, and data that connects to the internet from unauthorised access and usage. As more and more things are being attached to networks and connected to the internet (the era of Internet of Things (IoT)), it is becoming quite impossible to separate security on stand-alone computers from cybersecurity. Hence computer and network security need to go hand in hand to achieve the three CIA goals of security in the digital world. Various authors have defined cybersecurity from different perspectives. For instance, the definitions by Amoroso [40] and Kemmerer [41] mainly highlights the technical aspects of cybersecurity. More recently, Canongia and Mandarino Jr [42] defined cybersecurity as:

"The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure."

This definition broadly views cybersecurity from a national perspective with no reference to personal safety or privacy within cyberspace. Cavelty [43] made a distinction between national security and human security. He indicated that the former entails actions that affect social functions relying on IT and other critical infrastructures while the latter involves actions affecting acquired values like anonymity, privacy and other personal freedoms. More often than not, cybersecurity strategies tend to be targeted at protecting national and/or organisational security. Adopting a top-down approach by focusing on the higher level (especially the nation and big corporations) have only led to individuals' security needs being undermined. There is, therefore, the need to systematically balance national and individual security. This research seeks to provide a holistic understanding of the effect of individuals' cybersecurity perceptions, attitudes and/or behaviours. This holistic view of human online security is not just relevant in improving the usability of cybersecurity tools but also in determining appropriate policies.

Craigen et al. [44] draw attention to the fact that, most definitions on cybersecurity miss the interdisciplinary nature of the field and tends to focus on the technical perspective. They posited the following definition after reviewing the literature and engaging with a multidisciplinary group of cybersecurity practitioners from varying backgrounds:
"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."

Accordingly, their proposed definition is aimed at capturing the multi-dimensions of cybersecurity to promote more interdisciplinary approach in addressing emerging complex security challenges in cyberspace. Ross and Johnson [45] classify security controls into three categories of management, operational and technical countermeasures that are applied to protect the CIA of systems and the information they handle. Contrary to technical controls/mechanisms that use technology-based set-ups such as encryption techniques and firewalls as system protection measures, operational and managerial controls focus on security risks and incidents that are monitored and managed by people. Thus mechanisms such as usage policies, business continuity planning, employee training, local regulations, and other non-technical information security guidelines and/or procedures are considered to be operational and managerial security controls.

As more and more people are able to gather, process, transfer or store sensitive commercial and personal data over the internet, cybersecurity threats are also rapidly evolving. The interdependence nature of the internet is increasing the risk of security attacks aimed at destroying, stealing or denying access to vital information or web-based services. Achieving the aforementioned security goals are therefore as vital to the data protection needs of domestic internet users as to corporate and government networks. Thus whether a user is designing a new product line or sending instant messages to relatives, keeping some information confidential is always desired. People generally want to be assured that, nobody will tamper with their information without their consent. People also want their data to be readily available and accessible at any point in time. Unfortunately, any form of data, be it corporate or personal, that is exposed to the internet are at risk of being compromised. Internet users, therefore, need to be knowledgeable about security mechanisms that can be utilised to minimise such risks.

2.4 Technical Security Controls

Technical security controls include mechanisms such as firewalls, anti-viruses, user authentication, encryption technologies, Intrusion Detection Systems (IDS) and other technology-based security countermeasures. These mechanisms come in a variety of software and hardware packages that can be adopted to mitigate cybersecurity threats and attacks. For instance, different types of encryption applications are available for the protection of digital contents whiles in storage or during electronic transmissions. Some of the technical security controls also focus on authorising access to electronic resources.

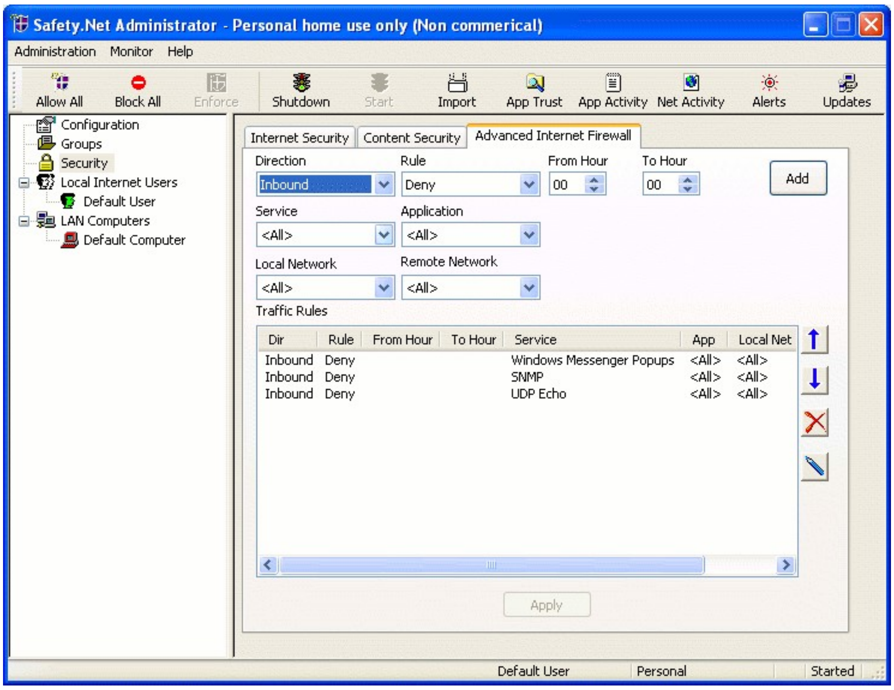
A number of usable computer security research papers have evaluated some of these technical security controls. Kainda et al. [46] classified usability studies in the field into six general categories which comprise: authentication, encryption, Public Key Infrastructure (PKI), device pairing, security tools, and security systems. User authentication and email encryption, in particular, have received significant attention from the usable cybersecurity community (e.g. [47–51]) However less attention has been paid to the other technical security controls such as anti-viruses and IDS. Here, technical mechanisms that are fundamental to cyber security such as firewalls, anti-phishing tools etc. are individually examined based on their existing usability studies. Although the security mechanisms examined here can be classified under some of the categories identified, they are mostly security tools.

2.4.1 Firewalls

Firewalls which are used as the first line of defence for computers connected to the internet could be in the form of a hardware or software which acts as filters between individual computer systems or home networks and external networks like the internet. In typical home settings, devices like routers, cable or digital subscriber line (DSL) modems, printers, and smart appliances like television, phones etc. can make up a home network. The choices of firewalls available to users, therefore, include those built into operating systems like Windows, those included in internet security suites, as well as stand-alone third-party firewall software or hardware. However, in the context of non-corporate internet users, firewalls are typically specialized software running on individual computers. These personal firewalls which are implemented in software are now considered to be an essential part of online security [52]. Examples are Agnitum Outpost Pro Firewall, Comodo Internet Security Plus, and Kaspersky Internet Security for computers running on Windows platform.

Firewalls generally have several security settings and require proper configurations in order to attain a proper balance between safety and accessibility [53]. Figure 2.4 shows an example of a firewall interface with several tabs for different settings and functionalities which a user needs to understand and configure. However, as is the case with most security mechanisms, firewall settings are complex and can be compromised by misconfiguration which can lead to security vulnerabilities [54]. Apart from serious security vulnerability which can be exploited by hackers, firewall misconfiguration can also limit users' options (if users choose firewall settings that are too restrictive). A number of researchers have focused on the usability of firewalls within corporate networks and have found them very unfriendly for even IT security experts [54–56].

While personal firewalls are not as complex as enterprise ones, the majority of internet users are not computer security expert and may not possess the knowledge and skills required to configure and manage firewalls. In effect, most personal firewalls



Direction: Inbound
Rule: Deny
From Hour: 00
To Hour: 00
Service: <All>
Application: <All>
Local Network: <All>
Remote Network: <All>

Traffic Rules

Dir	Rule	From Hour	To Hour	Service	App	Local Net
Inbound	Deny			Windows Messenger Popups	<All>	<All>
Inbound	Deny			SNMP	<All>	<All>
Inbound	Deny			UDP Echo	<All>	<All>

FIGURE 2.4: NetVeda Safety Net firewall configuration interface

come with pre-configured security policies that users can choose from and/or customize them to their specific needs. Others attempt to reduce the complexity of firewalls by concealing their operational details. Meanwhile, a number of usable security researchers who have investigated personal firewalls, emphasise the need to provide more information about the security state of personal firewalls to their users (e.g. [57–59]). For instance, Herzog and Shahmehri [57] found that, though Microsoft Windows XP built-in firewalls do not prevent outgoing connections, the basic interface provided does not clearly indicate the absence of such a feature. This has the potential of giving users a false sense of protection, hence making them more vulnerable to attacks. Even though the built-in firewalls for subsequent Microsoft Windows (Vista, Windows 7 and 8) included the feature to protect both inbound and outbound traffics, the basic interface provided still hides the ability to create firewall rules from users. Thus there is the need to provide enough functional details to enable users in making informed decisions and avoid dangerous errors whiles using these personal firewalls. In summary, although modern-day personal firewalls are generally considered usable from a traditional HCI point of view, several usability issues are discovered when evaluated based on usable security principles [57, 60].

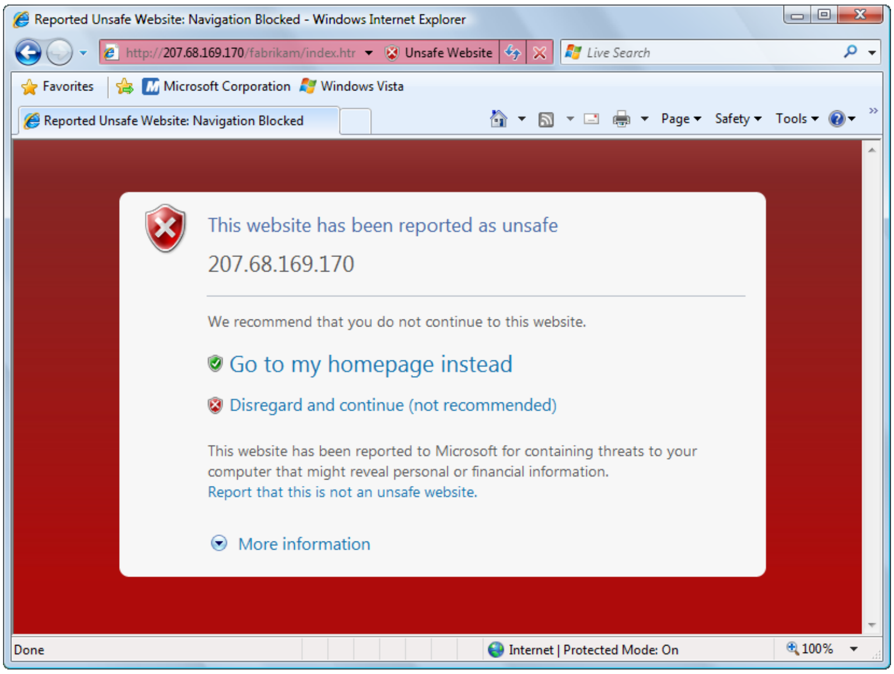
2.4.2 Anti-virus Software

Anti-virus is another popular tool commonly adopted by internet users to protect themselves against security threats. Some of the most popular anti-virus brands, include Symantec, McAfee, Kaspersky Lab, Bitdefender, and Avast. Although anti-virus plays a fundamental role in protecting users against different kinds of malware, usability studies on them are almost non-existent. This could be attributed to the view that most anti-viruses are designed to run in the background looking for known viruses and other suspicious processes hence limited interaction with users are expected. Consequently, most studies conducted on anti-viruses tend to focus on their technical effectiveness and mostly within the context of corporate organisations. Post and Kagan [61] evaluated the effectiveness of different anti-virus packages adopted by organisations and found that anti-viruses are less effective in preventing the spread of viruses on workstations than they are on network servers. They attributed the success on network servers to the fact that IT staffs put more effort into ensuring that the chosen anti-virus is installed and maintained properly.

Considering that many people requiring anti-viruses these days are not computer experts, it is important that these fundamental security tools are designed for users to comfortably use them in dealing with malware [62, 63]. The only papers found that touched on the usability of personal anti-viruses at the time of this review were those of [62, 64, 65]. Although Khan and Abbas [65] attempted to evaluate four different anti-virus software products for both security and usability, the approach they adopted falls short of adequate security usability studies. As is mostly the case for anti-virus software analysis, their study focused more on the technical capabilities of the four anti-virus products they chose to review rather than their usability. Cheung et al. [62] evaluated the usability of a commercial anti-virus software (Sophos) through a mixed approach of user survey, cognitive walk-through and heuristic evaluation. They found a number of usability problems with the interface provided for users to carry out tasks like scheduling a scan for their computer system and dealing with an identified virus. Furnell and Clarke [64] touched briefly on anti-virus usability and pointed out that as vendors move away from stand-alone security safeguards to integrated internet security suits, users are faced with more complex interfaces. Thus the consequent burden of understanding the full set of security functionality of anti-viruses provided through the surrounding options is increased.

2.4.3 Anti-Phishing Tools

Anti-phishing tools are now available as web browser toolbars which can be installed by users to protect themselves against attacks aimed at tricking them to give up personal information. Anti-phishing tools adopt various approaches including the use of blacklists, whitelists, ratings, and heuristics to determine fraudulent sites and activities online. These anti-phishing solutions ultimately depend on users' ability to make appropriate decisions from the feedbacks they receive either in the form of pop-up windows or other forms of icons as illustrated in Figures 2.5 and 2.6. Most usability studies on anti-phishing products, therefore, tend to focus on the effectiveness of the types of alerts provided to aid users' security decision online.


Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
http://207.68.169.170/fabrikam/index.htr
Unsafe Website
Live Search
Favorites
Microsoft Corporation
Windows Vista
Reported Unsafe Website: Navigation Blocked
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%

This website has been reported as unsafe

207.68.169.170

We recommend that you do not continue to this website.

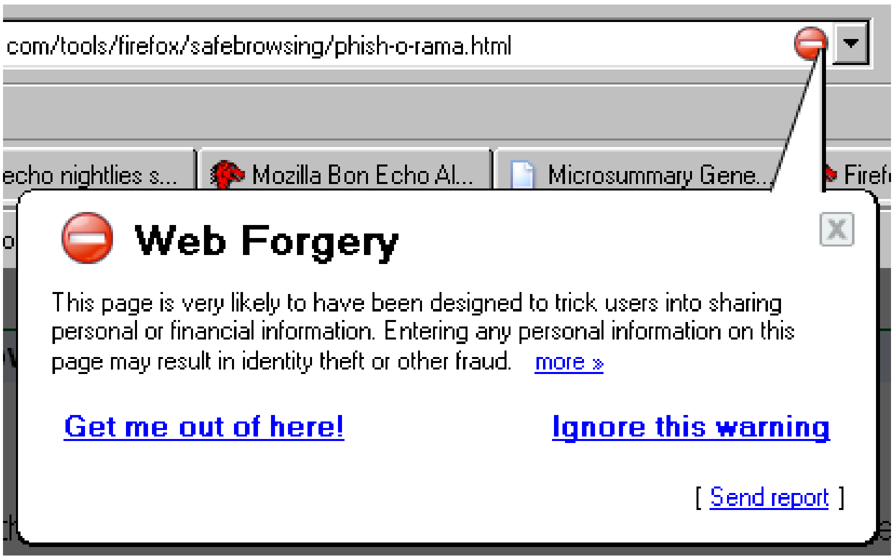
Go to my homepage instead

Disregard and continue (not recommended)

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this is not an unsafe website.

More information

FIGURE 2.5: A pop-up window alerting on a suspected phishing site with which a user has to make an explicit decision



This page is very likely to have been designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud.

FIGURE 2.6: An icon being used together with a pop-up window to indicate a suspected phishing site

Wu et al. [66] conducted usability studies on anti-phishing tools categorised into three groups based on the type of information displayed by the toolbars in the web browser and found all of them to be ineffective at preventing users from being tricked by high-level phishing attacks. They attributed most of the problems to the inability of users to check and interpret security warnings which were sometimes due to the nature of security indicators provided by the anti-phishing tool. Dhamija et al. [48] analysed a collection of phishing attacks and discovered that the anti-phishing cues involved were not effective for a substantial fraction of users.

2.4.4 Trust Systems and PKI

Digital certificates issued by Certification Authorities (CA) are used to establish trust in the digital world. Fundamentally, digital certificates provide a basis for trust by authoritatively binding identity to various forms of data structures so as to achieve trusted communications and other secured interactions within IT-systems. Thus digital certificates are used in verifying the authenticity of digital communications as well as other security-related interactions such as code signing, application policy signing, document signing, driver verification, and digital rights validation. Public key cryptography (PKC) and/or infrastructure (PKI), which is currently used to realise the concept of digital certificates and signatures, have multiple layers of protocols and working units dealing with issuance, verification, revocation and several software components [67]. CAs are the most essential units of any PKI system as they are responsible for the certification of the key pair/identity binding. Most Operating systems (OSs) and internet browsers are pre-configured with a list of trusted CAs to enhance usability and systems interoperability.

In recent times however, a few research articles have highlighted certain weaknesses in the digital certification system that is being exploited for fraudulent purposes. For instance, Wood [68] identified lack of rigorous identity vetting process, the extended time period for certificate revocation, unsafe default security settings for browsers and OS, and poor user attitude to security warnings as some of the weaknesses being exploited by malware authors. Accordingly, most software components that rely on digital certificates either provide warnings that users easily ignore, have critical settings that are disabled by defaults or by the malware itself. They also indicated that malware authors are abusing some of the strengths associated with PKC such as malware encryption as in the case of secure botnet command and control. On the other hand, Zissis and Lekkas [67] focused on the trust decision aspect of digital certification systems arguing that delegating the security judgement to intermediate entities such as internet browsers and OSs on behalf of the end user is not the way to go. They emphasised the need to improve the user-friendliness of trust interactions and digital certificates and proposed an approach that is based on openness so as to empower users to make informed trust decisions by themselves.

2.4.5 Encryption and Authentication Mechanisms

As mentioned earlier, email encryption and user authentication have received significant attention from the usable security research community (e.g.[47, 49–51, 69–72] etc.). However, there still remains the need to look at encryption and authentication mechanisms more holistically in terms of data protection in general rather than just emails. There are two main categories of encryption technologies available for encrypting data on personal computer disk drives. Software-based encryption such as BitLocker, FileVault and TrueCrypt uses the computer's CPU for all cryptographic operations including encryption and decryption. Hardware-based encryption is a more recent innovation whereby cryptographic functions are completely handled within the hard disk drive (e.g. Seagate Secure SED, Intel's SSD 320 AND 520 series). Müller et al. [73] evaluated the security of hardware-based Full Disk Encryption (FDE) and found that though they are more user-friendly, software-based FDE is generally more secure. Their findings are consistent with that of [74] who also concluded that the barriers of usability and performance are well addressed by hardware-based encryption. They, however, indicated that software-based products have the advantage of providing encryption at the folder and file level as well for removable storage devices.

The relevance of protecting sensitive data with encryption tools is highlighted in the face of all the risks associated with ubiquitous and interconnected computing. Encryption technologies basically help ensure that digitally stored personal and/or sensitive data is unexposed even when the storage systems are under attack, stolen, damaged or lost. Despite the recognisable benefits of data encryption, most users shy away from adopting these technologies. Most privacy breaches could have been prevented had the users involved encrypted their data or storage driver. Most people just assumed that once they have all layers of password authentication processes in place, their sensitive data are secured from prying eyes. Although encryption of data on tablets, notebooks, and laptops are now widely considered to be best practice towards the protection of privacy, adoption of encryption products is quite slow. According to [74], the main barriers to widespread adoption of encryption technologies are system performance, complexity, and cost. Thus encryption products have been found to be difficult to configure and implement even by IT experts.

2.4.6 Intrusion Detection Systems (IDS)

IDS which in recent times have become a standard component of network security management are computer programs that are used to help in identifying unauthorized use and abuse of computer systems [75]. Intrusion in this context refers to unauthorised accesses by either hackers or authorised users of a system that can cause wilful or incidental damage to a computer system and its resources. For instance, authorised users of a system can create vulnerabilities or damage by attempting to gain additional privileges for which they are not authorised. With increasing global network connectivity as well as growth of the network attack landscape, IDS provides the platform to automate the monitoring and analysis of network anomalies. Depending on where the intrusion is detected, IDS can be classified into either a Host-based or Network-based. The host-based IDS which detects malicious activities on the host they operate on have the advantage of being easier to implement in terms of time and effort [76]. On the other hand, Network-based IDS operates at the network level rather than at each separate host level and have the advantage of incurring minimal overhead cost in terms of its effect on the performance of other programs running over the network [77].

IDS are designed to support the detection of intrusion and effective real-time response to malicious activities that are detected. Thus, unlike most of the security controls reviewed in this research, IDS are not necessarily meant to strengthen the security perimeter but rather to detect attacks when they do happen and for prompt reaction to malicious events so as to minimise overall cost or damage of attacks. However, because IDS are not yet fully reliable in detecting intrusions due to problems with false positives and negatives, human experts are mostly required to work with them [76]. IDS were therefore conventionally used by network administrators as intrusion is essentially a network-based activity. In effect, IDS are generally designed for users with some level of computer security expertise. Although a number of published research works have indicated the need for usability studies on IDS, most of the research efforts in this area tends to focus on the capabilities of the different monitoring techniques that can be adopted in the IDS implementation be it the location of the detection, type of algorithm and so on and so forth. Patil et al. [78] performed a heuristic-based usability analysis of IDS UIs and found them to be highly difficult to learn and use. Specifically, interpretation of the IDS outputs was quite difficult for users due to too many technical specifications as well as inclusion of unrelated information on the display. The installation and configuration of the IDS tested were also found to be quite cumbersome.

2.5 Web Browser Security and Privacy Features

A web browser is an application software used to retrieve, transmit and present digital information resources on the web [79]. It has become the main gateway to the web as computer users now mostly use the browser to check emails, chat, play games, shop, watch movies, read news, search for articles etc. This trend has led to the emergence of browser-based operating systems (e.g. Chromium OS) targeted at people who spend most of their computer hours on the internet [80]. As the main gateway to the web, it has also become the first line of defence against system invasion and cyber attacks [81]. Most of the popular web browsers come with a lot of built-in security features to help protect the computer against malware infection and invasion of users' privacy. Some of the security mechanisms described in the preceding sections (2.4) (e.g. anti-phishing, encryption, and authentication mechanisms) are part of the security suits integrated into some of the modern browsers. However, there are other security and privacy features unique to web browsers due to their inherent vulnerabilities. For instance, the mechanisms used to control ActiveX, JavaScript, Cookies are necessary because they are software features used to improve user experience in web browsers.

Consequently, features like content management, private browsing, password manager, extension/ plug-in controls, etc. are among the security and privacy features commonly offered by most modern browsers. In 2013, Mylonas et al. [82] evaluated the security controls in popular desktop and smart-phone browsers and found 32 security and privacy features that can be configured through the browser's user interface (UI). Browsers at that time did not necessarily implement all of the identified features but almost all modern browsers now offer all of these controls and more. In this study, 34 different configurations were identified for three main desktop web browser controls namely: privacy/ content management, security maintenance, and extensions/plug-in controls (see Table 2.1). A preliminary evaluation conducted by the same authors in [83] revealed three major potential usability issues in desktop browsers namely: Invisibility of navigation paths, poor organisation of UI items, and inadequate Feedback/ User prompts. Earlier Botha et al. [84] also explored security features in desktop browsers comparing their availability in mobile browsers from an expert user's perspective. Their findings led to the conclusion that security features implemented on web browsers lack usability elements especially in the context of mobile devices.

Even though the studies referenced above touched on the user-friendliness of web browser security features, no empirical user studies were conducted with representative human participants. This thesis project has identified the usability testing of web

TABLE 2.1: A compilation of browser security and privacy controls

Controls	Available Configurations
Privacy & Content	1. Block cookies
	2. Block images
	3. Block pop-ups
	4. Block location data
	5. Block referrer
	6. Enable DNT
	7. History manager
	8. Private browsing
	9. Enable Sync Features
	10. Encrypt stored browsing data
	11. Back-up browsing data
Security Maintenance	12. Browser update
	13. Certificate manager
	14. Certificate warning
	15. Local blacklist
	16. Malware protection
	17. Modify user-agent
	18. Password Manager
	19. Phishing protection
	20. Proxy server
	21. Report rogue Website
	22. Search engine manager
	23. SSL/TLS version selection
	24. Task manager
	25. Website checking
Extensions/ Plugin Management	26. Disable Java
	27. Disable Scripting Languages
	28. Disable Extensions
	29. Disable Plugins
	30. Enable Extensions
	31. Enable Plugins
	32. Install / uninstall add-ons
	33. Update plugins
	34. Update extensions

browser security features with typical non-expert users as a critical step towards the design and development of more usable security tools. Designing more user-friendly UI for browser security features would empower users to take charge of their own safety online and be less vulnerable to cyber attacks. Existing usability studies involving web browsers mostly focused on specific features rather than the entire suites of built-in security and privacy controls. For instance Clark et al. [85] evaluated the usability of Tor which is a privacy tool for anonymous web browsing. They engaged expert evaluators to explore the Tor interface and installation process through a cognitive walk-through approach and heuristic analysis of the usability issues observed. Several studies have also focused on the usability of visual security cues in web browsers [48, 66, 86, 87] and found them ineffective due to varying usability issues.

2.6 Selection of Countermeasures

Before the revolution of PC, a few technical and physical mechanisms were enough to secure a complete computer system. However, as computer technology advanced from multiprocessing to distributed networked systems with Internet connections, additional technical and new operational controls are now required to protect computer systems from harm [88]. To effectively achieve the security objectives/goals mentioned earlier, one may need to adopt and integrate different types of security mechanisms on different levels.

Just as security needs differ from one corporate entity to another, it may also differ with different individuals. In his book "Secrets and Lies", Schneier [89] identified different types of security needs including privacy, anonymity, trust authentication, data integrity, audit trails and/or fraud prevention and detection. Schneier described these needs in relation to different categories of computer users (i.e. individuals, military organisations, private corporations, and governments). For instance, a university's security requirements may be different from that of a military organisation based on their approaches to information sharing. In some regards, universities are interested in making research findings available to other academics or the general public. Military organisations, on the other hand, prize secrecy and tend to implement multilevel security measures. In the case of individuals, some users may be more interested in controlling access to their private network whiles for others the priority may be to protect sensitive files on their computer systems. The key point here is that people need to be aware of their security objectives in order to determine appropriate levels of security requirements to be met. Cyber safety measures which may be physical, technical or operational can then be used to enforce security policies towards the achievement of digital security goals.

The adoption and integration of different types of controls have, therefore, become a more efficient and effective way of securing computer systems in the cyber world as it allows for a layered defence to be maintained. Although this principle applies to enterprise-based security solutions, it logically applies to individuals seeking computer security solutions as well. Thus a security culture is necessary on an individual level to support and sustain the defensive strategies once the required technical security mechanisms have been set-up. The operational controls, in this case, might include guidelines that will inform people how to act in certain situations with the goal of protecting their personal privacy, and data asset. For instance, a personal policy to always choose strong passwords and manage them securely is non-technical but can make it more difficult for a non-technical attacker to break into the person's computer system [90, 91].

2.7 Summary

This chapter covered the importance of cybersecurity in networked systems and discussed the different technical controls found in literature from a usability perspective. Table 2.2 presents a summary of all the security mechanisms covered in the review along with related references to any known usability glitches. The review revealed a fundamental gap in the extant literature. User studies that explored the user-friendliness of web browser security controls in its entirety with typical non-expert participants are almost non-existent. As these users all have varying characteristics and backgrounds, it is important to solicit their preferences, opinions, and reactions to existing tools in order to effectively adapt future cybersecurity designs to their satisfaction.

TABLE 2.2: Summary of available cybersecurity mechanisms and related usability issues.

Security mechanism	**Protection offered**	**Known usability issues**	**Refs.**
Personal Firewalls	Filter out and block unwanted traffics in and out of a computer network	Lack of clear security status indicators, Complex UI, and Technical Language,	[57–60]
Anti-virus software	Detect, prevent, and/ or eliminate malware infection	Complex UI, Inadequate configuration cues, and Poorly designed alerts.	[62, 64, 65].
Anti-Phishing Tools	Detect suspicious content contained in websites, e-mail, or other forms used in accessing data and alert the targeted user or automatically block the phishing content	Poorly designed pop-ups, Mismatched mental-models for security indicators, and Ineffective alert information.	[48, 66]

Trust Systems and PKI	Verify the authenticity of digital communications. Verify security-related interactions such as code signing, application policy signing, document signing, driver verification and digital rights validation.	Lack of user control options, Inefficient warning design	[67, 68]
Encryption and Authentication Mechanisms	Protect sensitive data from unauthorized access.	Complex configuration required, Technical Language, Lack of integrated guidelines	[47, 49–51, 69–72]
Intrusion Detection Systems (IDS)	detect attacks when they do happen for prompt reaction to malicious events	Irrelevant information, technical specifications, Complex installation and configuration requirements.	[78]
Security and Privacy Controls in Web browsers	Protect the computer against malware infection through the web browser, prevent or minimize user privacy invasion online.	Invisibility of navigation paths, poor organisation of UI items, ineffective security cues and inadequate feedback/ user prompts.	[83, 85–87]

The next chapter focuses on the usability and acceptability of security mechanisms. These two attributes are vital to cybersecurity mechanism as their value can diminish if users are unwilling to adopt them (acceptability) or cannot use them due to poor usability. The discussions of these two topics, therefore, led to the formulation of the research model and design in Chapter 3. The hypothesis formed based on the proposed research model will then be tested and evaluated in the subsequent chapters.

CHAPTER 3

Human Aspects of Cybersecurity: Background and Methodology

Contents

"Anyone who thinks that security products alone
offer true security is settling for the illusion of security"
Mitnick and Simon [92].

3.1 Introduction

In recent years, there has been an increasing interest in the role users play in maintaining security within the digital economy. The adoption and appropriate usage of security mechanisms by home computer users (hereinafter referred to as users or HCUs) in particular have become a central concern for the usable security research community. Howe et al. [93] described HCUs users as people who have not received any formal training to use computers but use them to support various tasks in non-work environments. Despite advances in cybersecurity technological solutions, most HCUs are still unable to effectively access them for the protection of their digital assets. As HCUs are increasingly targeted in security breaches [94], there is an urgent need to understand their cybersecurity behaviours and how best to enhance them. Unfortunately, reliable information on what influences users' cybersecurity practice (and how that information could be maximized to make cybersecurity mechanisms more usable) is still very scarce.

Recently, cybersecurity researchers and key industry players have shown an increased interest in making cybersecurity accessible to the average user as part of collective efforts towards the security of cyberspaces. People need to improve their security practices regularly which means they must be willing to learn and adopt the best security policies, and the mechanisms to ensure those policies. The National Institute of Standards and Technology (NIST) suggests that the best way of involving everybody is to create incentives that can motivate everybody within the cyber economy [95]. It is becoming increasingly important to minimise the gap between people and cybersecurity technologies in order to promote more frequent usage and reduce human errors and dissatisfaction. A very important step towards the achievement of this goal is to identify and understand the dimensions along which users are similar and dissimilar and the effects of these factors on interactions with security-related interfaces.

Usability is an important incentive as previous studies have highlighted its importance in determining the acceptance of any technology by users (e.g. [96]). Several usability studies on different types of security controls (e.g. firewalls, anti-virus) have illustrated how usability issues prevent end users from effectively leveraging them for their protection against security attacks [54, 62]. Usability is also known as a critical factor for technology acceptance [1, 24, 97]. Suh and Han [24] for instance, discovered that both security concerns and usability dimensions together have direct and indirect significant effects on the adoption of smartphones for internet banking. There is therefore, a reasonable assumption that improved usability of cybersecurity mechanisms can serve as a major incentive for users to adopt better security controls and behaviour online. However, lack of consideration of demographics such as gender, age, occupation and other socio-cultural variables puts a limitation on such assumptions. This is because differences in such variables can influence not just the perceived usability but the perceived acceptability and attitudes towards cybersecurity in general [98, 99]. Acquiring knowledge about users and their security behaviour is, therefore, a significant step in the process of improving the usability and acceptability of cybersecurity mechanisms. There is the need to further understand the factors that affect users' perceived benefits of security control as well as the dimensions that wholly describe people's attitude towards cybersecurity.

In this chapter, the second part of the literature and related works is presented, describing how usability and acceptability impacts on the adoption of cybersecurity tools by HCUs. It begins by describing the relationship between usability and software quality, laying and discussing the foundations of usable security. The various metrics used to evaluate usability are also outlined. Further sections discuss theories used in assessing the acceptability of information technology. Following the discussions on usability and acceptability evaluations, a method is elicited to better support the achievement of the research objectives. Thus the last part of the chapter presents the research model adopted in relation to the extant literature on usability and acceptability of cybersecurity mechanisms.

3.2 Usability of Security and Privacy Mechanisms

Usability broadly refers to the extent to which a system supports the ability to easily perform a desired task to achieve set goals in a manner that satisfies the user. It is regarded as a critical quality factor for the target users of a software [100]. Agarwal and Venkatesh [101] and Wilson [102] both remarked on the multidimensional nature of usability as a user interface characteristic requiring a multi-layered evaluation. Consequently, most of the definitions found on usability point to a set of dimensions rather than a definition of a single concept. For instance, usability for information systems is generally characterised by their ease of learning, memorability, reduced error rates, easy error recovery, efficiency and user satisfaction [1, 103]. The International Standards Organization (ISO) categorised these dimensions into three main attributes, defining usability as *" The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context"* [104]. Accordingly, the three ISO usability attributes of information systems are described as follows:

- Effectiveness refers to the successful completion of system task without errors and with minimal help. It is thus measured in terms of accuracy and completeness.
- Efficiency means that users are able to achieve specified goals quickly with the least possible effort. It is measured in terms of resources such as time, physical effort, mental workload etc.
- Satisfaction is the level of pleasure users associate with using the system. It is measured in terms of user comfort and acceptability.

For computing research, universal usability has been proposed for the design of computing technologies to accommodate users with different backgrounds in terms of age, gender, education, culture etc. A greater scope of the literature on usability engineering covers the design and development of usable computer applications. Hence several user-centred design guidelines (e.g.[103, 105]) are readily available and widely adopted in the design and development of consumer software. Although several consumer software are now successfully designed to be usable, security applications still seem to be lacking in their user-friendliness. For instance, most non-technical internet users are now able to successfully use web browsers to search for information and carry out different types of transactions on the internet. Contrarily, there has been little success with incorporating usability guidelines and standards into security-related interfaces. Security-related interfaces in the context of this research refer to the programs that allow users to manipulate security mechanisms on a system as well as control the effects of the users' manipulation and how security status is indicated.

Usability of security mechanisms, however, have longed been identified by computer security researchers as critical to ensuring the protection of information systems [50, 106]. This is because humans are a key component of any security system yet they are largely considered to be the weakest link of security. Mitnick and Simon [92] pointed out that no matter how technically robust a security technology is, an attacker can breakthrough by exploiting the human element. A cybersecurity mechanism thus can lose its value if users are unwilling to adopt it or cannot use it due to poor usability hence impact negatively on the usability of internet based applications [107]. Nevertheless, most non-security expert users still find it quite challenging to understand and correctly configure available security mechanisms to avoid system breaches and cyber-attacks.

A number of usable security studies (e.g.[46, 50, 108]) have made a distinction between usability of security software and non-security software and argued that usable security design strategies should essentially consider and address inherent properties that make the security domain quite challenging. Whitten and Tygar [50] discussed five properties underlying the usability problem of security and defined usable security software to be characterised by four underlying factors namely: awareness of security tasks, learnability, error prevention and comfortability of the user interface.

"Security software is usable if the people who are expected to use it: 1. are reliably made aware of the security tasks they need to perform; 2. are able to figure out how to successfully perform those tasks; 3. don't make dangerous errors; and 4. are sufficiently comfortable with the interface to continue using it."

They chose to evaluate the usability of a public key encryption program (PGP 5.0), which came with a good user interface by traditional usability standard but found that it was not usable enough for the average computer user. Accordingly, different interface design techniques are required for effective security-related interfaces and a special case exist when adopting prevailing general usability standards for security mechanisms. For instance, Johnston et al. [58] had to modify Nielsen's [105] usability heuristics into what they referred to as HCI-S criteria before using it to analyse and identify usability problems with the interface of an internet connection firewall. HCI-S is defined as:

"the part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security." [58]

Church [109] identified limitations in mechanism usability studies and argued that usability of security systems remains problematic partially as a result of security researchers focusing less on the usability of systems within their social context. He highlighted some of the limitations of mechanism usability studies which are characterised by experiments and tend to be more focused on the correctness of security systems and less on theoretical principles. Accordingly, mechanism studies that have been the mainstay of usable security research are not sufficient for capturing typical usability issues within a social context. Consequently, the incorporation of such findings into the design and development/modification of cybersecurity mechanisms were unsuccessful in making them usable for different categories of users. Both objective and subjective usability measures are thus required to determine the actual desirability and usefulness of these mechanisms to users. While effectiveness and efficiency attributes of usability can be objectively measured with data on time taken to complete tasks, accuracy or error rates, subjective measures involving user perceptions of usefulness, comfortability, risk, etc. requires a predictive model of acceptance for the domain of security [110].

3.3 Predicting Cybersecurity Acceptance

As highlighted in section 3.2, although usability evaluation is critical in determining the proper implementation of security tools, it cannot fully explain and predict actual adoption and usage. Usability which is part of the overall system acceptability focuses on the extent to which the system can be used while acceptability is concerned with how well the system supports the needs and requirements of all stakeholders (see Figure 3.1) [1, 111]. An acceptance model is thus required to explain and predict the acceptability of cybersecurity designs and implementation.

Previous studies have identified useful insights into users' security behaviour by focusing on one or two influential factors from existing cognitive theories such as the Theory of Reasoned Action (TRA) [112], Theory of Planned Behaviour (TPB) [113], Diffusion of Innovation theory [114] and the Protection Motivation Theory (PMT) [115, 116]. This thesis seeks to explore a wider variety of these dimensions by integrating the Technology Acceptance Model (TAM) with PMT to explain and predict individuals' security behaviours. TAM identifies two considerations in an individual's decision to adopt an

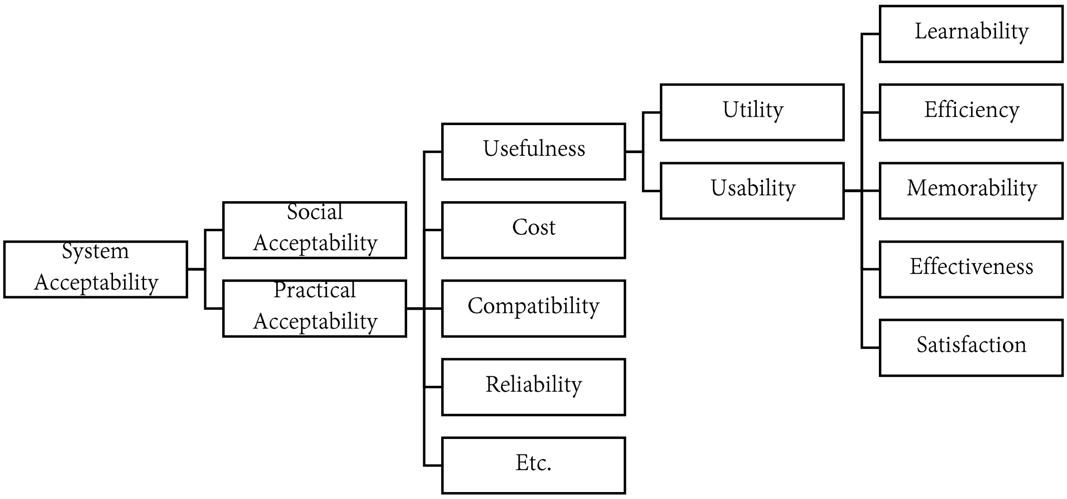


FIGURE 3.1: A composition of the system acceptability attributes [1]

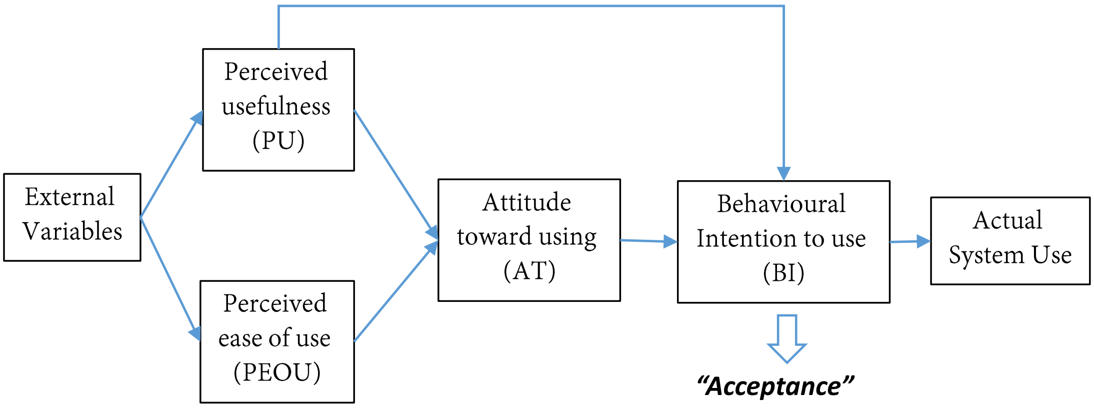

External Variables
Perceived usefulness (PU)
Perceived ease of use (PEOU)
Attitude toward using (AT)
Behavioural Intention to use (BI)
Actual System Use
"Acceptance"

FIGURE 3.2: The Technology Acceptance Model (TAM)

information system: *perceived usefulness* (PU) and *perceived ease of use* (PEOU). Through these, TAM provides a theoretical framework for exploring the effect of external variables on beliefs that are internalised, and their subsequent impact on intentions and actual behaviour (see Figure 3.2). The TAM has been adopted in studying and predicting user acceptance of various forms of technology since its inception. This has led to a substantial amount of theoretical and empirical support being accumulated in its favour and is particularly regarded as being the most robust framework in explaining the adoption behaviours of information technologies (e.g. [117]).

Determinants used to assess the acceptability of technology, however, varies depending on the application domain [118]. The meaning of the TAM constructs as defined in the relevant literature [119] are thus adapted for the context of cybersecurity countermeasures in this thesis. To enable a more thorough examination of security-related behaviour, constructs from the PMT are also considered. PMT which is based on fear

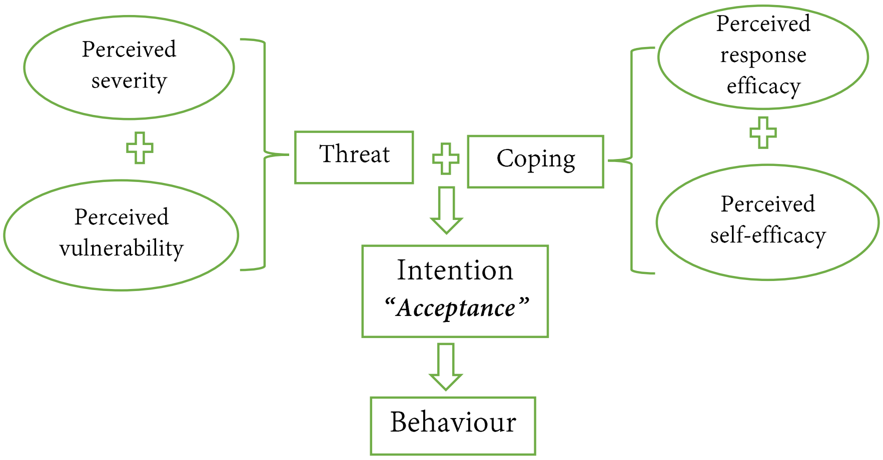


FIGURE 3.3: Flowchart of the PMT model

appeals, offers a relevant background in assessing the causal effect of user's threat perception and security concerns on behaviour. Threat appraisal is a key aspect of the PMT and refers to the beliefs that individuals form about perceived risk when they become aware of security threats [120]. Their perceived risk is then evaluated against the effectiveness of the coping mechanisms that are made available (see Figure 3.3). In order to address cybersecurity issues, the development of user models that can infer more than just the users' level of expertise is a vital requirement. A comprehensive understanding of what influences human behaviour is, therefore, necessary to effectively address the human element of cybersecurity. For instance, Bravo-Lillo et al. [121] attributed the difficulty associated with designing effective security-decision user interfaces to non-compliant behaviours that users have developed over the years.

3.4 Understanding Human Components of Cybersecurity

The need to understand users within any human-computer systems has long been identified as a critical design principle by HCI researchers and professionals. In recent times, computer security researchers have also accented the influences of human behaviour on the usefulness of technical security solutions. [122, 123]. Although Asghar [124] focused on mathematical analysis in his research on human authentication protocols, he admitted that human behaviour needs to be considered to make such protocols more practicable. A plethora of research studies on human information security behaviours exist but are generally within the contexts of specific organisations (e.g. [125–127]). Stanton et al. [126], explored information security behaviours from the perspective of security practitioners and information technology experts through interviews and behaviour ratings. They developed a six-element categorisation of end-user security-related behaviours which when arranged on a two-dimensional map appear to represent different skill levels and motivations that comprise the resultant behaviour.

They realised that security-centred organisations tend to have users with more effective security-related behaviours than other types of organisations. Accordingly, several mechanisms like training and motivation can impact on users information security behaviours. Insight on users and their perceptions are therefore critical to the design and development of effective security solutions targeted at non-expert users.

There is a considerable knowledge gap as far as the understanding of cybersecurity behaviours of individuals are concerned. Most of the studies cited so far mainly utilised survey-based approaches which were targeted at employees of specific organisations. Surveys can be limited in capturing realistic user behaviours since people hardly give an accurate report of their thoughts and actions. For instance, users within an organisation might possess required skills for a desired action but may report a lack of awareness just to avoid being labelled by their colleagues. Consequently, the lack of reliable behavioural data on users' online security actions has become a major challenge to addressing the human component of cybersecurity. Sasse et al. [128] proposed the adoption of behavioural science research findings in addressing notions of cybersecurity such as removing the title of 'weakest link' from the user. Several behavioural studies have shown useful insights into the dynamics of individual's expectations and users' trust perceptions when interacting with technology in general. The challenge that remains is how the design of security systems can draw inferences from such findings.

According to Sasse and Flechais [129], three distinct elements comprise any technical security operating within a social context: product, process and panorama. The product aspect provides the security controls and mechanisms, while the process addresses the security decision making aspects and the panorama perspective deals with the context within which the security is to be operated. Pfleeger and Caputo [123] adopted these three viewpoints of security whiles examining existing theories from behavioural science with the goal of illustrating their potential relevance to cybersecurity. They highlighted and demonstrated possible implications of several models, concepts and heuristics which constitute findings from different areas of behavioural science including, cognitive science, psychology, medicine and many other disciplines. These findings are believed to be relevant to the design, development and implementation of cybersecurity. However, they recognised the difficulty involved in transferring behavioural findings to technological contexts. A multi-disciplinary approach is therefore recommended as the best way of merging behavioural science with the field of computing so as to impact on the usefulness and usability of cybersecurity. Accordingly behavioural science provides a framework to identify and describe individual attitudes towards cybersecurity in general. Computational algorithms can then be applied on relevant cybersecurity behavioural attributes to formulate and implement effective user models for the domain of computer security. Although behavioural science findings are likely to yield useful insights into cybersecurity-related attitudes and behaviours, their applicability and level of impact that can be achieved are yet to be verified.

3.4.1 The Impact of Individual Characteristics on Acceptability

The acceptance and adoption of cybersecurity technologies may vary from one individual to another depending on their distinctive characteristics. Individuals differ in terms of personality, level of experience, cognitive characteristics, background and other demographics. Various aspects of inidvidual differences have been examined in previous research. For instance, Thong et al. [130] examined three individual differences variables (computer self-efficacy, computer experience and domain knowledge) in their digital library user acceptance model. Chau [131] incorporated computer attitude and self-efficacy into the original TAM as external variables affecting perceived usefulness and ease of use. Other studies that examined self-efficacy by integrating it with TAM includes [132–135]. Lu et al. [119] developed a TAM for wireless internet in which they included demographic variables such as age, gender and income as individual differences to be examined. Thong et al. [136] focused on the direct and intermixing effects of individual differences on the acceptance of digital libraries. They found among other factors that individual differences such as self-efficacy, experience and domain knowledge affects perceived ease of use of digital libraries.

Although the topic of individual differences is a long-standing research area in the field of HCI [137], it has not been fully explored within the context of cybersecurity. Dillon and Watson [138] examined previous analyses of users in HCI and concluded that a significant support for generalisation across applications could be gained by relying on more updated findings on individual differences. Chen et al. [139] also reviewed research on individual characteristics within the context of virtual environments. They noted that theories and methodologies developed based on knowledge on individual differences in the past may not be able to fully determine the effects of these differences on the use of newer and emerging virtual technologies. According to Egan [140], differences in system designs and training methods have less impact on performance level when compared to individual differences. This is consistent with Pare and Elam [141] research finding that personal factors have a stronger influence on behaviour than other social and environmental factors when computers are adopted voluntarily. Focusing on knowledge workers, they adopted social psychological frameworks that highlight the importance of attitudes and other socio-cultural elements to assess factors that influences decisions to use personal computers.

The importance of understanding user characteristics and how that impacts on cybersecurity performance cannot be overemphasised. It has become necessary to identify and examine the critical factors that affect individual attitude towards cybersecurity and the relative impact of each factor. An extensive study of the relations between various aspects of individual differences and cybersecurity-related factors is thus required to be part of the process of developing effective models of users. As reviewed in this section, most studies have only considered a limited number of the variables pertaining to individual differences. This thesis project explored a wider variety of these individual characteristics and examined their relative impact on user perceptions, values, and attitudes within the context of cybersecurity. One of the most significant attitudes missing in models describing security behaviour is that towards personal data. The next subsection discusses the role of personal data as an underlying construct for both privacy and digital security.

3.4.2 The Role of Personal Data

There seems to be some controversy surrounding the concepts of security and privacy in terms of what they are or represent. In the corporate world where institutions tend to handle both concepts jointly, the two terms are seen as one and the same. In academia, however, a distinction is usually made between privacy and security due to the peculiarities of the variables and dimensions underlying the two concepts. Security and Privacy have been defined in various ways depending on the context and/or subject domain. More especially privacy has been found to be difficult to define hence there is no universally accepted definition for the concept. Banisar et al. [142] noted that the different perceptions of privacy are widely based on different factors like context and environment. They indicated that privacy has four main aspects which deal with personal data, the physical body, communications and territories. Privacy in terms of personal data is generally referred to as Information Privacy which is the focus point for this research. For instance, Clarke [143] defines privacy as: *"the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations"*. Information privacy, on the other hand, is defined as: *"the interest an individual has in controlling or at least significantly influencing, the handling of data about themselves"* [143]. In the context of digital data and cyberspace, privacy concerns involve unauthorised collection, distribution and misuse of personal data.

Security in the digital world, however, is concerned with three main goals, namely: confidentiality, integrity and availability which is commonly referred to by the acronym "CIA". According to Schneier [89], the confidentiality aspect of security has to do with privacy. Thus using security controls to prevent unauthorised access to sensitive data. However, security concerns generally go beyond privacy to include data corruption or loss and denial of services to computing resources. For instance, a virus infection may not necessarily lead to unauthorised collection and use of personal data but can cause severe damage to a computer system. Privacy is too often viewed as a purely legal issue while security is usually considered as mainly a technical issue as upheld by these articles [25, 144, 145]. Others have emphasised the importance of treating security as a process involving policies, strategies and security controls rather than just a technical product [88–91]. Likewise, privacy can be achieved through either legal and regulatory measures that mandate opt in and opt out choices or technical solutions that enable users to enforce their privacy preferences [146].

There is however no doubt that the concept of security and privacy are strongly related. A common factor underlying the dimensions of these two concepts is personal data [147]. Information privacy which has become one of the most vital aspects of privacy is concerned with protecting the personal data of individuals. However, the range of potential implications in relation to the collection and sharing of personal data goes beyond the issue of privacy and includes constructs related to security, risk and benefits. Although personal data has been recognized as a key issue within the HCI community, there are comparatively few studies exploring individuals' attitudes towards personal data.

Iachello and Hong [148] review several privacy-related literature within the context of HCI and identified the need for a deeper understanding of individual's attitudes towards the phenomena as a major challenge. Ackerman and Cranor [149] also acknowledge the fact that different aspects of privacy pose a big challenge for the design of usable systems. Essentially the available information is insufficient to guide stakeholders including new technology and interface designers in dealing with or addressing issues related to personal data. Thus designers and engineers need to understand social issues regarding personal data in order to develop systems that can adequately support values that constitute acceptable social behaviours. Examining the construct of personal data and how it is perceived by people has therefore been identified in this thesis as a critical component in understanding and predicting people's attitude towards cybersecurity.

3.5 Proposed Causal Model For Cybersecurity Behaviour

This section summarises and presents the causal model emerging from the review of literature focusing on the human aspect of security. As shown in Figure 3.4, the proposed model is based primarily on the TAM discussed in Section 3.3 above. In the model, user acceptance is examined by two cybersecurity behaviours — intention to use and actual usage. According to TAM, PU and PEOU are the primary determinants that determines the intention to use and subsequent usage behaviour. PMT, on the other hand, measures the components of a fear appeal in determining the variables that impact on protection motivation in the form of behavioural intentions. This thesis adopts TAM as a core theoretical foundation and extends it with PMT's cognitive mediation processes of threat and coping appraisal to develop a predictive model for cybersecurity. The model is further augmented with two additional user insights related to personalized digital security as primary determinants to empirically assess and predict user's cybersecurity behaviours. These are Value for Personalization (VFP) and Attitude to Personal Data (APD).

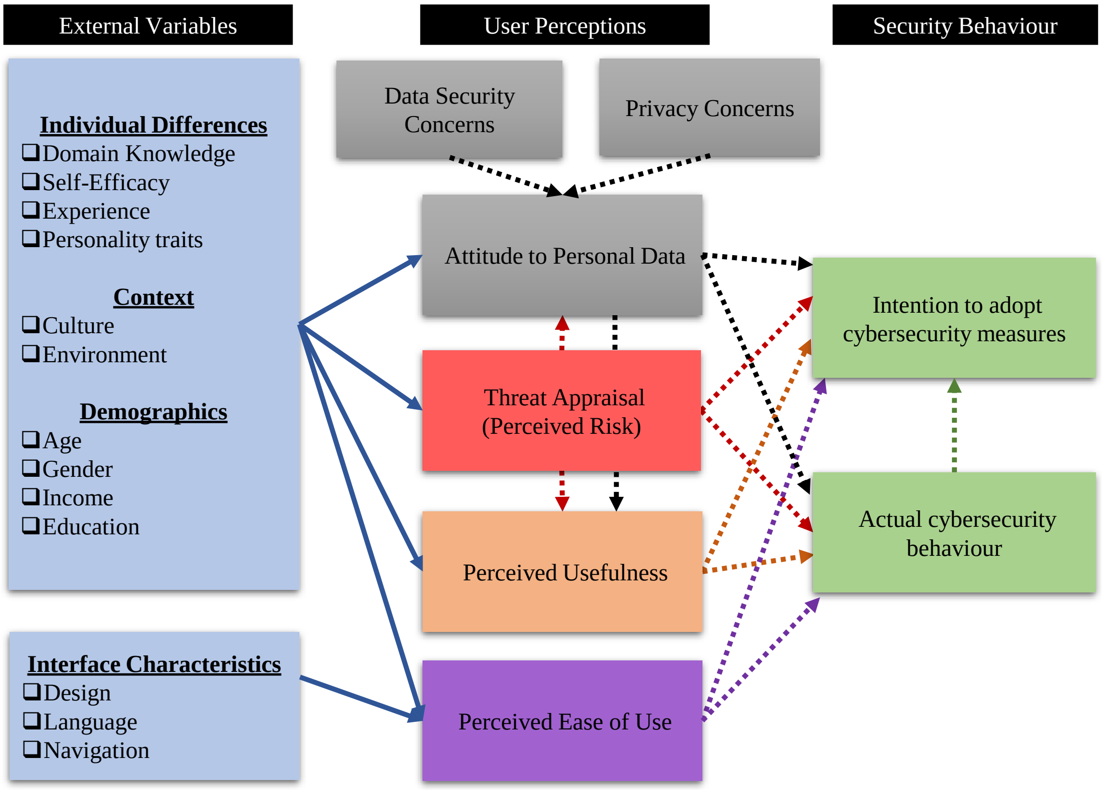


FIGURE 3.4: Proposed Causal Model

The research model is built around all the external variables identified as possible factors influencing PEOU, PU, and perceived risk (PR) of technology in general. The research thus explores variables like the context of use and user demographics such as age, gender, and/or education and their influence on people's attitude towards cybersecurity mechanisms. Other than *attitude to personal data* (APD), all the constructs in the model are adapted from previous behavioural models used in various different fields, including psychology and HCI. APD here refers to the value people place on their data, and their tendency to adopt measures to protect it. Because APD is a common factor underlying the constructs of both security and privacy, we have theorised that personal data and how it is perceived by individuals, influences security-related behaviour. As such, individual's perceptions and attitude to personal data are hypothesised to have an effect on the adoption and acceptance of cybersecurity tools.

3.6 Research Design

This thesis is grounded in design research and was conducted in three main phases as depicted in Figure 3.6. Design research was first introduced in the educational design literature for new innovation in the field to be based on prior research findings [150]. In recent years, more and more researchers are adopting the approach for the testing and refinement of various aspects of Information Systems (IS) including algorithms, computer interfaces, system designs, user models etc. [151, 152]. Design research thus encompasses different techniques and procedures from a variety of disciplines including Engineering and Computer Science. The design science framework itself is characterised by three main distinct but interdependent research cycles namely; *relevance, design and rigour* [2, 152] (see Figure 3.5). Accordingly, the relevance cycle involves the requirement elicitation process through field testing and evaluation. The design cycle involves an iterative research process of building and fully evaluating the design product for the appropriate environment (relevance cycle). The knowledge discovery from the design cycle is then released into the rigour cycle as an addition to the existing knowledge base.

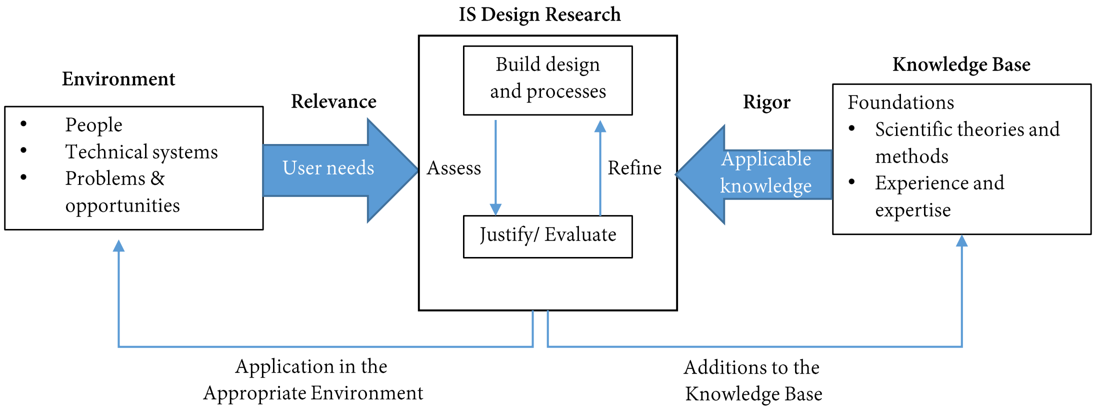


FIGURE 3.5: Design science research cycle for information systems [2]

Phase one of the thesis thus consisted of a user study conducted to identify usability problems and elicit requirement towards the design and development of more effective cybersecurity tools for non-expert internet users. Phase two of the thesis was in two parts. Following the identification of critical cybersecurity behavioural factors from the extant literature review, the first part of phase two involved the development of a measurement instrument for the construct of personal data. As this thesis identified and introduced APD as a key determinant of cybersecurity behaviour, a measurement instrument is required in order to successfully incorporate it into existing behavioural models. This then provides a novel framework to best examine and predict attitudes towards cybersecurity. The second part of phase two evaluates the proposed causal model in its entirety through user survey and predictive modelling. The findings from phase one and two are then used to formulate a machine learning framework for personalized adaptive cybersecurity for the design and evaluation cycle in phase three.

3.7 Chapter Summary

The underlying background of this thesis is presented in Chapter 2 and Chapter 3. An overview of the research model and methodology is provided in this chapter. The

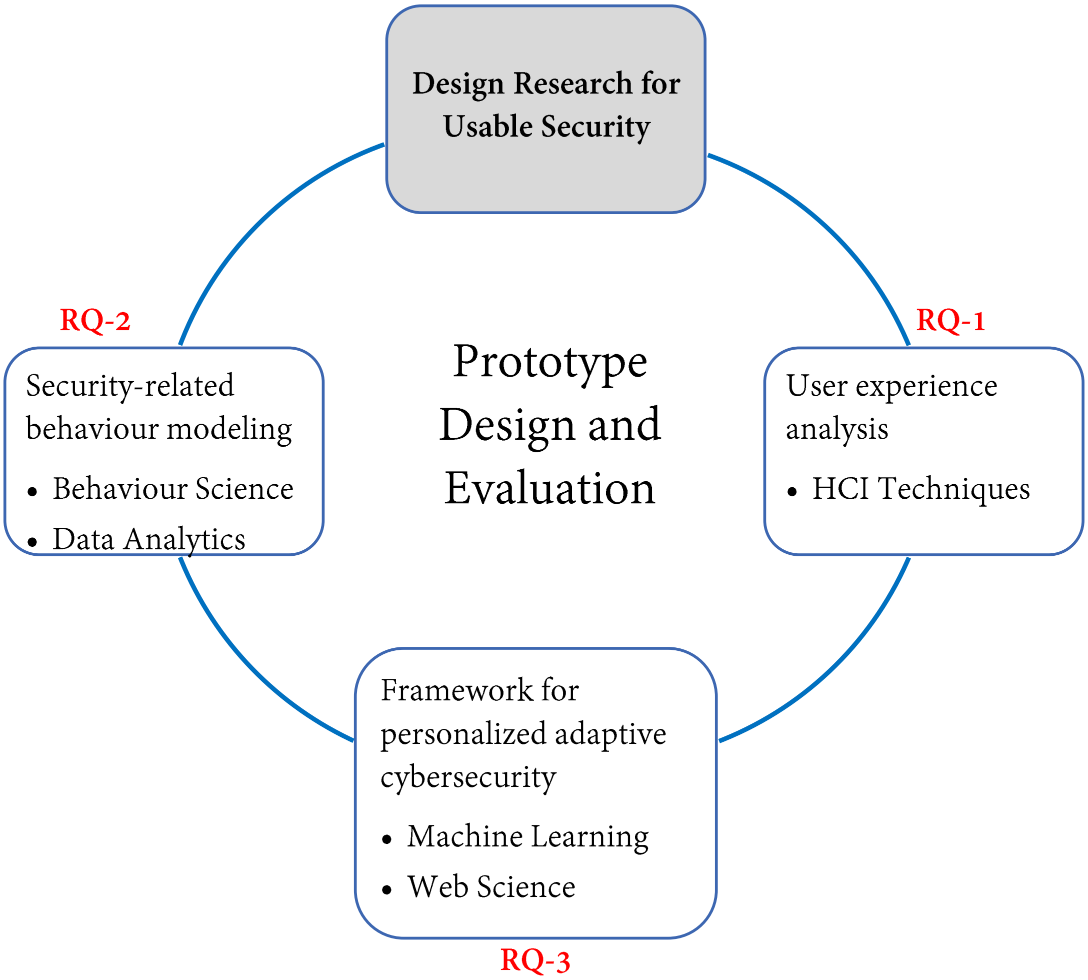

Design Research for Usable Security
RQ-2
Security-related behaviour modeling
• Behaviour Science
• Data Analytics
Prototype Design and Evaluation
RQ-1
User experience analysis
• HCI Techniques
Framework for personalized adaptive cybersecurity
• Machine Learning
• Web Science
RQ-3

FIGURE 3.6: Conceptual Framework linking the different facets of the research

proofs of concepts are presented in the following chapters, further investigating factors influencing user's protection behaviour and how that can be leveraged to address cybersecurity usability and acceptability issues. To achieve *rigour* for the design research cycle, various specific aspects of background literature are provided throughout the thesis chapters properly grounding the research in prevailing theories and methodologies. As shown in Figure 3.6, the research draws on theories and techniques from multi-disciplines subsequently making contributions that add to the existing Cybersecurity and HCI knowledge base.

CHAPTER 4

User Experience Analysis for Usable Cybersecurity Requirements

Contents

4.1 Introduction

The web browser is application software used to retrieve, transmit and present digital information resources on the web [79]. It is thus a ubiquitous application for client access to internet products and services. Nowadays, personal computers come with pre-installed applications including web browsers such as Microsoft IE, Apple Safari etc. Other browsers like Google Chrome, Qihoo 360, Mozilla Firefox, Tencent QQ etc. are usually downloaded and installed by the users themselves as a matter of preference. As an application that can be used to access the internet, it also serves as an entry point to the device on which it is installed. Features like ActiveX, Cookies, and JavaScripts used by browsers to improve the browsing experience for users do come with some security risks. Cybercriminals often exploit these web browser features to gain access to computers connected to the internet for various forms of security and privacy breaches.

Most web browsers, however, come with inbuilt security features that need to be optimized for safe internet browsing. When users fail to correctly configure their browsers, whether pre-installed or installed by themselves, they put themselves at a higher risk for various forms of cyber attacks. Nevertheless, users often fail to optimize the security settings of their preferred browsers, mostly leaving them in their default state. Although browsers are one of the most frequently used application on personal computers, their security and privacy features seem to be largely ignored by most home computer users. It appears that web browser security features are not exempted from the general notion of cumbersomeness often associated with security configurations by most novice computer users as underscored by the usable security literature [50, 79]. Given the range of threats facing internet users today, it is crucial that they are enabled to configure their web browsers securely to make them less vulnerable to malicious attacks. A first step towards this goal is to evaluate these features in existing web browsers with typical non-expert users.

This chapter describes a user study practically conducted to evaluate the usability of the inbuilt security features for three popular web browsers. The results of the within-subjects empirical usability study are presented and discussed. The study aimed to achieve three main goals:

1. Discover specific usability problems with web browser security interfaces and interactions in general. This is determined by observing participants' ability/inability to accomplish specific security tasks and error rates.

2. Explore which security user interface design users prefer. To determine which web browser's security interface has the best overall usability, the System Usability Scale (SUS) is adopted. Participants are required to complete the SUS after using each browser for all study tasks. This is used to compute and compare the overall usability score of the three web browsers.

3. Gather possible new user requirement for web browser security functionalities. In the study, participants use all three web browsers with distinct interfaces and provide feedback describing what they like and what they wish was different or available.

4.2 Assessing Usable Security

While usability testing is well established, far too little attention has been paid to the usability of cybersecurity from the HCI community. The National Research Council [146] calls for more usable security research highlighting the need to ensure the security and privacy of information systems with user-centred security designs. Standard software usability testing involves observation of a primary task being performed towards a primary goal with the specific application being evaluated [153]. Users encounter various security applications (e.g. password, encryption, anti-phishing) within cyberspace but security concerns may not be a top priority while performing their primary tasks (e.g. banking, shopping, entertainment etc.). Although a secure experience is desired, security is a secondary goal for most computer users. It is therefore important that the experimental tasks presented to participants are made realistic by associating them with possible primary goals. Several usable security research has highlighted the need to create more realistic contexts for completing security tasks when applying available usability testing techniques to best support experimental validity [154]. Situated usability testing (SUT) allows the researcher to evaluate the usability of a security mechanism involving secondary tasks in the context of the users performing a primary task. For this study, scenarios are used to create a SUT condition that presented participants with primary tasks other than security to attend to but requires them to optimise their web browser security settings.

4.3 Study Methodology

The aim of this study is to investigate the usability challenges surrounding web browser security settings. To do this, we first identified three most popular web browsers in windows platforms (desktops and laptops). At the time this study was conducted, statistics compiled using StatCounter.com [155], a web analytics service, showed Google Chrome (GC) as having the biggest desktop browser market share worldwide. Another global statistics compiled on desktop browser usage in 2015 and 2016 confirmed GC as being the most used web browser in the world followed by Firefox (FF) and then Internet Explorer (IE) [156] – see Figure 4.1.

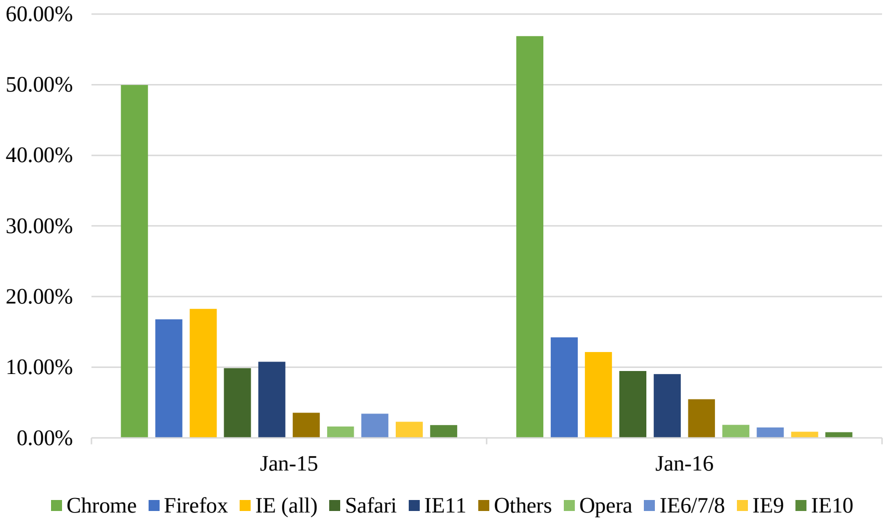


FIGURE 4.1: Worldwide Desktop & Tablet Browser Statistics for 2015 and 2016

Since the study was conducted in China with both Chinese and foreign participants, their browser usage trend was also compiled and again GC emerged as the most popular in terms of the total number of web page viewed with desktop browsers (Figure 4.2). This trend was however quite new in China at the time. According to data from Baidu in August 2014, Microsoft IE with a market share of 47.62% ranked 1st among the top 6 web browsers in China by total reach which included Chrome, Sougou, Cheetah, QQ Browser and 2345. IE was also among the top three internet browsers together with Qihoo 360 browser and Chrome in another 2014 data set from CNZZ (owned by Alibaba Group)[1]. Hackworth [29] indicated that most malware authors targeted IE and other Microsoft applications to produce a greater Return on Investment (ROI) due to its popularity. This, together with usability issues could be a contributing factor for its decreasing adoption rate.

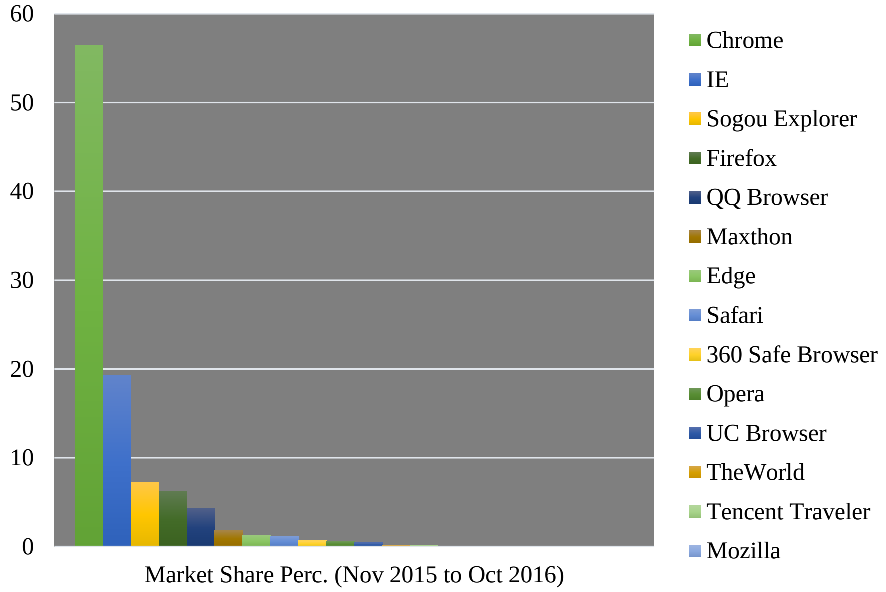


FIGURE 4.2: Top 10 desktop browsers in China as at Oct. 2016

Based on the results from the survey and existing statistics on the most used web browsers (see Figure 4.1 and 4.2), the study focused on using Google Chrome (Released in 2016 and updated on November 20, 2016), Firefox (Version 47.0.2, Released on November 1, 2016) and Internet Explorer (IE 11, updated on August 9, 2016) to conduct the study (Appendix A provide screenshots of the three browser's main settings page). The study design is described in the ensuing subsections with respect to the data collection approach and the basis for the study methodology.

4.3.1 Study Overview

The protocol analysis methodology is combined with observation and the SUS in a SUT to evaluate the usability of the three commonly used web browser's security settings (GC, IE and FF). The primary goal is to identify underlying usability issues as well

[1] http://www.cnzz.com/o_index.php?lang=zh_CN

as merits of specific interface attributes prefered by users allowing us to propose design recommendations for future web browser security interface and user interactions. In reviewing existing work on usable security, it has become very clear that several security labs and research studies have yielded valuable insights into user's security behaviour over the past decade. A major gap, however, is lack of studies that reflect users' actual security behaviour (e.g. have they optimised the security settings of their own personal computer?) within specific contexts.

To better understand users' web browsing security behaviour, it was deemed necessary to inspect study participants' actual browser security settings. Gathering real web browser security settings dataset on users' personal computers/laptops could help in measuring the impact of actual security behaviours exhibited by users on the security state of their personal computers. To this effect, in addition to the SUT adopted for this study, physical inspection of participants' browser security settings was carried out to better compare users' behavioural intentions and actual security behaviours. During the inspection, participants were interviewed on their motivation for choosing specific security configurations after accessing whether or not the said settings adequately meet their security/privacy goals.

4.3.2 The Experimental Set-up

The usability testing was conducted at the University of Nottingham, Ningbo China campus and the methodology was reviewed and approved by the university's ethics committee. Two Windows 8 laptops with a webcam and a microphone were set up in a room specifically booked for the experiment. A usability software tool (Morae)[2] was used to record, observe and collate data for the user study. The Morae program consists of three main components (Recorder, Observer and Manager) that allow for a smooth integration of the usability testing stages right from set-up to data analysis. The recorder component was installed on the designated laptop for the experiment to record participants' interactions while performing the study tasks. Thus Morae served as a screen capture/recording tool to aid in collecting data on how users navigate the various interfaces as well as their thought as they were being prompted to think aloud whiles performing each task. The three web browsers were also installed on the experimental laptop in their default state (i.e. no prior changes were made to the browser settings). The study explicitly focused on the security settings' interfaces of the three web browsers. Morae Observer and Manager were both installed on the study coordinators' laptop that allowed them to remotely observe the study, collaborate and take notes all in real-time. The types of data captured with the Morae program during a study session include on-screen activity, keyboard/mouse clicks, text notes, as well

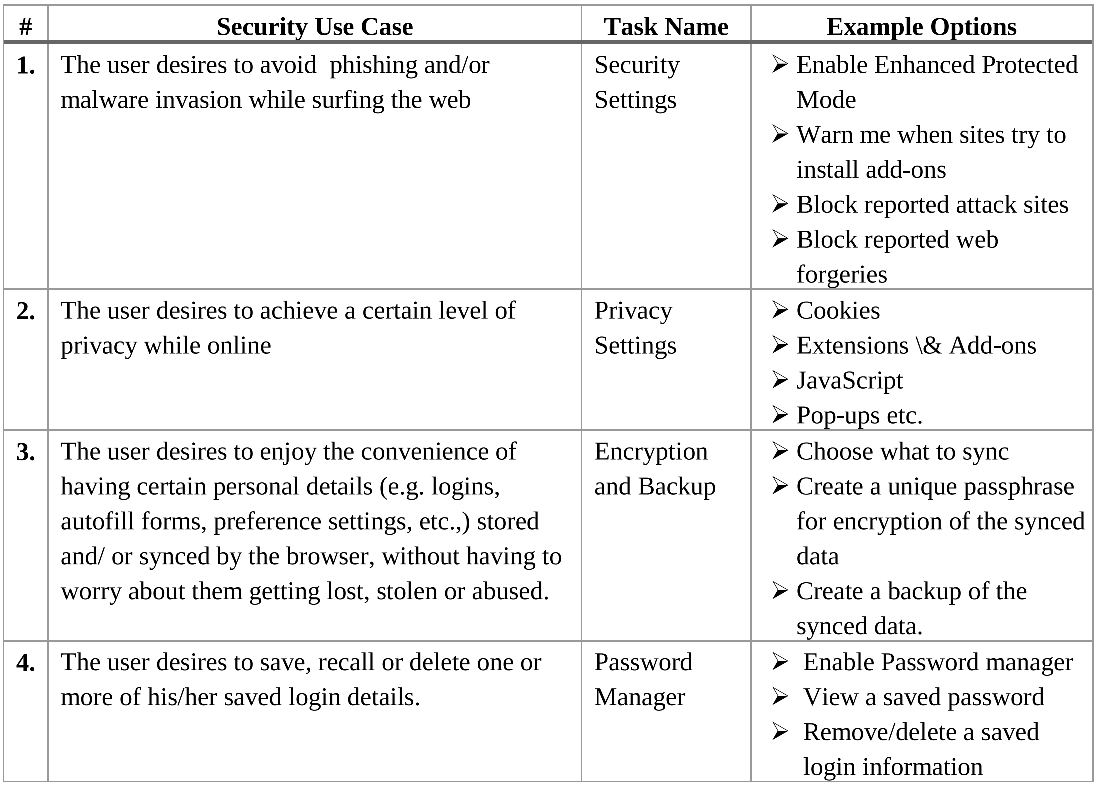
[2] https://www.techsmith.com/morae.html

as audio and videos. For the purposes of the usability evaluation, each browser was evaluated in its default configuration on Windows 8.

4.3.2.1 Scenario and Task Design

During the study, participants were presented with four different scenarios regarding the level of security/privacy desired for specific primary goals requiring a web browser. Each scenario was paired with specific web browser security configuration tasks to form four different security cases on the participants' task sheet. Table 4.1 presents a summary of the security cases used to describe the user interaction scenarios required to achieve browser security and privacy goals. The four security cases used for this study were thus based on the typical security functionalities of a web browser that a user ought to optimise. For the observer's task sheet, the corresponding steps that users are required to follow in performing each specific task are also outlined (see Appendix B). This enabled the evaluator to observe what users were struggling with and what they are clearly doing differently. The set of tasks with their corresponding scenarios were repeatedly presented one at a time by the recorder so that each participant completed them with all three web browsers.

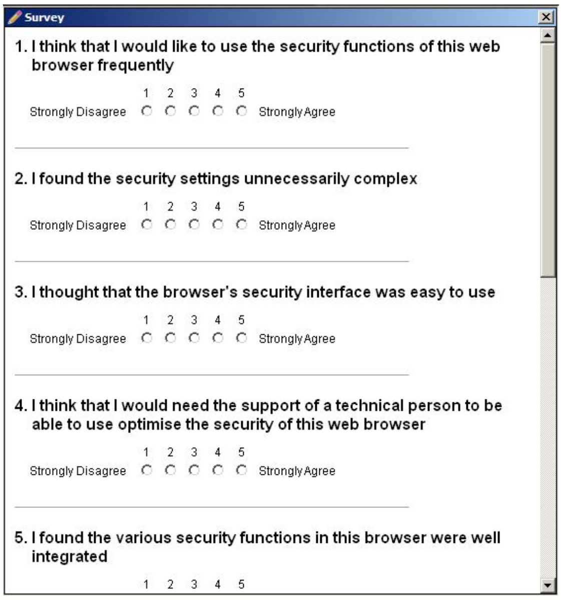
TABLE 4.1: Summary of the 4 security use cases and related tasks



#	Security Use Case	Task Name	Example Options
1.	The user desires to avoid phishing and/or malware invasion while surfing the web	Security Settings	➢ Enable Enhanced Protected Mode ➢ Warn me when sites try to install add-ons ➢ Block reported attack sites ➢ Block reported web forgeries
2.	The user desires to achieve a certain level of privacy while online	Privacy Settings	➢ Cookies ➢ Extensions \& Add-ons ➢ JavaScript ➢ Pop-ups etc.
3.	The user desires to enjoy the convenience of having certain personal details (e.g. logins, autofill forms, preference settings, etc.,) stored and/ or synced by the browser, without having to worry about them getting lost, stolen or abused.	Encryption and Backup	➢ Choose what to sync ➢ Create a unique passphrase for encryption of the synced data ➢ Create a backup of the synced data.
4.	The user desires to save, recall or delete one or more of his/her saved login details.	Password Manager	➢ Enable Password manager ➢ View a saved password ➢ Remove/delete a saved login information

4.3.2.2 Survey

The survey for the study was divided into two which were both administered using the recorder. The first consists of a set of demographic questions which participants were required to answer before they are presented with the study tasks. The second part of the questionnaire was administered to participants immediately after using a web browser to complete the set of study tasks. It consisted of the ten SUS questions adapted from Brooke et al. [157], Brooke [158] — see Figure 4.3). The SUS survey was used to elicit partcipants' feedback on their satisfaction with the web browsers' security settings.



1. I think that I would like to use the security functions of this web browser frequently

Strongly Disagree 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ Strongly Agree

2. I found the security settings unnecessarily complex

Strongly Disagree 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ Strongly Agree

3. I thought that the browser's security interface was easy to use

Strongly Disagree 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ Strongly Agree

4. I think that I would need the support of a technical person to be able to use optimise the security of this web browser

Strongly Disagree 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ Strongly Agree

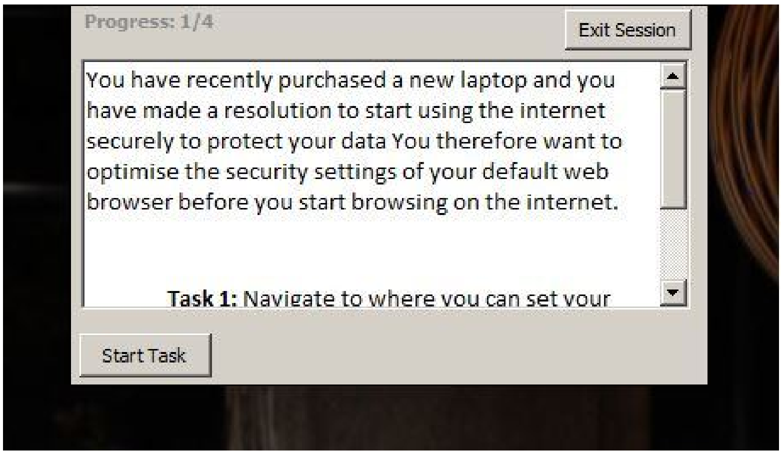
5. I found the various security functions in this browser were well integrated

1 2 3 4 5

FIGURE 4.3: Screenshot of the SUS questions presented by Morae

4.3.3 Procedure

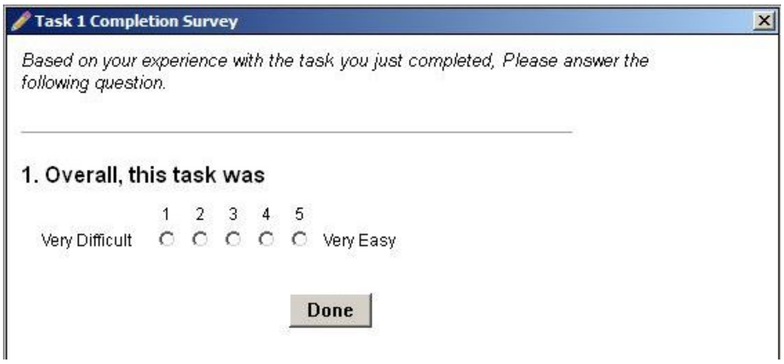
Participants were welcomed to the usability laboratory and issued with the study information sheet outlining the purpose of the usability study. They were given time to read through the information sheet before signing the consent form. Once the necessary consent forms were completed, a verbal explanation of the experimental procedures was given. The Morae program then presents the demographic data survey for participants to complete before allowing them to start the study tasks. Participants were asked to "think-aloud" at the beginning of the session. A neutral demonstration of thinking aloud while signing into the laptop is provided in accordance with the think-aloud protocol. Once the survey is completed, the tasks are presented to the participant on the screen one at a time. Participants were asked to complete them in the order presented. To ensure that participants understood the requirement for the task, they were required to click the start button before attempting the task (see Figure 4.4). This also signals the recorder to start timing the duration for completing the task. The stop button on the task instruction screen also needs to be clicked at the end of each task. The completion of each task is followed by a task difficulty level statement to collect participants ratings of the task with respect to the task environment (browser type) (Figure 4.5).



You have recently purchased a new laptop and you have made a resolution to start using the internet securely to protect your data You therefore want to optimise the security settings of your default web browser before you start browsing on the internet.

Task 1: Navigate to where you can set your

FIGURE 4.4: Screenshot A Task Instruction Screen



Based on your experience with the task you just completed, Please answer the following question.

1. Overall, this task was

Very Difficult 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ Very Easy

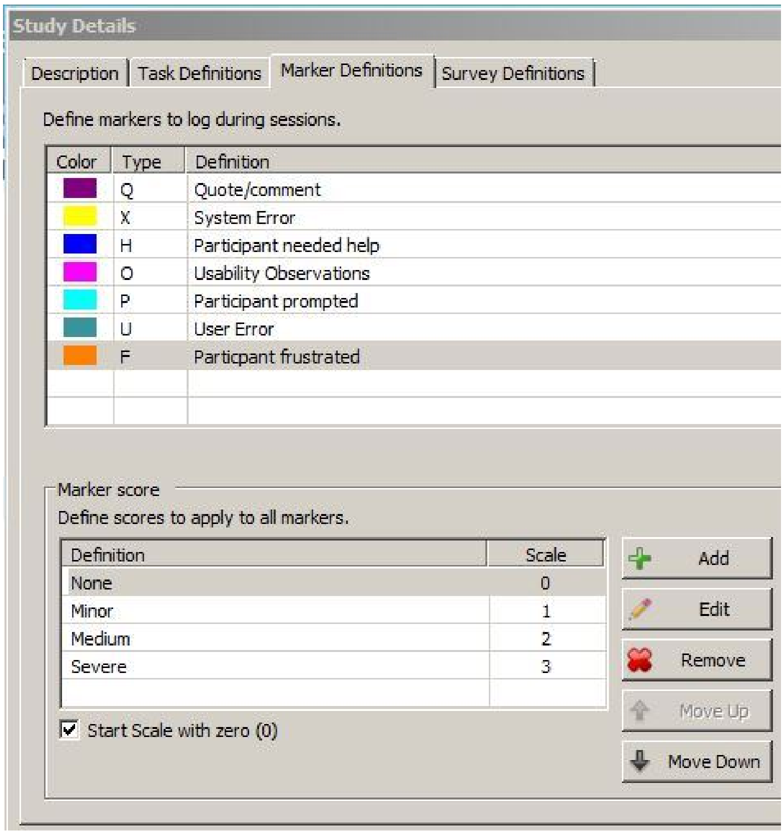
FIGURE 4.5: Screenshot of The Task Difficulty Likert-scale Statement

An evaluator sits behind the observer laptop opposite the participants, occasionally prompting them to keep talking. Apart from reminders to keep talking, other types of interventions were used to gather explanations about participants actions, expressions and experiences. The interventions used were adopted from the ten intervention types and corresponding triggers developed by [159] based on the think-aloud literature. For instance, a dissatisfaction expressed by the participant would trigger a user expectation enquiry intervention (e.g. "what were you expecting to happen?") from the evaluator. Suggestion intervention triggers such as "What would you suggest to make it more visible?" were used to solicit suggestions from participants who express negative feelings or disapproval for specific aspects of the browser's security component. The evaluator stayed with each participant throughout the session but remained neutral by cordially declining to provide further instructions to participants asking for help. In such cases, they were reminded about the goal of the study to test the usability of the given web browser by observing how they accomplish the specified task without outside help. Participants were however encouraged to take whatever steps they normally would, to solve similar computing problems if they got stuck with any of the task.

After completion of the tasks outlined in all four security use cases and survey questions for the three web browsers, participants were interviewed briefly on their views on web browser security settings. Semi-structured questions were used to elicit their opinions on what they think an ideal web browser security interface should look like and which aspects of web browser security component they would like to be automated.

4.3.4 Data Collection

The study ran for two weeks. The usability program installed on the laptop recorded video of participants while they interacted directly with each web browser's security interface to complete the specified tasks. With the aid of Morae, the evaluator recorded observations on participants' actions throughout the sessions logging any obvious misunderstandings about the security components, any frustrations and whether they succeeded in completing the task. These were done with pre-configured markers encoded into the program as part of the study set-up (Figure 4.6).



Define markers to log during sessions.

Color	Type	Definition
🟪	Q	Quote/comment
🟨	X	System Error
🟦	H	Participant needed help
🟪	O	Usability Observations
🟦	P	Participant prompted
🟦	U	User Error
🟧	F	Particpant frustrated

Marker score

Define scores to apply to all markers.

Definition	Scale
None	0
Minor	1
Medium	2
Severe	3

☑ Start Scale with zero (0)

FIGURE 4.6: Marker And Score Definitions Used for Logging

The success level of each task was recorded by the evaluator using the following possible outcomes:

Completed with ease: The task was successfully completed without any difficulty.

Completed with difficulty: The participant struggled but eventually completed the task after several attempts.

Failed to complete: The participant tried but gave up without completing the task.

False Completion: The participant did not complete the task or made mistakes but

falsely claimed a successful completion.
All the outcomes were considered for usability problem analysis in terms of time taken and error rates. The fourth outcome is quite dangerous as it gives the user a false sense of privacy and security online.

The Morae program was also used to immediately transcribe some of the things participants said while thinking aloud and performing the study tasks which were labelled as quotes/comments. The video recordings of all the usability testing sessions were later transcribed verbatim. This was done using the Manager component of the Morae software. The transcribed data was then exported into an Excel spreadsheet for coding along with those generated by the Observer during the testing sessions.

4.3.5 Data Analysis

The data was analysed both qualitatively and quantitatively using inferential and descriptive statistical methods to determine usability issues as well as effective features of security interfaces. The three main usability metrics discussed in Chapter 3: *effectiveness*, *efficiency* and *satisfaction* defined by ANSI/ISO [160, 161] informed the overall analysis. Dependent variables such as task time, completion and error rates were used to measure the effectiveness and efficiency. Satisfaction, on the other hand, was measured based on participants feedback through the think-aloud protocol and the SUS survey. Specifically, statistical analysis was conducted on the security use cases and individual task time metrics, as well as the error counts, to determine which of the security interface designs were more effective. Individual task time and error counts were compared to the entire sample population to identify significant trends that may be specific to users with similar demographic characteristics. Consequently, the performance metrics of task time, error count, and satisfaction score were analysed together with the qualitative data gathered to assess possible design guidelines for personalized adaptive cybersecurity.

4.4 Results

This section presents the results along with descriptions of the types of analysis performed on the data collected.

4.4.1 Participants' Profile

To allow for cross-cultural comparison, only Chinese and British who were mostly university students and staff from a variety of faculties were allowed to take part in the study. Consequently, twenty individuals (10 Chinese and 10 British citizens) who are typical users of the three web browsers identified, were recruited as study participants. A few had technical backgrounds, two were Computer Science undergraduate students but none of the participants had specialization in computer/information security. Of the 20 participants, 11 were males (55%) and nine females (45%). The gender difference of two participants is insignificant and should not affect the study's analysis of gender-specific factors related to usable security. Participants skewed towards 25 – 34 years old $(12; 60\%)$ while 25% were 18 – 24 years old, and 15% were 35 – 44 years old. The majority of the participants had post-graduate degree (9), seven (7) of them had bachelor's degree and few had either high school diploma (2) or were in college (2).

Majority of the participants self-rated their general computer and cybersecurity competency level at 2 or higher on a scale of 1 to 5. Both the computer and cybersecurity competency ratings were categorised into 3 levels of low (1), medium (2–3) and high (4–5). Similarities were found between self-reported competency levels for both computer and cybersecurity whereby a large proportion of the participants are categorised as having a medium level of knowledge. Only one individual reported having a low computer competency level and two individual rated their cybersecurity familiarity as low (Figure 4.7). Shapiro Wilk's test and a visual inspection of their histograms, normal Q-Q and box plots showed that the self-reported ratings for cybersecurity experience were not always normally distributed across the various demographic groups. Since the sample size is not big enough to ignore the normality distribution assumption of a t-test, a Mann-Whitney U Test was used to test all variables when comparing two independent samples.

From this data, it can be concluded that self-reported expertise level in the female group was statistically significantly higher than the male group $(U = 19.5, p < 0.05)$. The test however, revealed no significant difference existed between males and females self-reported computer expertise levels $(U = 32.0, p > 0.05)$. As shown in Table 4.2, no significant differences were found among the two groups of nationalities' self-reported expertise levels either. Multiple comparisons were not performed for age group and education level demographic variables because the overall test (Independent-Samples Kruskal-Wallis Test) did not indicate significant differences across these samples.

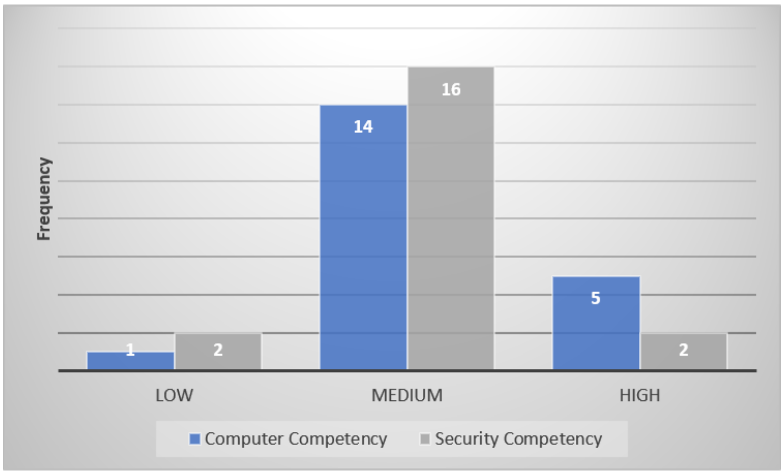


FIGURE 4.7: Computer and Security Competency Level Reported (n=20)

TABLE 4.2: Mann-Whitney U Test results for differences between gender and nationality group on self-reported competencies

Variables		N	Mean Rank	Sum of Ranks	U	Asymp. Sig. (2-tailed)	Exact Sig. [2*(1-tailed Sig.)]
Cybersecurity experience	Female	9	13.83	124.50	19.5	0.015	0.02
	Male	11	7.77	85.50			
	Total	20					
Computer Skill level	Female	9	12.44	112.00	32.0	0.161	0.201
	Male	11	8.91	98.00			
	Total	20					
Cybersecurity experience	British	10	9.70	97.00	42	0.517	0.579
	Chinese	10	11.30	113.00			
	Total	20					
Computer Skill level	British	10	11.90	119.00	36	0.265	0.315
	Chinese	10	9.10	91.00			
	Total	20					

4.4.2 Effectiveness, Efficiency and Demographic Metrics

The study produced quantifiable data to objectively measure and evaluate the usability of security functionalities built into web browsers. Two main objects characterised the analysis conducted on the quantifiable data generated from the study. One of the objectives is to compare the usability of the three web browsers' security interfaces to determine which interface was most effective and efficient. The other objective is to investigate which demographic characteristics impacted on individual usability expectations.

4.4.2.1 Task Success Rate by Browser

According to the metrics defined by ANSI/ISO, completion and error rates constitute measures of effectiveness. As shown in Figure 4.8, most participants were able to complete at least 2 out of the 4 core security case tasks. Figure 4.9 illustrates the completion task rate achieved for each of the three browsers. It can be noted that the major drop-out occurred in task 3 (back-up and encryption). The main challenge observed with this task was that participants struggled to locate the configuration page where they could control the back-up settings. This was mostly due to their unmatched mental models with the system. For instance, some participants who wanted to do this on GC, chose to search for backup or encryption with the search box rather than going into the sync settings.

4.4.2.2 User and System Error logs

A related samples Friedman's Two-Way Analysis of Variance by Ranks indicates a significant difference in the distribution of error counts by task across the three web

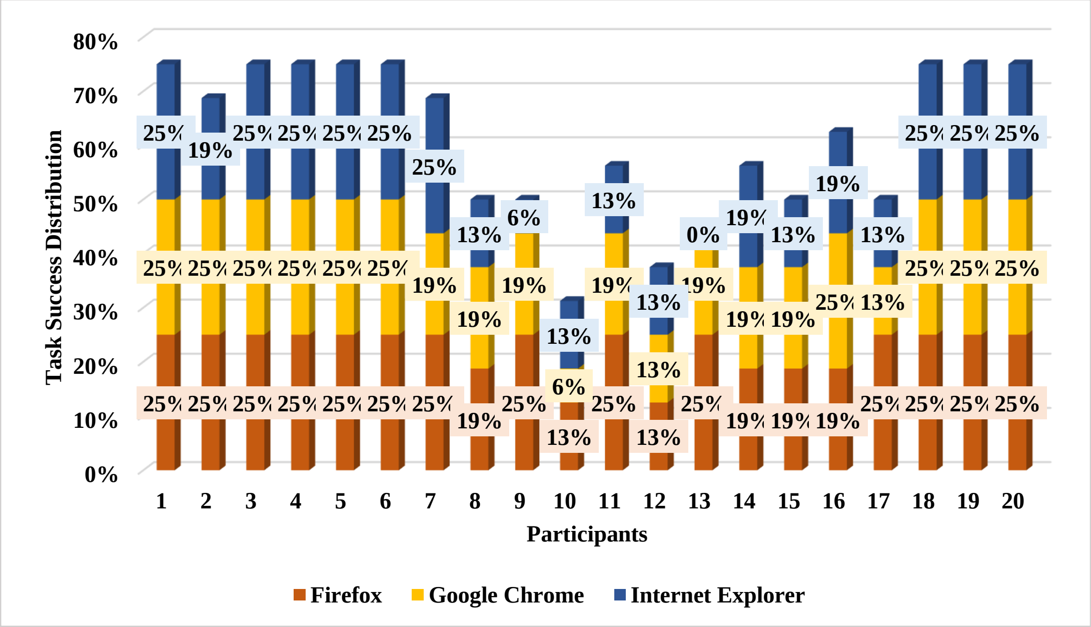


FIGURE 4.8: Overall Task Success Distribution by Participants

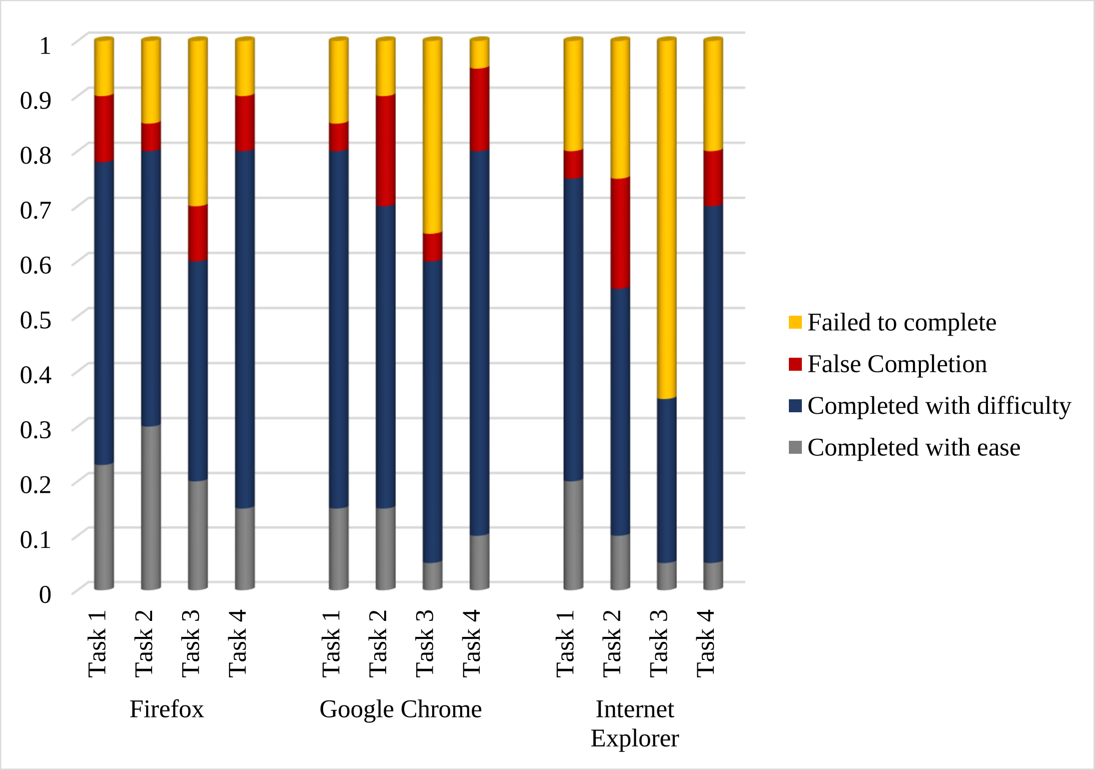
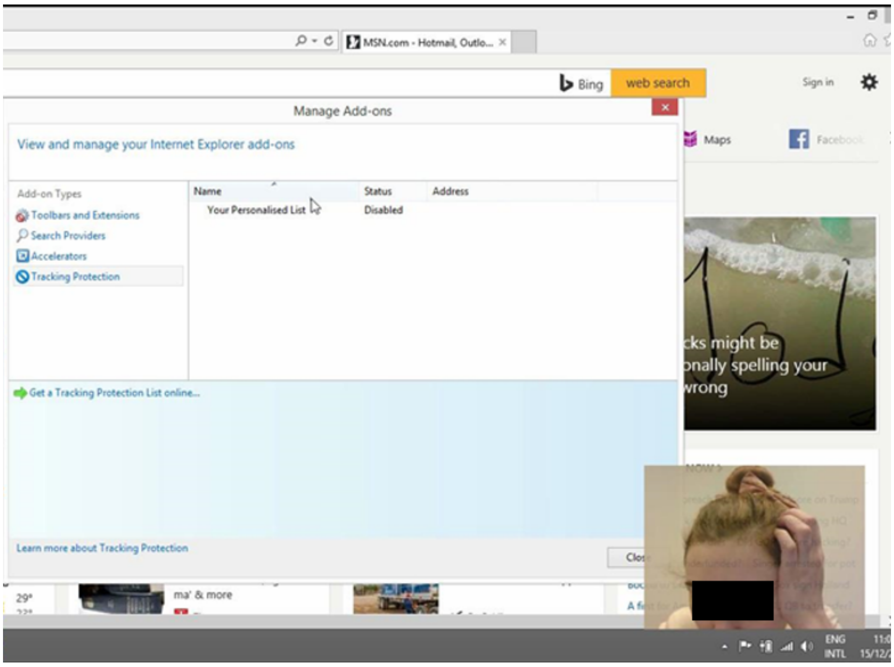


FIGURE 4.9: Task Completion Rate By Browsers

browsers $\chi^2(11) = 23.356, p = 0.008$. The error count was consistently high on cybersecurity case task 4 - password manager, with a recorded error count of 14, 15 and 18 for FF, GC and IE respectively (see Table 4.3). IE appeared to have logged a significantly higher number of errors on all four cybersecurity case tasks. The most common error log had to do with participants mistaking content settings for protection against malicious programs.

TABLE 4.3: Error Count for the cybersecurity case tasks by web browsers

Browser		**EC_T1**	**EC_T2**	**EC_T3**	**EC_T4**
	N	20	20	20	20
Firefox	Sum	4	6	3	14
Google Chrome	Sum	6	2	8	15
Internet Explorer	Sum	10	7	6	18
Total	N	60	60	60	60
	Sum	20	15	17	47
	Mean	7	5	6	16
	Std. Deviation	0.729	0.541	0.715	1.059


[redacted]

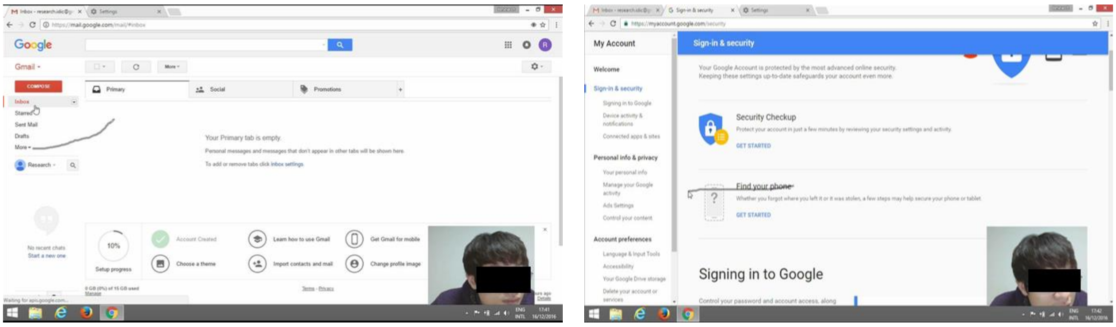
Manage Add-ons

View and manage your Internet Explorer add-ons

Name	Status	Address
Your Personalised List	Disabled	

FIGURE 4.10: Screenshot of an example error logged in IE where the user was trying to access security controls on a wrong interface

For instance on IE instead of customising protected mode under security settings to address cybersecurity case 1, a number of participants chose to turn on tracking protection in the safety menu instead. In these cases, the participants' actions were geared towards privacy preference settings rather than prevention of possible cyber-attacks through vulnerabilities in the browser. These users typically failed to adjust ActiveX settings that can malfunction and be used to remotely control, corrupt and/or destroy information on the PC. Some of the participants also went to enable and/or disable some pre-installed extensions on the "Manage add-ons" interface rather than accessing security and privacy settings available on the "Internet options" menu of IE. Two participants totally ignored the "Settings" menu on GC and attempted to complete the password manager use case with their *Gmail* account instead.


[redacted]
[redacted]

Your Primary tab is empty.

Personal messages and messages that don't appear in other tabs will be shown here.

To add or remove tabs click inbox settings.

No recent chats
Start a new one

Your Google Account is protected by the most advanced online security. Keeping these settings up-to-date safeguards your account even more.

Security Checkup
Protect your account in just a few minutes by reviewing your security settings and activity.
GET STARTED

Find your phone
Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet.
GET STARTED

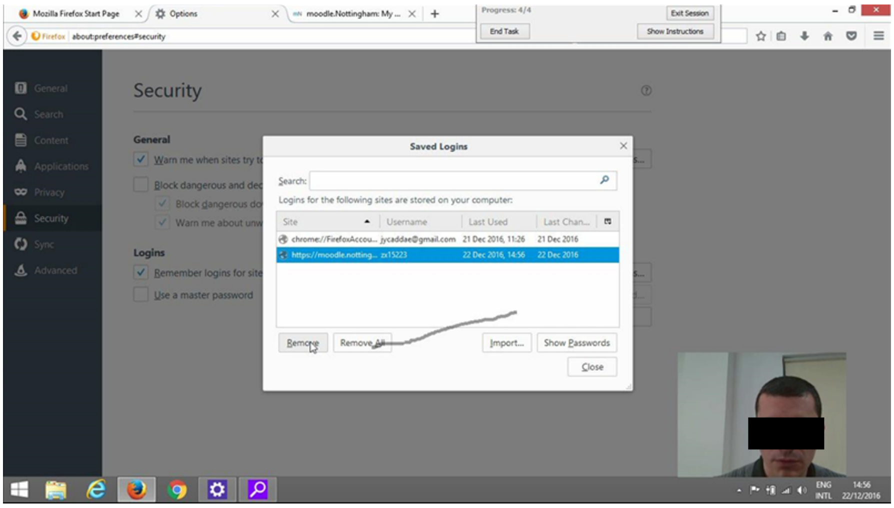
Signing in to Google
Control your password and account access, along

Screenshot A

Screenshot B

FIGURE 4.11: Example errors logged on GC with participants navigating to the wrong interfaces while attempting to perform the security use cases

Some of the error logged by the Morae software used to conduct the usability study were system based. For instance in Firefox, few participants missed a step in the password manager task and deleted their saved passwords because the system failed to ask for a confirmation. Similar errors were logged for GC as well because the system failed to prompt participants to confirm delete actions for saved login details. Figures 4.10, 4.11 and 4.12 are screenshots of some of the errors logged during the study. All these error logs reflect usability issues inherent in the various UI designed for optimizing security and privacy on the three web browsers.


[redacted]

Saved Logins

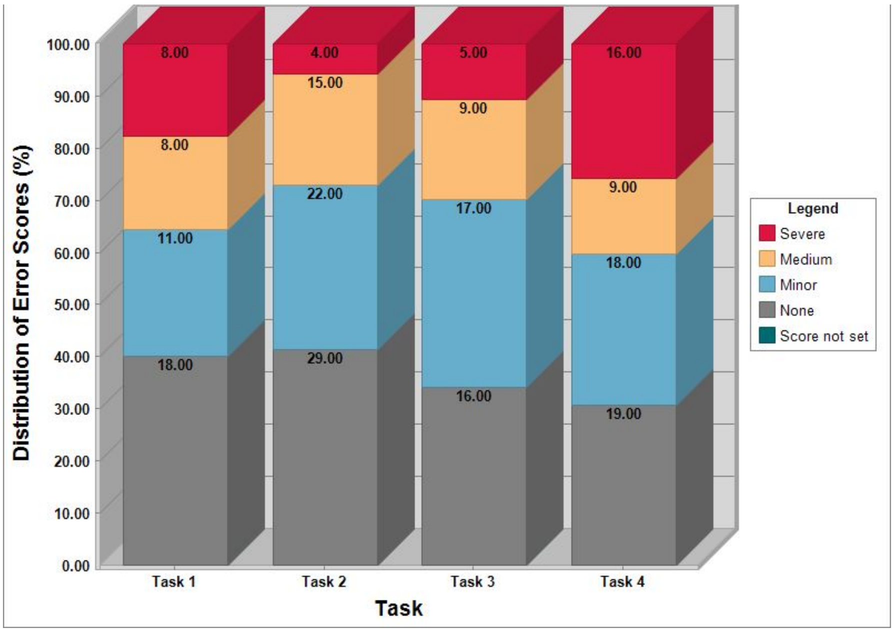
Search:

Logins for the following sites are stored on your computer:

Site	Username	Last Used	Last Chan...
chrome://FirefoxAccou...	jycaddae@gmail.com	21 Dec 2016, 11:26	21 Dec 2016
https://moodle.notting...	zx15223	22 Dec 2016, 14:56	22 Dec 2016

FIGURE 4.12: Screenshot of system related error logged in Firefox whereby delete actions were not confirmed with the user and no undo function provided

The importance of categorising the severity of identified usability problems has been emphasized in the literature. Consequently, several sets of ordered categorization structures have been proposed to reflect the impact of the identified problem on a user, from minor to major (e.g.[162–165]). Nielsen [162] proposed five levels of categorisation for problem severity — catastrophic, major, minor, cosmetic or not a usability problem. Molich and Dumas [165] offered a three-point scale that categorise problem severity based primarily on how it impacts on task duration — minor ("delays user briefly"), serious ("delays user significantly") and catastrophic ("prevents user from completing their task"). These categorisation approaches were adapted for scoring each user and system error in terms of their impact on performance or emotional state of the participants during the study. The distribution of error scores captured is presented in Figure 4.13 with four levels of severity on usability.



None: not a usability problem; Minor: causes some frustration and brief delay; Medium: causes moderate frustration and significantly delays user; Severe: causes severe frustration and prevents task completion

FIGURE 4.13: Distribution of Error Scores by Task

4.4.2.3 Task Time Summary by Browser

Task Time metrics are used to measure the efficiency of each browser's security interface design. Descriptive statistics on the time taken to complete each of the four security case tasks are presented in Table 4.4 for all the three web browsers. The mean task time duration to complete the cybersecurity tasks are quite similar across the three web browsers. However, The Friedman Test results in Table 4.5 revealed significant differences in the overall tasks completion time across the three browsers except task two. The best performing web browser in terms of time taken for each cybersecurity task case can be observed from the task time summary table and the mean ranks obtained from the Friedman Test. For Task one, both GC and IE had similar average task duration although IE had a greater recorded maximum time of 584.64 seconds compared to GC 447.01 seconds. FF had the lowest recorded maximum and mean time to complete both security and privacy settings cases (Task 1 & 2). However, FF's backup and encryption (Task 3) mean time (327.25 seconds) was greater than that of GC (255.53 seconds) and IE (136.81 seconds). The password manager security case (Task 4) recorded similar mean time for both FF (328.90 seconds) and IE (391.67 seconds) compared to 287.87 seconds for GC. The best task time values for each cybersecurity case is highlighted in both the Tables 4.4 and 4.5. FF appeared to be significantly more efficient in

TABLE 4.4: Average Task Time by Web Browser

Case Summaries

Browser		**T1_TS**	**T2_TS**	**T3_TS**	**T4_TS**
Firefox	N	20.00	20.00	20.00	20.00
	Mean	**114.46**	**191.63**	342.25	323.90
	Minimum	41.42	17.13	128.77	21.36
	Maximum	224.40	356.45	981.25	645.77
	Grouped Median	98.16	192.15	319.14	294.31
	Std. Deviation	58.57	97.19	198.15	183.61
Google Chrome	N	20.00	20.00	20.00	20.00
	Mean	212.46	230.38	230.53	**272.87**
	Minimum	31.48	54.67	41.94	29.86
	Maximum	447.01	637.99	541.81	786.19
	Grouped Median	185.77	188.19	196.66	245.76
	Std. Deviation	120.06	150.98	147.23	183.98
Internet Explorer	N	20.00	20.00	20.00	20.00
	Mean	225.85	228.78	**161.81**	391.67
	Minimum	53.79	51.05	26.78	162.00
	Maximum	584.64	820.21	666.00	913.53
	Grouped Median	210.33	163.01	115.09	349.30
	Std. Deviation	139.02	179.35	140.28	202.48
Total	N	60.00	60.00	60.00	60.00
	Mean	184.26	216.93	244.86	329.48
	Minimum	31.48	17.13	26.78	21.36
	Maximum	584.64	820.21	981.25	913.53
	Grouped Median	139.57	183.64	196.66	305.51
	Std. Deviation	120.33	145.15	177.72	193.31

TS: Task Time in Seconds

completing cybersecurity tasks 1 and 2 but less effective in completing tasks 3 and 4. IE seemed to be less effective in completing all tasks. Even though it recorded the lowest mean time for task 3, this was mainly due to most participants deciding not to waste time figuring out how the backup and encryption feature works in IE. Thus most participants failed to complete task 3 using the IE browser. GC recorded the lowest mean time (287.87 seconds) on task 4 although it had a greater maximum time (768.19 seconds) than FF (645.77 seconds). Taken together, these observed differences in efficiency preliminarily reflects the distinctiveness in the three browser's UI design.

Research method developments in Human Factors have identified the need to complement traditional usability evaluation with user event data automatically generated by the interface being tested [166]. More recently, Kortum and Acemyan [167] conducted a study to compare traditional usability metrics with automatically generated interface events and found very strong correlations between the SUS scores and mouse-based measurements. In this study, the number of mouse clicks and movements were automatically generated with Morae Recorder while participants perform the study task. These were exported into Microsoft Excel to visualise and compare the average mouse clicks and movements per task for the three web browsers.

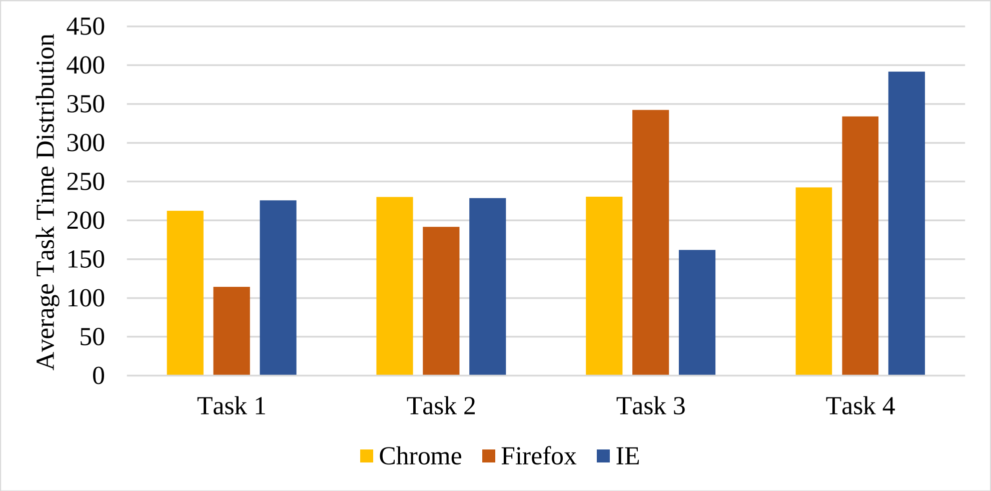


FIGURE 4.14: Average Task Completion Time Distribution By Browsers

TABLE 4.5: Friedman Test results for task time differences by browsers

Task	Browser	Mean Rank[a]	N	Chi-Square	df	Asymp. Sig.
Task 1	**FF**	**1.45**	20	10.300	2	0.006
	GC	2.10				
	IE	2.45				
Task 2	**FF**	**1.85**	20	0.700	2	0.705
	GC	2.05				
	IE	2.10				
Task 3	**IE**	**1.50**	20	11.100	2	0.004
	GC	1.95				
	FF	2.55				
Task 4	**GC**	**1.60**	20	8.400	2	0.015
	FF	1.90				
	IE	2.50				

a. Mean rank of task time displayed in ascending order

As shown in Figure 4.15, mouse clicks increased with task difficulty levels. It can also be seen that there were generally less number of mouse clicks when performing the study task with GC. Interestingly participants complained about the long list of options on GC's main settings page. However, lower number of mouse clicks here can be attributed to the search box provided which some participants discovered and used though some others missed it. GC's lower number of mouse clicks for completing the study tasks is however not consistent with the average mouse movement plotted. Apart from task 4, IE had the lowest number of mouse movements per study task. This outcome can be attributed to the slider implemented for security and privacy settings. Participant's satisfaction towards the sliders included on IE's security interface is highlighted in the user preference analysis section (4.4.4.2).

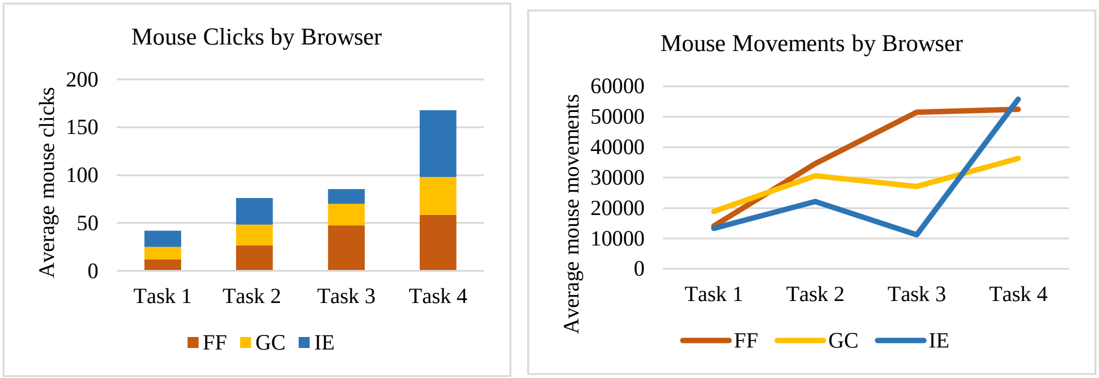


FIGURE 4.15: Average number of mouse clicks and mouse movements per task for the three browsers tested

4.4.3 System Usability Scale (SUS) Scores

The SUS adopted as part of the usability evaluation, is a standard usability metric that is referenced in many publications as a post-study evaluation survey (e.g. [168]). It is used to assign a scalar value (0-100) to a system based on user feedback. Thus, a single numeric score is used to estimate the overall usability of a system under evaluation with higher scores indicating greater usability. SUS is a 10-item survey instrument that can be easily adapted to evaluate user experience on different types of interactive systems including system applications, electronic devices, websites etc. Each participant responded to the ten questions relating to their experience with web browser security controls (WBSC) after completing all four security case tasks. The questions alternate between positive and negative statements about the WBSC and answers are given using a five point Likert scale (see 4.3).

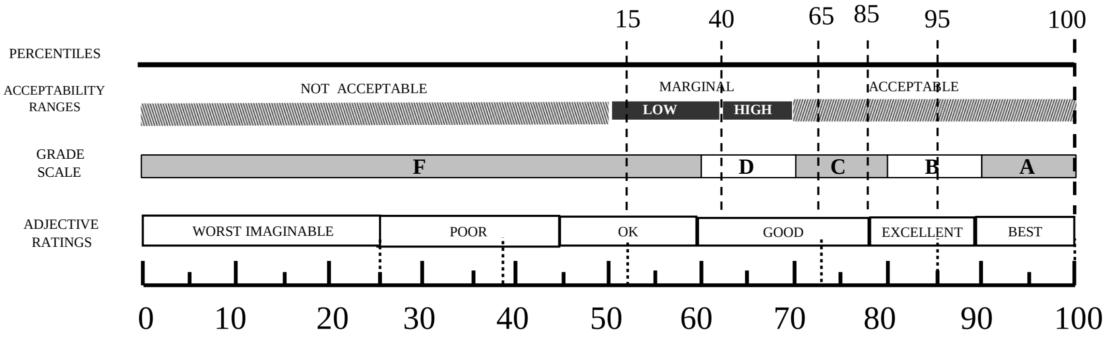


FIGURE 4.16: Adjective-based interpretation of SUS scores

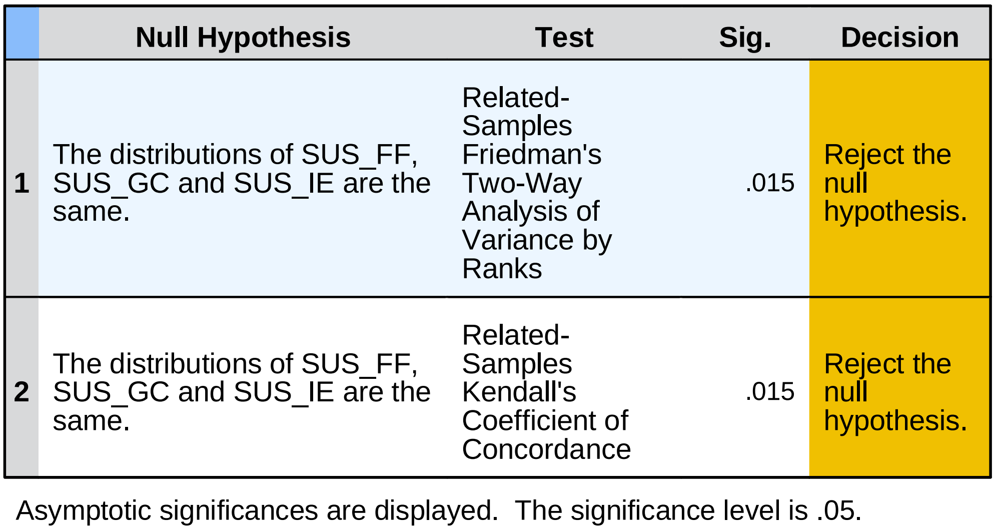
SUS has been shown to be reliable across different sets of study participants than other commercially available ones [169–171]. It has been used to effectively grade the usability levels of different kinds of systems. A number of researchers have analysed several of these usability studies to derive adjective-based ratings describing SUS scores [172, 173]. These adjective-based ratings is used here to aid the interpretation of the SUS scores and provide readers with a better context for understanding each browser's usability level (see Figure 4.16). Using these ratings, IE's SUS score of 40.13 for its security interface is rated as having "Poor" usability. It fall below the 15th percentile, is considered as "Not Acceptable" and given a letter grade of "F". Even though the security interfaces for GC and FF are rated as "OK" and "Good" with SUS scores of 56.50 and 61.88 respectively, their usability is still not impressive. According to the adjective-based scale, both scores fall below the 40th percentile, and are classified as having a "Low-marginal" usability acceptability. FF is given grade "D", whereas GC is given a failing grade of "F".

TABLE 4.6: SUS scores by browser and participant preferences

Browser	**N**	**SUS**			**Influence on Task Difficulty**			**Is Participants' favourite browser**
		Mean	**S.D**	**Median**	**Easy**	**Somewhat Hard**	**Hard**	
Firefox	20	61.88	20.50	58.75	18%	43%	40%	30%
Google Chrome	20	56.50	21.44	58.75	11%	48%	41%	65%
Internet Explorer	20	40.13	22.01	35.00	18%	43%	40%	5%

A Friedman test performed indicated a significant difference exists between at least two of the three browsers' SUS scores $\chi^2(df = 2, p < 0.05) = 8.430$ (see Table 4.7). Tests of the three a priori hypotheses were conducted using Bonferroni adjusted alpha levels of .017 per test (.05/3). Wilcoxon signed rank test results in Table 4.8 shows that the SUS scores given for IE (M = 40.13, SD = 22.01) was significantly lower than those in both the case of GC (M = 56.50, SD = 21.44), (Z=-3.124, p =0.001) and in the FF condition (M = 61.88, SD = 20.50), (Z=-2.820, p = 0.003). The pairwise comparison of the SUS scores for GC with those of FF was non-significant.

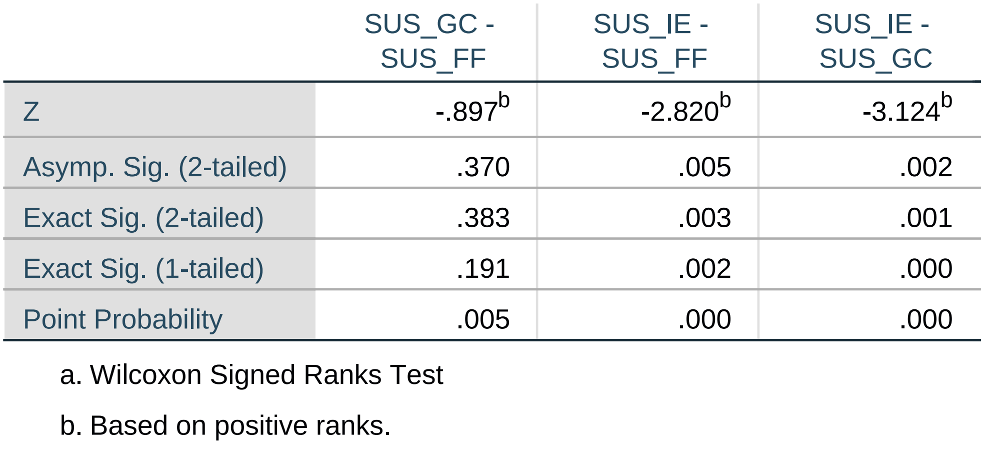
TABLE 4.7: Browser SUS Hypothesis Test Summary



	Null Hypothesis	Test	Sig.	Decision
1	The distributions of SUS_FF, SUS_GC and SUS_IE are the same.	Related-Samples Friedman's Two-Way Analysis of Variance by Ranks	.015	Reject the null hypothesis.
2	The distributions of SUS_FF, SUS_GC and SUS_IE are the same.	Related-Samples Kendall's Coefficient of Concordance	.015	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

TABLE 4.8: Wilcoxon Signed Ranks Test Statistics on SUS by Browser



	SUS_GC - SUS_FF	SUS_IE - SUS_FF	SUS_IE - SUS_GC
Z	-.897b	-2.820b	-3.124b
Asymp. Sig. (2-tailed)	.370	.005	.002
Exact Sig. (2-tailed)	.383	.003	.001
Exact Sig. (1-tailed)	.191	.002	.000
Point Probability	.005	.000	.000

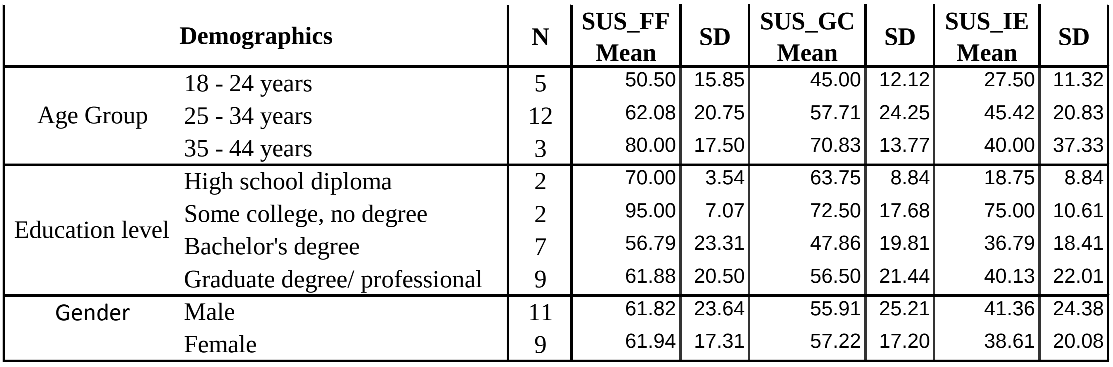
a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

4.4.3.1 SUS by Demographics

To investigate whether or not the demographic characteristics influenced usability expectations, hence adoption of cybersecurity tools, the SUS scores were compared between the demographic variables (gender, age group and education level). There appears to be some differences in SUS by browser based on Age Group. The mean SUS result in Table 4.9 showed a slightly higher usability expectation pattern for the younger age groups. However, a Kruskal-Wallis test conducted found no significant differences in mean SUS scores for any of the three age groups ($\chi^2(2) = 3.664, p = 0.160$) (see Table 4.10 and Figure 4.18).

TABLE 4.9: Mean SUS Score by Browser based on Age, Education and Gender



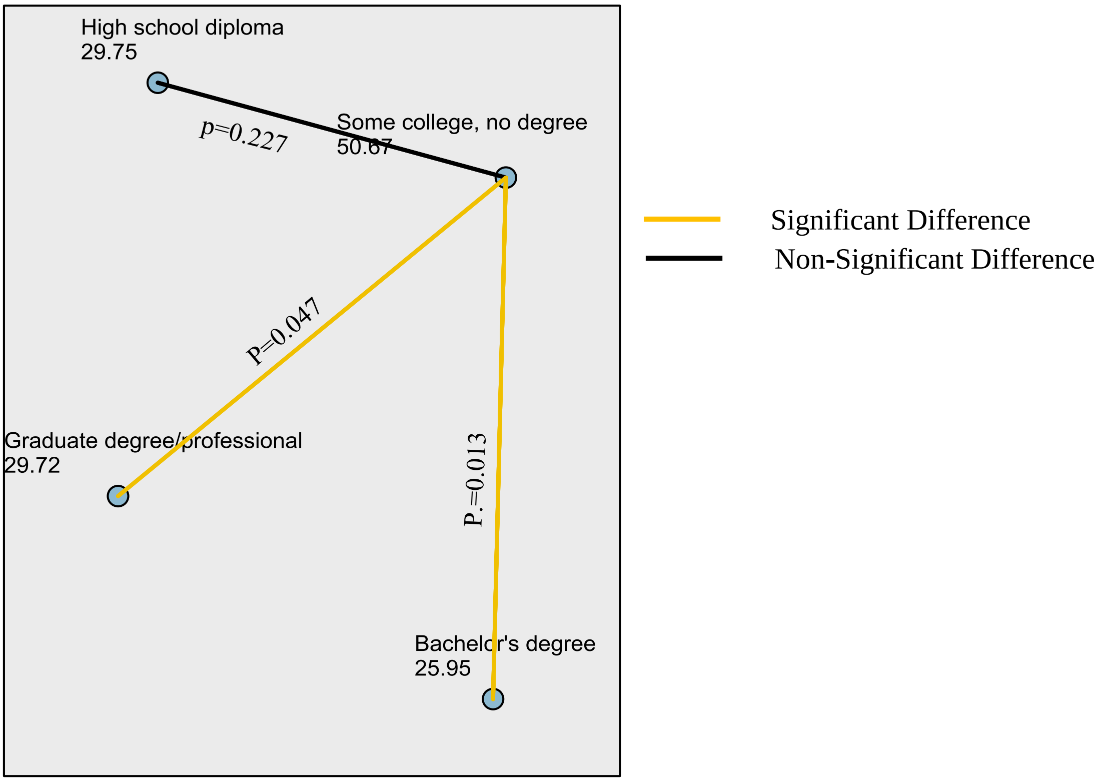
Demographics		N	SUS_FF Mean	SD	SUS_GC Mean	SD	SUS_IE Mean	SD
Age Group	18 - 24 years	5	50.50	15.85	45.00	12.12	27.50	11.32
	25 - 34 years	12	62.08	20.75	57.71	24.25	45.42	20.83
	35 - 44 years	3	80.00	17.50	70.83	13.77	40.00	37.33
Education level	High school diploma	2	70.00	3.54	63.75	8.84	18.75	8.84
	Some college, no degree	2	95.00	7.07	72.50	17.68	75.00	10.61
	Bachelor's degree	7	56.79	23.31	47.86	19.81	36.79	18.41
	Graduate degree/ professional	9	61.88	20.50	56.50	21.44	40.13	22.01
Gender	Male	11	61.82	23.64	55.91	25.21	41.36	24.38
	Female	9	61.94	17.31	57.22	17.20	38.61	20.08

There also seemed to be a relationship between participant's education level and SUS ratings based on the mean scores in Table 4.9. Participants who completed a higher level education seem to have higher usability expectation pattern and vice versa. A Kruskal-Wallis H test (Table 4.10), showed that there was a statistically significant difference in SUS score between the different education levels, $\chi^2(3) = 9.501, p = 0.023$. As shown in Figure 4.17, The relationship between some of the SUS scores and level of education was significant although the pattern is inconsistent with initial observation in the mean SUS scores in Table 4.9. The result however, indicates that education affects usability expectations.

TABLE 4.10: SUS Hypothesis Test Summary for Demographic Variables

#	Null Hypothesis	Test	Sig.	Decision
1	The distribution of SUS Scores is the same across categories of Age Group.	Independent-Samples Kruskal-Wallis Test	0.16	Retain the null hypothesis.
2	The distribution of SUS Scores is the same across categories of Education level.	Independent-Samples Kruskal-Wallis Test	0.023	Reject the null hypothesis.
3	The distribution of SUS Scores is the same across categories of Gender.	Independent-Samples Mann-Whitney U Test	0.02	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Each node shows the sample average rank of Education level. The significance level is 0.05. Significance values displayed have been adjusted by the Bonferroni correction for multiple tests.

FIGURE 4.17: Pairwise Comparisons of Education Level

The SUS ratings on each of the web browser's security interface appeared to be somewhat higher for males than females (see Table 4.9). An independent-samples Mann-Whitney U test (Table 4.10) showed that the distributions in the two gender groups also differed significantly ($U = 292.50, P < 0.05$ two-tailed). As can be seen in Figure 4.19, male participants generally rated the usability of WBSC higher than their female counterparts.

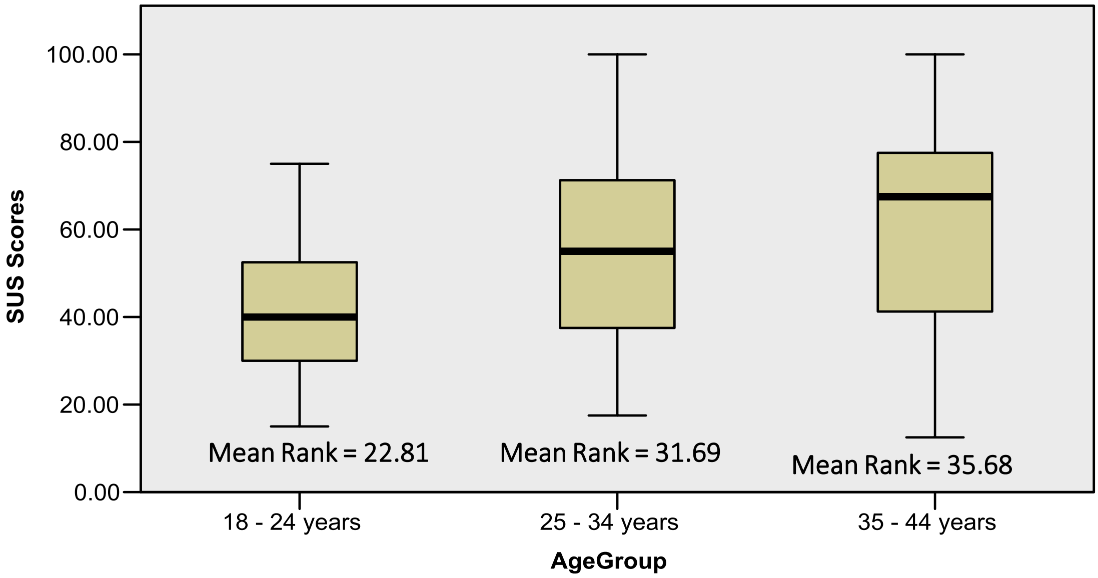


FIGURE 4.18: Kruskal-Wallis Test for SUS Scores by Age Group

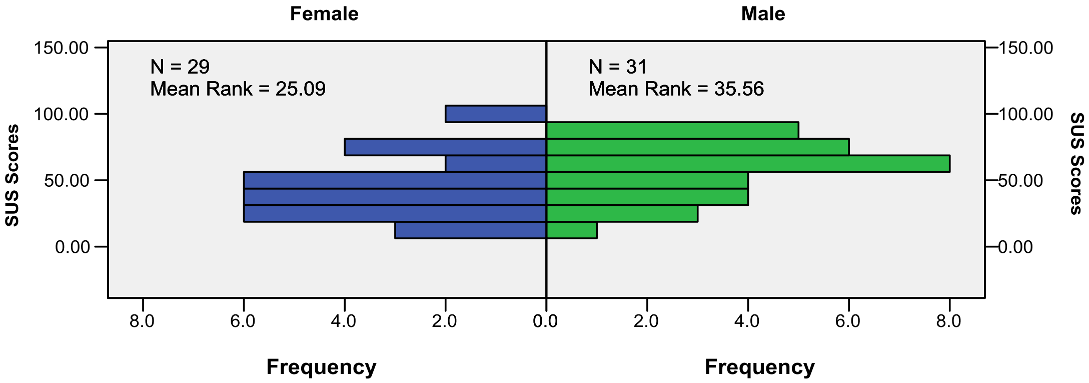


FIGURE 4.19: Mann-Whitney U Test Comparing SUS Scores by Gender

4.4.4 Usability Problems Analysis and User Requirements

The usability testing of the three web browsers involved a think-aloud protocol. Think-aloud protocol in usability testing allows the *learnability* aspect of an application under evaluation to be assessed for novice users [174]. Think-aloud can also reveal participants mental model about how the system being evaluated should work. The think-aloud together with steps taken by the novice user to perform the study tasks is often used to determine whether or not the user knows how to do the task. The combined approach also allows points of confusion, frustration and other usability issues to be noted [159]. For this study, the transcripts generated from the think-aloud protocol were coded with a specific focus on the study aim of uncovering usability problems, user preferences and requirements for personalized cybersecurity design. The analysis concentrated on discovering utterances relevant for usability problem analysis in the security interfaces.

TABLE 4.11: Definition of Classification Labels with Examples

Categories	Definitions	Examples
Reading	Read out texts and links	*“Allow sites to check if you have payment methods saved ...”* *“Delete temporary files, history, cookies…”*
Action	Performing an action, describing how a particular action is performed and/or explaining the reason(s) for performing or not performing an action.	*“Ok so am just trying to find password manager now so am on the sync page where it says sync across all device and ask for password.”* *“So backup is essential. Just make a copy of that folder and I store it somewhere else”*
Evaluation	Summarise understanding or give evaluation of interface object, content or the outcomes of actions.	*“Am used to Google Chrome so if I were to save my password with them for the autofill information that would sort of be all right.”* *‘’ ... so like it has this little adjustable slider for me to adjust my security``*
User Experience	Express positive or negative feelings, aesthetic preferences towards the browser interface or compare to another interface or recall of past experiences	*“Okay so nothing popped-up, just deleted it straight off without warning”* *“I really like how Firefox had the list on the side. You just click on it and then it shows like everything else on another page”*
Problem Formulation	Verbalise difficulties, including utterances that participants indicate uncertainty; and utterances that participants not only express a negative feeling or disapproval, but also indicate that it was caused by system based issue(s).	*" I click on that and it removed. It just removed with one button. Now am feeling like if I clicked on something else and the click removed then the password would be removed without some kind of a pop-up box saying that are you sure you want to remove this. Okay so that is worrisome.”* *“It seems that I have to be digging through a list of different folders instead of being giving a link to click on so I can save some time."*
Impact	Indicate outcomes or impacts caused by difficulties encountered, including the repeated mention of a difficulty, and implications of errors made	*“Am not very sure about what does encryption here mean. I would just end it here, It sounds too sophisticated.”* *“The search results is telling me to open the control panel. Where is that? I don't know about this so I think I would have to leave this.”*
Recommendation	Give recommendations on how to improve the interface or solutions to difficulties experienced	*“It would be good to have it confirm delete action before deleting.”* *“ If they like clearly distinguish which security features novices like me should be messing with I would have more confidence."* *“Why can’t they have like an indicator that automatically shows you your security and privacy level anytime the browser is opened?”*

Question	Asking a question or indicate confusion or misunderstanding about interface tasks	*``About dangerous list of websites, where can I put on exceptions? how do I do that?``*
		``What is active-x filter? What is it doing here under security. Should I turn it off?``

NVivo 12 Pro [175] was used to integrate all the qualitative data gathered from the process and for all the content and thematic analysis. First of all, each test session

TABLE 4.12: Summary of Themes

Themes	**Participants (N = 20)**
Usability Issues	
Inconsistencies	19
Menu Navigation/Visibility	16
Uncertainties	15
Technical Language	13
Error Recovery	12
Design Preferences	
Simplistic Design	17
Search Function	12
Slider	10
Recommendations/ Requirements	
Automatic Back-up	20
System Status	17
Automated Assistance	16
Notifications/Alerts	14

was transcribed and segmented into individual utterances. Each utterance had a single topic though varying in length. The individual utterances were annotated with the participant number and browser name. This allowed for context-appreciative coding to be used whereby the segmenting and coding was entwined during the analysis. Yang [176] emphasised the importance of contextual checking for accurate interpretation of utterances. Therefore during the categorisation, the test session videos were repeatedly visited and examined for contextual information on the utterances. Patterns and threads were identified in the transcripts which were marked with labels and then grouped together. Initially, 18 nodes emerged from the process. The nodes were later reduced to the 8 categories shown in Table 4.11 after merging labels with similar utterances. Multiple rounds of meetings were held to discuss themes emerging from clustering the patterns in the data set and to resolve coding disagreements. The final set of themes that emerged from the qualitative data (Table 4.12) were cross-checked for validation by two other researchers who were not initially part of the theme development process. The prefix *P* is used to indicate a participant in reference to some of the representative utterances for the themes discussed below.

4.4.4.1 Usability Issues

Majority of the participants complained about inconsistencies of terms used across the three security interfaces evaluated. For instance, in GC, the security settings interface can be assessed through settings while this is respectively labelled as Internet Options and Options in IE and FF. The problem is further compounded in IE whereby the menu item labelled Safety caused first-time users among the participants to be misled to the “Manage add-ons” interface rather than the security settings interface. Terms like add-ons, extensions and toolbars were also noted to be inconsistent and confusing. Another major inconsistency noted by most participants has to do with how privacy and security configuration items were organised. For instance, FF and IE had block dangerous sites under security settings while GC presented it under privacy settings. In a typical example, P15 remarked *"Actually the security settings are under privacy, that is a little bit counter-intuitive"* while looking for how to secure the browser from dangerous sites. P7 also stated that *"There is inconsistency because I want to block pop-up and it was in the content tab. I would have expected it to be on the privacy tab."*

A second popular usability sub-theme is the visibility of several of the menu items. 16/20 participants found the organization of the various menu items on the settings interface to be unintuitive typically complaining about time wasted having to *"sieve through loads of information before finding the settings I want.''* This problem was more pronounced in the IE and GC interface as fully expressed by P4 *"With Google, you have to keep scrolling through the entire list everything was just like one after the other and Internet Explorer which has multiple tabs, I click on the tab then another box clicks opens up another and another box opens up. Very time consuming."* Although GC provided a search box on their settings interface, few of the participants seem to have noticed and made use of it instead of scrolling through the long list of settings.

15/20 participants expressed uncertainties about what needed to be done to achieve some of the goals outlined in the core-tasks. P5's comment characterises this theme *"What is active-x filter? What is it doing here under security. Should I turn it off?"* Some participants kept trying until they achieved the objective set out in the security case while a few gave up after one or two attempts but sometimes leading to false task completion. Thus when not sure of what they are to do, participants would typically comment on: *"I'm not too sure how to optimize it myself."* or *"I think I did it"*. In a typical false completion scenario caused by uncertainty one participant reasoned: *''It looks like Mozilla from what am seeing they don't really have that option to disable pop-ups and I need to install an extension like an Add-blocker"*. Thus in the absence of a clear indication of the security or privacy state, the participant erroneously believed there were no pop-ups to be blocked. A lot more of the utterances captured under the uncertainty sub-theme pointed to the fact that participants were mostly unsure about whether their settings were correctly activated. They often commented on *"Nothing to show but I think am done"* or *"Am not sure if it is here or somewhere else."* All 3 interfaces provided little or no feedback and participants kept looking for some indication that they had been successful. P1's comment exemplifies a typical outcome of such uncertainty: *"Scrolling through one more time just in case I need to do something. It didn't notify me that the changes have been saved. May be not."*

Another usability sub-theme pertains to the language used to label configurable items on the security interfaces. 13/20 participants express displeasure about the fact that they could not understand some of the terminologies typically commenting on *"I feel* *like I need to be a computer scientist to understand some of this"*. Participants who indicated they had never tried to optimise their security or privacy settings particularly struggled to understand some of the terminology employed in the security interfaces. P9 and P18's comments capture this sentiment: *''So would this be the option to further enhance security? Well seems like I need some basic degree of computer security knowledge to understand what these different terms are like JavaScript , .Net Framework..."*

"It's a language that computer scientists would maybe would understand, like a programmer behind Mozilla Firefox they would know what they're looking at whereas me I'm just trying to find my profile folder trying to find files that says password list or something. But am not really finding it so like I looked on Mozilla maintenance and looked everywhere on Firefox."

The Error-recovery sub-theme emerged primarily because of how GC's password manager is implemented. The participants whose utterances led to the formulation of this sub-theme found they were unable to recover their login details accidentally deleted while exploring the GC's password manager function. Thus they mistakenly deleted their saved login details and could not recover since GC did not offer a delete confirmation or undo function. P4's comment illustrates this sub-theme: *"Oh so nothing poped-up, just deleted it straight off. I feel like if I click on another one to check my password it would delete again. Okay so I just go back onto say login. Yeah now it shows invalid log-in. My password has been removed!"* Some of the participants desperately tried to recover the lost login details by turning to a search engine for possible guidelines or tutorials. They soon discovered that recovery from a loss of login details depends on the existence of an up-to-date backup. This did not sound like a simple task for most of the participants as it involved finding the right menu (GC), or the right file (FF and IE). This dread is better expressed by P13: *"It would be the most difficult one that I have to do. I would have to look online so if I wanted to back up my data I'd have to search and play some kind of tutorial..."*.

4.4.4.2 User Preferences for Security Design

Utterances indicating what participants liked or disliked about the three web browser security components tested converged into three main sub-themes. Although majority of the participants indicated at the start of the usability testing that their preferred browser was GC, a lot more seems to have taken to FF's design after interacting with all the three browsers' interfaces. P8's comment exemplifies the reaction of participants who were first-time users of FF's security /privacy settings: *" I have never checked-out Firefox settings but am really liking how simple their interface look"*. When asked for further clarification, participants revealed they were comfortable with FF's security/privacy page because it is simple, attractive and has a non-technical feel to it, unlike the other two interfaces. P11 explained: *"I really like how Firefox had the list on the side. You just click on it and then it shows like everything else on another page"* P6 also said: *"...so after using all three, I prefer Mozilla's interface. Feels like it was designed for non-technical users"*. It can be deduced from this sub-themes that design aesthetics matter to non-expert cybercitizens and it can lure them to interact more with cybersecurity tools even if security/privacy is a secondary goal to them. P4's comment supports this deduction: *"I have never tried Firefox settings but now I really like their interface. Made things easy. I mean there was just this one minor problem of me not finding the user profile but everything else is looks good."*

Another design preference emerging as a sub-theme is the acknowledgement of the search function's usefulness, expressed by 12/20 participants. Particularly, those that were aware of, or discovered the search function included on GC's settings page during the testing typically commented on: *"Settings in Google is just a very straightforward process. I don't have to go into different settings or more options. I just need to type what I want into the search engine to make my changes"*. While using the search to locate the password manager in GC, P16 explained: "It would take longer if I have to manually scan through everything before I find the option am looking for..." although the search was not helpful in this particular instance. This was because P16 searched for *"'Logins"* instead of *"Password"* having first encountered the term while configuring password manager in FF. It appears the search function is only useful if the user already knows exactly what to do to meet a specific security/privacy need (e.g. block third-party cookies, manage passwords etc.). P8's comment supports this point: *"I wouldn't have been able to come here and change anything on my own but, with the instructions given in the task I can just search for the key terms and not feel overwhelmed by all the details am seeing here"*.. Interestingly, even though both GC and FF had provided a search box for their settings, none of the participants seemed to have the need for it when using FF to perform the study task. They felt comfortable enough to explore the interface on their own. In IE, P16 complained about the lack of a search box saying *"I can see so many options, I wish there was a search box because it looks like it would take a while for me to find the password manager, at this rate I might not even find it"*.

Half of the study participants were very pleased about the slider used to gauge security and privacy levels in the IE interface. This emerged into the third sub-theme categorised under user preference. P7 remarked: *"I like that I can just slide to the level I want, I don't even need to understand the details"*. Sliders are generally used in applications to allow users to make adjustment until they obtain their preferred settings (e.g. image filters, volume control etc.). In such applications, sliders don't only make it easy for users to determine their preference from a range of values but they also reflect the current state of the settings before and after it has been controlled. While the slider implemented in IE settings achieves these objectives, some participants felt they were not given enough options to choose from to reflect their personal preference. P8 explained: *"I like the sliders but I wish there were more levels to choose from. I definitely don't want low but medium doesn't cover everything I want and high is too much"*.

4.4.4.3 Requirements/ Recommendations

While performing the third study task (Back-up and Encryption), a number of participants made suggestions about how the process could be simplified. 18/20 participants made suggestions similar to what P2 said: *"Instead of this plenty steps, there could be a click of a button, so like a window comes up for me to choose a storage location for the back-up"* Others like P5 recommended an automatic backup of their saved logins once a storage location has been specified, saying: *"If I choose a storage location, an auto back-up should be possible"*. However, a lesser number of the participants (12/20) recommending auto-backup welcomed the idea of automated assistance options, when asked as a follow-up to the automatic back-up suggestion. Their responses indicated a concern for the implication that might have on their privacy. P19 remarked: *"If it can automatically know what I want, then it's going to find out what I've searched for even if it's not in my history. And I don't really like the idea of person knowing where I live"*. However, majority of the participants indicated a desire for an option to customize the settings interface and improve organization/ visibility of frequently assessed menu items.

Other user requirements for web browser security settings gathered from the qualitative data were the need to include clear system status indicators on the settings page and the desire for personalized notifications/ alerts on security events. Comments made by P1 and P8 respectively reflects these requirements: P1 said: *"If they can simplify the interface and just include some indicators for security and privacy for people like me who don't know cybersecurity. That would be easy to read at least"* and P8 commented *"Some of this security alerts can be annoying. For that one I don't mind if they use my context to make it sensitive"*.

In this section, the comprehensive usability related findings from analysis of the quantitative data, subjective ratings (SUS), observations and participants' verbal feedback has been presented. The common usability problems identified in all the three web browsers are summarised in Table 4.13.

TABLE 4.13: Summary of usability issues and browser comparisons.

Usability Issues	Impact	Comparison Among The Three Interfaces Evaluated
Too many technical terms	Participants had difficulty completing some of the tasks because they did not understand some of the technical terms used on the interface e.g. Cookies, ActiveX, JavaScript etc.	All three interface had technical terms but IE security settings dominated this problem.

Continued on next page

Table 4.13 – *Continued from previous page*

Difficult to learn and understand	It was difficult for inexperienced participants to learn and/or determine how to perform some of the security tasks.	Those participants who had never configured their browser security settings struggled the most to perform task 3 and 4 on all three web browsers.
Inadequate Feedback and Status Indicators	Participants became uncertain where there were no clear indication of the effect of changes made. In some cases lack of clear security and privacy status indicator resulted in user error (False completion).	False completion was observed across the three web browsers' security interfaces but adequate feedback was particularly missing in GC's settings.
Inadequate Error prevention or recovery	Participants were not warned about some of the settings implication which affected their browsing experience (e.g. inability to sign-in on any websites because they had gone and enabled all the security features) and there were no simple undo options.	This was observed in all the three browsers' security interfaces.
Inefficiency	It took longer then expected for participants to complete some of the study task due.	IE was the least efficient in terms of task completion time.
Inconsistency	Participants got confused due to inconsistencies in terms of different labeling across the three web browsers hence difficulty in transferring knowledge from previous experience.	Inconsistency in the form of global design and labeling impacted on the usability of all three security interface tested.
Ineffectiveness	Although participants generally had high regard for the browsers' inbuilt security features, they still were unable to complete some of the security case tasks.	Unsuccessful task completion was recorded for all the three web browser security settings.

Continued on next page

Table 4.13 – *Continued from previous page*

Poor User Satisfaction	Participants were dissatisfied with how long it took them to complete certain security tasks as well as some of the inconvenience resulting from the changes they made. (e.g. inability to access certain websites that they did not think were harmful.	None of the three interfaces fared too well in terms of user's subjective ratings (SUS scores). However, IE received the lowest satisfaction ratings from participants.
Poor visibility	Participants missed certain core elements of the interface design (e.g. search box in GC, pop-up blocker in FF, password manager in IE) that were required to successfully complete some of the tasks.	This issue was evident in all the three security settings interfaces tested.

4.5 Discussion of Results

The study's results support the conclusion that there are indeed usability issues with existing inbuilt security features in web browsers and there is a clear opportunity for more effective and efficient design to meet user expectations. Specifically, the usability of the three WBSC was measured with the three usability metrics defined by ANSI/ISO: effectiveness, efficiency and satisfaction. In terms of effectiveness, the inability of participants to complete core security tasks outlined in the study was significantly high for all the three WBSC. Moreover, effectiveness cannot be achieved if majority of users made mistakes while attempting to complete a task with a system [177]. Factors such as technical language usage, inconsistent terminologies as well as inadequate feedback and clear system status indicators on the three UIs also affected the speed with which users completed core security tasks. Thus there were several instances where participants who were interacting with these WBSC for the first time got confused due to their inability to comprehend technical terminologies such as ActiveX, JavaScript etc. and ended up spending more time trying to figure out what to do with such features. Satisfaction, which is the most subjective part of usability, was measured with the system usability scale, an industry wide standardized scale. Satisfaction among users is known to ensure the continued use of an emerging technology. At a minimum, SUS score of 70 is considered acceptable to achieve satisfaction among users of security tools [178]. None of the three browsers security settings achieved this score from participants SUS ratings.

Clark et al. [85] reviewed various usable security research sources and came up with a set of heuristic guidelines for usable security *walkthroughs*. Accordingly, security applications are usable if users:

- are reliably made aware of the steps they have to perform to complete a core task.
- are able to determine how to perform these steps.
- can tell when they have successfully completed a core task.
- are able to recognize, diagnose, and recover from non-critical errors.
- are able to avoid making dangerous errors from which they cannot recover.
- are comfortable with the terminology used in any interface dialogues or documentation.
- are sufficiently comfortable with the interface to continue using it.
- are made aware of the application's status at all times.

Similar to the anonymity software they evaluated, securing a web browser involves the *learnability* of available configurations. Looking at the usability problems identified and summarised in Table 4.13, all three WBSC examined violated some of these usable security heuristics. Thus, none of the security interfaces of the three web browsers was without some severe usability issues. Even FF's security UI, which was the most favoured by participants after performing the study task with all three web browsers, lacked critical attributes of a usable security. Multiple issues arose because the security features were not always presented in a manner that matched users' mental models about how personal security and privacy should be controlled. Though several problems were detected using the think-aloud protocols, some positive feedbacks emerged that can guide specific design changes towards improving the usability of cybersecurity tools. The protocols also provided some insight into how users interact with security tools and their mental models about how WBSC should work. As shown in the analysis of the think-aloud protocol, users expressed mixed preferences with regards to automation. Most participants indicated a preference for partial automation of specific features (e.g. backup, blocking of third party cookies), a few wanted the entire security and privacy optimization process to be automated within the web browsers. Consequently, the findings suggest three main directions to improve the usability of desktop web browser security components:

1. Provision of personalizable and adaptive UI ,
2. Provision of automated functionalities and assistance,
3. Improving user engagement and enjoyment with minimalistic and modern aesthetics design.

Adaptability, which refers to the ability of a system to adapt to contextual changes, is progressively becoming an essential characteristic for user interface design [179–181]. Adaptive and/or personalised interfaces have been proposed as possible ways of addressing usability and acceptability issues related to different user domain and contexts [182, 183]. A distinction is made between adaptive and adaptable user interfaces: the latter refers to the enablement of users to control the adjustments to the interface by themselves instead of the system making the modifications automatically as in the case of the former [184]. Reasons for system adaptation studies in the past included intelligent user interface development [185] and varying interfaces according to user requirements [186]. The Computing Research Association et al. [18] report suggests that the problem of usable security is mostly rooted in the design of the security system and its accompanying user interface which are difficult to adopt by end-users. The concept of an adaptive interface however, implies that the interface has to adapt to the user instead of the converse.

Notwithstanding the inherent benefits of adaptive human-computer interfaces, adaptation is generally underscored with several complex modelling requirements and implementation problems that need to be addressed. In order to ensure that the adaptive interface can change with respect to both the task domain and the context of the current user, an effective user model needs to be developed. There is therefore a general consensus in the adaptive interface research community that user models are among the first issues that need to be addressed for adaptive systems. User models may differ from one individual to the other in adaptive systems and the system needs to be able to adjust to individual characteristics and preferences. Characterising and building identified user differences into the system is therefore a difficult but a crucial goal in the design of adaptive interfaces.

Several studies on systems adaptation highlight the need for user models underlying adaptive systems to account for evolving variations in user capabilities [183, 187, 188]. In effect, user models in adaptive systems generally lead to the collection of context parameters such as*command types*, *error rates*, and *speed* for the purposes of inferring users levels of expertise. This is despite the fact that researchers have long recognised other individual characteristics that go beyond *level of experience* to be part of the factors that affect the level of performance when users are interacting with human-computer interfaces [137]. Focusing on levels of expertise and capabilities as an approach to user modelling may therefore not be useful in understanding the task environment of the user. Thus, the extent to which these models represent the dynamics of people and/or groups of users in the real world is limited. Although adaptive user interfaces are designed to automatically update the user models during actual interaction sessions through behaviour monitoring, it is important to input information on the different categories of user characteristics to serve as a baseline.

It is worth noting that the study was not without limitations. First, the study was conducted with participants from one university hence generalization needs to be done with caution. The education level of the participants was also generally high and may not be very representative of the population of novice and/ or home computer users who are the main focus of this study.

4.6 Chapter Summary

In this chapter, the results of a within-subjects empirical usability study for the security settings of three web browsers have been presented. The study highlights the importance of testing security mechanisms with representative users and with realistic scenarios that provide context for security goals to be achieved. The usability testing was performed to better understand issues that exist within inbuilt security component for web browsers. Usability problems common to all three browser security UIs tested were discovered and reported. The findings discussed can inform future development of cybersecurity tools that can have less demand on users' cognitive resources and increase their rate of adoption. The particular security vulnerabilities exposed due to these usability problems were also noted. The findings suggests that designers need to carefully consider how the content and organization of cybersecurity tools are presented to novice and/or home computer users.

Personalization and automated functions characterised the requirements solicited from participants during the study. The relevance of the augmented behavioural model proposed for adaptive cybersecurity in Chapter 3 is clearly supported by these findings. An iterative process of user feedback, design, and user testing is however required to produce user-centred automated assistance and adaptive security features in web browsers. This thesis first identified critical cybersecurity behaviour and acceptance variables relevant for the provision of personalized adaptive cybersecurity in Chapter 3. Chapters 5 and 6 present the studies conducted to test and evaluate the ensuing predictive model based on the variables identified. Based on findings from the studies presented in Chapters 4, 5, and 6, a preliminary prototype adaptive web browser security control is then designed and evaluated in chapter 7.

CHAPTER 5

Measuring Cybersecurity Behavioural Attitudes

Contents

5.1 Introduction

The amount of personal data being captured, collated, analysed and shared is growing every day. The trend is mediated by technologies such as smart-phones, social networking, and smart-meters [189]. Previous work has highlighted that personal privacy is more vulnerable to erosions when contextual and personal information is gathered by pervasive computing systems [8, 190]. Although personal data is recognized as a key issue requiring innovative cybersecurity measures within the digital economy, there are comparatively few studies exploring individuals' attitudes towards it. Iachello and Hong [191] reviewed privacy related literature within the context of HCI and identified the need for a deeper understanding of individuals' attitudes towards the phenomena as a major challenge. Lederer et al. [192] also acknowledged the fact that different aspects of privacy pose a challenge for the design of usable systems. Essentially, there is not enough information available to guide stakeholders, including new technology designers and policy-makers, in dealing with or addressing issues related to personal data. Innovative mobile information service providers are, for instance, faced with the question of how different users will respond to personal and context-aware services. Cybersecurity designers especially need to understand different aspects of personal data issues to be able to develop systems that can adequately support values that constitute acceptable social behaviour.

The lack of empirically identified factors influencing individuals' digital security behaviour presents a major challenge to address the human component of cybersecurity. As technologies become more personalized and context-aware, there is a need to understand the interfaces and functionality required to accommodate individual differences in both use and attitude. The study presented in this chapter is part of this thesis attempts towards addressing the critical issue of leveraging knowledge about individual differences for the design of usable and adaptive cybersecurity. To identify relevant determinants of cybersecurity practices and predict individuals' security behaviour, we have presented an improved cybersecurity research model in Chapter 3 that integrates Planned Motivation Theory (PMT) with the Technology Acceptance Model (TAM), and enables a wider variety of factors influencing cybersecurity behaviour to be explored (Figure 3.4). The research model is designed to consider the personal data ecosystem and how external factors such as users' prior experiences and demographic characteristics could shape an individual's beliefs regarding the benefits and consequences of certain security-related behaviour.

Consequently, developing a Attitude to Personal Data (APD) measurement scale is determined to be essential in understanding and responding to people's views and attitude towards the data set around which digital technologies are built. Against this background, the different dimensions of attitudes toward personal data was examined in this research with the aim of developing an APD scale, and verifying the dimensions of attitudes toward different types of personal data. Thus, the chapter focuses specifically on the development of a quantitative APD measurement scale for the capture and analysis of attitudes across groups, contexts, and datasets. Such an instrument could then be adopted in further pragmatic research activities to substantiate propositions in this area to offer theoretically informed guidelines for addressing personal data issues. Essentially, the results presented in this chapter support the inclusion of personal data as a measurable variable in behavioural models being amplified for adaptive cybersecurity.

5.2 Background and Related Work

Technological advancement has the potential to enhance peoples' lives in many ways by facilitating the generation and sharing of knowledge. However, whenever we interact directly or indirectly with technologies, we leave behind data trails and digital footprints which can be used to generate information about our lives and activities. A considerable and increasing amount of information is gathered about us which are processed, stored, explored, shared, commercialized, and potentially misused by both public and private individuals and/or organizations. This raises concerns about issues such as privacy, security and other digital asset rights [193]. Consequently, when personal data is gathered, such as by pervasive computing devices, it is important to consider the range of potential implications for the individuals concerned. Previous research projects have explored personal data, mostly focusing on exploring people's attitude towards a single or limited subset of existing and/or near future technologies rather than the personal data itself. For instance, Brown [194] adopted vignette-based survey to explore the social implications of data gathered through "Internet of things" (IoT) in homes. They highlight a range of concerns about the technical systems but in some cases, it is unclear if these are due to the interface, data collection, display or data being collected. Although research approaches that explore users' attitudes to an identified technology are useful in assessing users' perceptions of a technology's usage of sensitive resources, it is also valuable to look at attitudes towards the data itself rather than the technologies through which it is created and accessed [195].

A requisite preliminary stage in the creation of a validated measurement instrument is a consideration of the relevant construct dimensions. The relevant construct, in this case, is individuals' attitudes towards personal data. In defining attitude to personal data, the general definition for *attitude* is adopted from the behavioural science literature and applied it to this research context. Therefore, *Attitude to personal data* (APD) here, refers to the behavioural tendency of an individual to negatively or positively evaluate the disclosure of a personal data. To successfully capture the factors influencing individuals' attitude to personal data, existing literature on the underlying dimensions of the concept was first reviewed. We started by considering available definitions of the object towards which attitude is being measured — Personal Data. In the UK's Data Protection Act 1998, personal data is defined as:

> *"data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression*

> *of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."* [196]

Personal information is also defined in the Privacy Protection Act of Australia as: *"...information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not"* [197].
The key component of these definitions is identifiability which means that a certain level of personal information can be handled without legal implications as long as they are anonymized [198]. Consequently, any information that can reasonably be directly or indirectly linked to an individual's identity qualifies as a personal identifiable information (PII) and requires careful handling [199]. Information considered to be linkable to individuals includes medical, educational and financial records [200]. With this background, a decision was made to focus on measuring and comparing attitude towards 4 main types of personal data (Social Media, Personal Emails, Financial and Health records).

It was realized during the review of existing literature on personal data that, although the concept has now become a hot topic in the cybersecurity and privacy research community, much of the focus has been on developing technical and legal countermeasures. Studies exploring the individual behavioural elements of the concept are quite limited hence, information on the structure of personal data as a psychometric construct is very scanty. The majority of the literature exploring personal data attitude based their studies on health and/or medical records. Rindfleisch [201] for instance proposed and explained three concepts underlying health care information protection concerns – security, confidentiality, and privacy. Wellcome Trust [202] also measured and classified peoples' attitude to health data into identity, attention and control concerns.

Consequently, three major themes were initially identified in the literature as dimensions of public views to personal data. These include issues related to security, risk/benefit trade-off, and privacy/confidentiality. These dimensions mostly overlap with the eight underlying principles of the fair information practices outlined in the United States: PPSC [203] and the for Economic Co-operation and Development [204] reports. The attention concern described by [202], where users express mixed blessings about giving away their personal information, falls within the object of purpose specification principle. Thus, a user may give out personal information for an immediate benefit but may not be sure of the future implications of such an action. The principle of use limitation extends to the case where a user may be concerned about their identity being abused once their personal data is disclosed to access a service. The principle of collection limitation aims to addresse security and privacy concerns, by providing a framework for limiting the amount of specific PII that can be collected within specific contexts. Most definitions of privacy refer to people's ability to control the terms under which their personal information are acquired and used (e.g. [201, 205, 206]). Collection limitation is about having a limit to the collection of personal data and doing so in a legalized manner. The dimension of control is illustrated as a personal data concern with users' comments on losing their free will and not being able to go for 'opt-outs' as illustrated in the Wellcome Trust report.

The World Economic Forum [207] hosted a global dialogue on the emerging issues surrounding the collection and use of personal data by clustering the eight principles into three main themes: *"Protection and security, Accountability and Rights, and responsibilities for using personal data"*. Security here has to do with the integrity, availability and controlled access to information. This clearly encompasses the control concern identified by Wellcome Trust. The concept of confidentiality described by [201] directly overlaps with the principle of use limitations as they both have to do with the release of information when accessing a service (in this case health care) in a legal manner that limits the extent to which they may further be used or released. Rindfleisch [201] refers to privacy as the right and desire of a person to control the disclosure of personal health information. This description is very much synonymous to the general definitions of privacy identified in the literature as mentioned earlier.

Though there are limited studies attempting to measure attitude to personal data directly, several studies have explored privacy concerns. Smith et al. [208] developed the Concern for Information Privacy (CFIP) scale which identified and measured four factors (collection, errors, secondary use and unauthorized access to information) as the dimensions of a person's privacy concern about organizations. Malhotra et al. [209] later identified three aspects of information privacy namely: attitudes towards the collection of personal information, control over personal information and awareness of privacy practices. More recently, Hong and Thong [210], consolidated existing conceptualization of Internet Privacy Concerns (IPC) including [208] and [209] in their study and came up with six first-order factors of IPC – collection, secondary usage, errors, improper access, control, and awareness. When reviewing these IPC measurement instruments, this article focuses on the broader personal data ecosystem by identifying constructs that goes beyond privacy concerns to encompass other construct domains. Table 5.1 summarizes the construct domains generated from the review of existing literature pertaining to attitudes toward personal data.

5.3 Scale Development

This section describes the multi-stage scale development study conducted to develop a measurement instrument for APD. Fundamentally, the issues of reliability and validity underpin the development of an attitude scale right from item generation, the theoretical deduction of a factor structure and resulting psychometric analysis. Previous scale

TABLE 5.1: Potential Constructs of Attitude to Personal Data

Construct Domain	**Construct Definition**	**Relevant Literature**
Awareness	Conscious of issues surrounding the disclosure and use of personal data. Being aware of the general interest in personal data.	[202, 209, 211–214]
Collection	Concerns over the amount of specific types of personal data collected/disclosed within a specific context	[208, 209, 215]
Responsibility	The perception of who should be held accountable for the protection of personal data (individuals vs. data protection authorities)	[207, 216]
Cost-Benefit	Perceived risks and benefits of linking personal information disclosed to different kinds of data for different purposes. Thus, the positive or negative effects of sharing personal data in general.	[202, 207, 217]
Privacy/ Confidentiality	Perception of control concerning who can have access to one's personal information and the need for anonymity	[209, 217]
Protection/ Security	Perception of the relevance and adequacy of existing technical and legal protective measures to ensure integrity, confidentiality and reliability of personal data	[207, 217–219]
Exposure/ Experience	The impact of past experience with disclosure of personal data	[220, 221]
Protective behavior	Actual steps taken to demonstrate a positive attitude to personal data such as choosing to opt-out, adoption of cybersecurity measures etc.	[222, 223]
Interest	The level of attention or complacency exhibited towards personal data protection	[214, 224]
Sensitivity	the perception that a specific set of personal data will have damaging effect if exposed. The degree of risk associated to the disclosure of a personal data	[225, 226]

development studies as well as recommendations from [227] on how to improve the scale development process provided guidance for the research. Subsequently, an iterative process (see Figure 5.1) is adopted to assess the consistency of the scale items with the dimensions of personal data attitudes identified in the literature. This following sub-sections describes the procedures involved in developing and assessing the APD instrument.

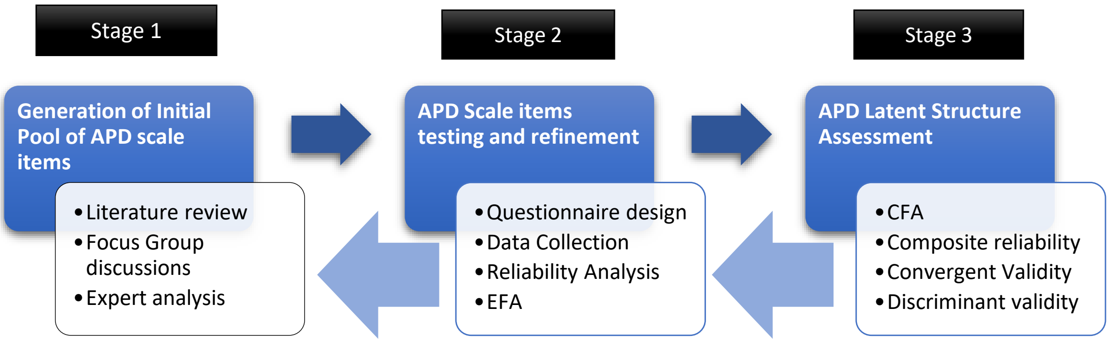


FIGURE 5.1: Iterative work-flow adopted for the APD measurement scale development

5.3.1 Generation of Initial Pool of APD Items

Following an examination of existing personal data related literature, definitions, and surveys (including [193, 219]), 50 Likert-type attitudinal items related to the 10 construct domains identified was generated. The items drawn from these sources were rephrased to mainly reflect attitudes towards four different types of personal data namely: Email, Social Media (online personal data); Financial and Health (offline personal records). Since we did not find a measurement scale specifically designed for attitude towards personal data in the existing literature, an exploratory study was conducted as a preliminary step toward generating the APD scale items. To ensure the content validity of construct domains predetermined from the literature review, focus group discussions were held using open-ended questions to elicit themes that constituted individuals' view on the four types of personal data. 50 additional items were generated based on responses emerging from the focus group discussion on personal data matters. This resulted in an initial pool of 100 items serving as the basis for the APD measurement. 64 items were eventually dropped following an exercise to merge similar themes and convert the 100 items into generic personal data statements. Thus, those that were obviously pointing to a specific type of personal data (e.g. I feel my profile information on any social media is much secured) were discarded.

5.3.2 Scale Specification and Refinement

The research team reviewed the remaining 46 items based on the 10 construct definitions in Table 5.1. Items from previous privacy related measurement scales were adapted to fit the APD context as much as it was possible to do so. Items generated for the Experience and Sensitivity construct domains were dropped as they were mainly measured with categorical rather than scale data in previous studies. To minimize the tendency of respondents agreeing with a statement or providing the same responses due to acquiescent response bias, some items were worded negatively. To do this the direction of each statement (positive or negative attitude to personal data) needed to be determined. Items that were categorized as unable to judge statements were discarded. For instance, we could not indicate whether a statement like 'I do not mind sharing such information with family and friends' is a positive or negative attitude towards personal data. Consequently, the items were further reduced to 34 APD statements.

Each of the items was a statement to which people were asked about their level of agreement on a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). Thus, attitude to personal data was quantified as a continuous variable. Questions relating to some of the theoretically distinct aspects of personal data discussed earlier were included. For instance, items relating to security/identity (e.g. 'There should be stronger laws to protect such personal data'), control/privacy (e.g. 'I consider the privacy policy of institutions where I give out such personal details') and possible benefits of surrendering personal data (e.g. 'I am happy to provide such personal details to support government policy and decision making'). The scale involved both positively and negatively worded items. To ensure that a higher numbered response on the Likert scale would represent positive attitudes, all negatively worded items were reversed before the data was analyzed.

5.3.3 Data Collection

A web-based questionnaire was developed based on the 34 APD items. The questionnaire had two main sections of demographics and the attitude to personal data items with four research design conditions (Personal Email, Social Media, Financial and Health data). Essentially participants were randomly presented the generic statements with respect to one of the four types of personal data outlined above until they were almost evenly distributed across the groups. A non-probability sampling approach was adopted to collect responses from participants over the internet. Email invitations and anonymous link to the survey was posted on social media sites (Facebook, Twitter and LinkedIn). To further expand the sample size, snow-balling and convenience sampling techniques were also used.

After several follow-up rounds, a total of 256 responses was received out of which 247 completed datasets was extracted at the data cleaning and preparation stage. Of the 247 respondents, 51.4% (127) were male and 48.6% (120) were female. The average age of the sample was 36 years (range: 17 – 67 years). As presented in Table 5.2, most respondents use Social Media (90.7%) out of which most of them preferred to use Facebook (47.8%). Respondents who have not had previous experience with personal information misuse formed a significant portion of the sample population (83%).

5.4 Analysis and Results

5.4.1 Reliability Analysis

The 34 items of the attitude to personal data measure were subjected to an iterative scale purification procedure. To determine the internal consistency of the items, the

TABLE 5.2: Participant demographics

Sample characteristic	**n**	**(%)**	**Sample characteristic**	**n**	**(%)**
Gender			Education		
Male	127	51.4	12th grade or less	11	4.5
Female	120	48.6	Associate degree	38	15.4
Total	247	100	Bachelor's degree	36	14.6
Age*			Graduate/ postgraduate	29	11.7
17-24	47	19	High school diploma	105	42.5
25-35	159	64.4	Some college (no degree)	28	11.3
35-67	41	16.6	Total	247	100
Total	247	100			
Average	36		Favorite Social Media		
Ethnicity			Facebook	118	47.8
African/ Black	58	23.5	Twitter	36	14.6
Asian/ Pacific Islander	49	19.8	None	23	9.3
Caucasian/ White	110	44.5	WhatsApp	20	8.1
Hispanic/ Latino	30	12.1	Instagram	15	6.1
Total	247	100	LinkedIn	12	4.9
			Others**	23	9.3
Uses Social Media (SM)			Total	247	100
Yes	224	90.7	Number of Email Accounts per participants		
No	23	9.3	1-3	163	66
Number of SM subscriptions per participants			4-5	71	28.7
1-2	129	52.2	6-7	13	5.3
3-4	74	30	Total	247	100
≥ 5	44	17.8	Had prior experience with personal data misuse		
Have Email Account			Yes	42	17
Yes	245	99.2	No	205	83
No	2	0.8	Total	247	100

**Given in years*
***Includes 10 different social media such as reddit, WeChat, youtube etc.*

most widely used reliability method of computing the Cronbach‘s alpha was adopted [228]. This yielded 0.926, indicating a high reliability of the 34-item scale. A correlation matrix generated with SPSS was scanned to check the pattern of relationships among the items. There is no singularity in the data as all the correlation coefficients were less than 0.8 [229]. Another commonly accepted procedure used to further assess the internal consistency of the items was the item-to-total correlations. A close look at the inter-item correlations and item-to-total correlations of each item revealed inadequate performance of some items. If the items are all measuring attitude to personal data, then each item ought to correlate with the total score from the questionnaire [230]. The correlation between participants' score on an item and the sum of their scores on all the items is represented by the r value. Three of the items that poorly correlated

$(r < 0.4)$ were removed from the APD items. This conforms to the generally accepted rule-of-thumb that item-to-total correlations should exceed 0.30 [231]. After deleting the items that fell below this standard, 31 items remained in the pre-final version of the questionnaire. The 31 items were then subjected to a separate reliability test. This resulted in an acceptable item-total correlation but the Cronbach alpha remained at 0.926.

5.4.2 Exploratory Factor Analysis (EFA)

An exploratory factor analysis can help to empirically determine how many constructs, or factors, underlie the set of APD items [230, 232]. To determine the appropriateness of the factor analysis, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity were first examined. The KMO value for the data set was 0.899 and Bartlett's Test of Sphericity was significant $(p < 0.000)$, indicating that the factor analysis was appropriate. The initial EFA analysis produced a pattern matrix consisting of seven factors based on Eigenvalues greater than one and accounted for 64.135% of the total variance. Only one item loaded on the 7th factor and most of the items generated for Protective Behavior and the Interest Scale were loading together. To minimize errors associated with under-extraction and/or over-extraction, a mixed approach based on both the eigenvalue and scree plot results was adopted. For instance, under-extraction error could lead to inconsistencies in the analysis and interpretation of the results [233].

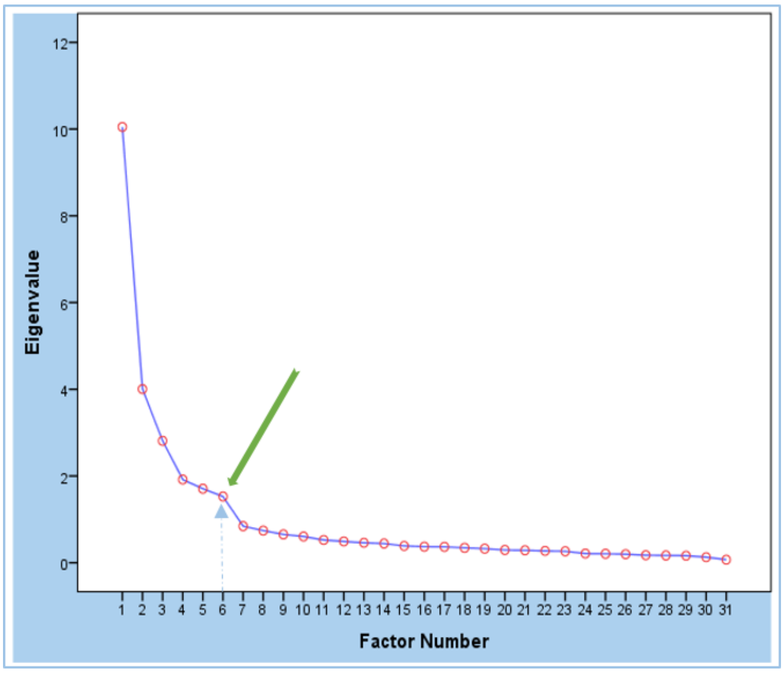


FIGURE 5.2: Scree plot of factors underlying the APD scale.

In effect, based on the initial factor extraction and the results from the scree test (Figure 5.2), the factor analysis was repeated to extract a 6-factor solution with an oblique rotation method to allow the obtained components to correlate (Table 5.3). This supports the assumption that APD dimensions are related yet distinct from each other [234]. The final six-factor model emerging from the 31 APD items explained 63.983% of the total variance. Factor 1 contained the items measuring protective behaviour and interest, while factor 2 focused on the items measuring privacy. Factor 3 involved the items measuring cost-benefit and factor 4 contained the items measuring awareness. Factor 5 consist of the items measuring responsibility, and factor 6 involve those items measuring security.

5.4.3 Assessment of the Factor Structure

Next, Confirmatory Factor Analysis (CFA) was conducted using AMOS 23 to examine the factor structure obtained from the EFA. Maximum likelihood parameter estimates were used to examine the model fit. Researchers are required to report several fit indices in order to characterize the fitness of a model correctly with the following boundary scores indicating good model fit — $\chi^2/df = 2.0–5.0, RMSEA < 0.06[< 0.05, < 0.08]$ and $CFI > 0.94$ [235]. Results of the CFA ($\chi^2/df = 1.802, RMSEA = 0.057$ and $CFI = 0.940$) indicate that the measurement model fits the data quite well. The 6-factor solution is therefore supported by the CFA results.

TABLE 5.3: APD Scale Items and CFA Results

Scale Items	Factor Loadings	SMC	CR	AVE
Protective Behavior/ Interest (BEH)			0.92	0.67
I always optimize my privacy settings when I create an online profile	0.90	0.81		
I consider the privacy policy of institutions where I give out such personal details	0.84	0.71		
I regularly look out for new policies on personal data protection	0.84	0.70		
I would opt out of a service due to privacy issues related to such data - **Recoded**	0.82	0.67		
I watch for ways to protect my personal information from unauthorized access	0.80	0.65		
I use security tools such as firewalls, encryption and other security settings to protect my private data	0.71	0.51		
Privacy/ Confidentiality Concerns (PRI)			0.91	0.63
I am concerned about my information online being linked to my publicly available offline data	0.88	0.78		
I'm concerned that too much personal information about me is being collected by so many organizations	0.82	0.67		
I worry about such information getting exposed - **Recoded**	0.81	0.66		
It usually bothers me when am asked to provide such personal information	0.80	0.65		
I am concerned about sharing such personal information because it could be used in a way I did not foresee.	0.74	0.55		

Continued on next page

Table 5.3 – *Continued from previous page*

Scale Items	**Factor Loadings**	**SMC**	**CR**	**AVE**
It usually bothers me when I do not have control over decisions about how my personal information is collected, used, and shared	0.67	0.45		
Cost-Benefit (COB)			0.93	0.73
The risk posed to me if such personal information is exposed outweighs the benefits of sharing it.	0.92	0.85		
In general, my need to obtain services is greater than my concern about privacy	0.87	0.76		
I am happy to provide such personal details to support government policy and decision making	0.84	0.70		
I value the personalized services I received from providing such personal data	0.84	0.71		
Such personal information can be used to victimize people - **Recoded**	0.80	0.64		
Awareness (AWA)			0.86	0.504
Such details about me are of value to external organizations	0.84	0.70		
Researchers need my consent to access my personal data - **Recoded**	0.78	0.61		
Service providers do not have the right to sell personal details of their users - **Recoded**	0.68	0.47		
Companies seeking information should disclose the way data is collected, processed, and used	0.68	0.46		
It usually bothers me when commercial/government organizations seeking such information do not disclose the way the data will be processed, used and secured	0.66	0.44		
It is very important to me that I am aware and knowledgeable about how my personal information will be used	0.59	0.35		
Responsibility (RES)			0.84	0.57
Responsibilities lie with data handlers to ensure consistent and helpful applications of use (and not abuse)	0.78	0.61		
Designated data protection authorities are responsible for ensuring such personal data are only processed in accordance with the data protection regulations	0.77	0.59		
I would welcome the opportunity to pay for the privacy of such personal details - **Recoded**	0.75	0.57		
I would prefer to be personally responsible for the security of such personal data - **Recoded**	0.73	0.53		
Security (SEC)			0.85	0.59
I am concerned that databases that contain my personal information are not protected from unauthorized access	0.78	0.61		
I worry about wrong information being linked to my identity due to security breaches	0.77	0.59		
I worry about such information getting missing due to lack of adequate security measures	0.77	0.59		

Continued on next page

Table 5.3 – *Continued from previous page*

Scale Items	**Factor Loadings**	**SMC**	**CR**	**AVE**
I believe stronger security measures are required to ensure the correctness of such personal information	0.74	0.55		

As shown in Table 5.3, the reliability of the APD scale is supported by the composite reliability (CR) estimates (> 0.7) ranging from $0.84to0.93$, indicating a good internal consistency of the multiple items for each construct in the model. The convergent validity was evaluated by checking all the values of average variance extracted (AVE) and the factor loadings. As shown in Table 5.3 the estimated AVEs of all the APD dimensions were all greater than the unexplained variances (> 0.5) and all the factor loadings for the six constructs were above 0.5 and were significant for the individual items. The examination of the AVEs together with the factor loadings therefore confirmed the convergent validity of the APD latent constructs. To investigate the discriminant validity of the APD scale, the suggestions provided by Bertea and Zait [236] regarding use of AVE analysis were followed. Accordingly, the value of the AVE for each construct should be at least 0.50 and the square root of each construct's AVE should be much larger than the correlation of the specific construct with any other constructs. The results from the AVE analysis presented in Table 5.4 show that the shared variance between any two constructs was not greater than the square root of the corresponding AVEs. In summary, the assessments carried out to verify the measurement model yielded evidence for the reliability of the latent constructs.

TABLE 5.4: APD Factor Inter-correlations

Constructs	**BEH**	**PRI**	**COB**	**AWA**	**RES**	**SEC**	**M**	**SD**
BEH	0.82						4.01	0.59
PRI	0.40*	0.79					3.51	0.79
COB	0.27*	0.18*	0.86				2.32	0.84
AWA	0.41*	0.53*	0.47*	0.71			2.94	0.71
RES	0.32*	0.19*	0.51*	0.34*	0.76		2.80	0.85
SEC	0.60*	0.53*	0.24*	0.50*	0.29*	0.77	3.95	0.58

* *Correlation is significant at the 0.01 lever (2-tailed)*

5.4.4 Analysis of Variance

The data was also analyzed to determine whether there are differences between the four types of personal data. A series of Multivariate Analysis of Variance (MANOVA) was performed using factor scores for participants' responses on the six constructs identified above as the dependent variables (DVs); and type of personal data (Email, Health Data, Financial Records and Social Media), prior experience (Figure 5.3) and sensitivity responses (Yes and No) as the independent variables (IVs). — see Figure 5.4. Bartlett's approach was used to compute the factor scores in SPSS to obtain unbiased

TABLE 5.5: Multivariate ANOVA done on the factor scores for the 6 APD constructs across 4 types of personal data

	Value	F	Hypothesis df	Error df	Sig.
Pillai's trace	0.132	1.759	18	690	0.026 p<.05
Wilks' lambda	**0.873**	**1.77***	**18**	**645.367**	**0.025 p<.05**
Hotelling's trace	0.141	1.778	18	680	0.024 p<.05
Note:	Each F tests the,multivariate effect of Type of Personal Data. These tests are based on the,linearly independent pairwise comparisons among the estimated marginal means.				

* *Wilk's lambda and the difference is significant*

estimates of the true factor scores [237]. As shown in Table 5.5, the multivariate test using WilksLambda revealed an overall significant effect for data type as an IV on the DVs $(F = 1.77)$ at $p = 0.025(p < 0.05)$. Univariate analysis for the effect of type of personal data in the survey, presented in Table 5.6, significantly predicted responses related to Behavior $(p < 0.05)$ and Privacy Concerns $(p < 0.05)$. Finally, post hoc testing (with Least Significant Difference (LSD)) revealed highest Protective Behavior scores for Health Data (mean = 24.87, SD = 3.03) and Email (mean = 24.19, SD = 3.44), with Health Data being significantly higher (at $p < 0.05$) than Social Media (mean = 23.51, SD = 3.72). No significant mean difference in Privacy Concerns scores were obtained between the four types of personal data but the highest score was for Financial Records (mean= 21.58, SD= 5.16). The implications of these findings are discussed in the next section.

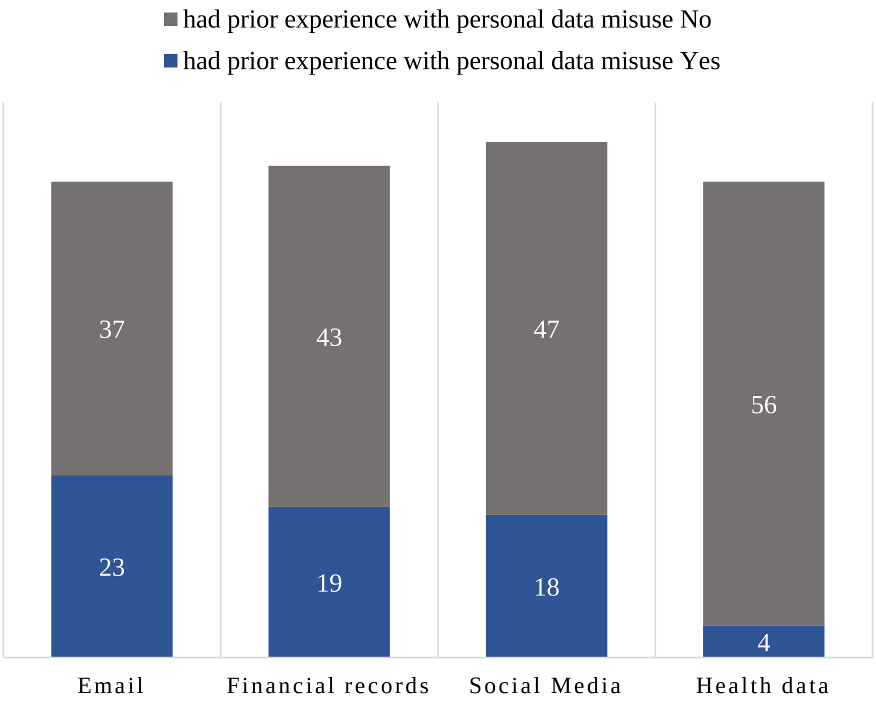


FIGURE 5.3: A frequency distribution of responses per personal data type and prior misuse experience

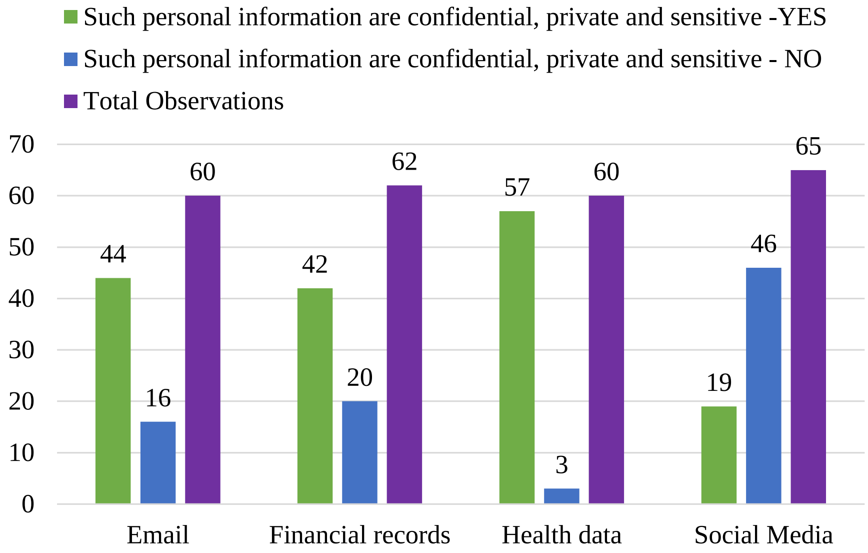


FIGURE 5.4: A frequency distribution of responses per personal data type and perception of sensitivity of data type

TABLE 5.6: Univariate Test done on each of the 6 DVs for the types of personal data

Dependent Variable		Sum of Squares	df	Mean Square	F	Sig.
Dimensions of APD	**Behavior**	**8.624**	**3**	**2.875**	**2.887**	**0.036**
	Privacy	**9.478**	**3**	**3.159**	**3.042**	**0.03**
	Cost_Benefit	0.42	3	0.14	0.133	0.94
	Responsibility	3.733	3	1.244	1.128	0.338
	Security	7.224	3	2.408	2.073	0.105
Note:	The F examines the effect of Type of Personal Data. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.					

5.4.5 Cluster Analysis

To identify homogeneous groups in the dataset, we used a TwoStep clustering approach to cluster participants based on the six APD factor scores computed. TwoStep Clustering was chosen due to its ability to automatically determine the optimal number of clusters in the dataset using an agglomerative hierarchal method [238]. BIC (Schwarz's Bayesian Information Criterion) was used first to determine the number of clusters, then AIC (Akaike's Information Criterion) was used. Table 5.7 summarizes the results obtained with BIC, which do not differ from those obtained with AIC. The cluster centroids facilitated interpretation of the resultant cluster solution. The resulting clusters are labelled based on the Protective Behavior (BEH) factor which happens to be the overall important predictor variable (see Figure 5.5). The first cluster, which is the largest (57.9%), contains participants with responses indicating a general privacy consciousness (mean Privacy factor $score = 0.11$) and a somewhat protective attitude towards their personal data, with a mean score of 0.06 on the BEH factor. The second cluster contain 23.9% of the total participants with responses indicating high Awareness on Personal Data issues, and obtained the highest mean score on the BEH factor (0.84). The third cluster is the smallest (18.2%) and consist mainly of participants whose responses indicate a general lack of interest in Personal Data related issues, and scored the lowest on all six APD factors, especially on BEH $(Mean = -1.30)$.

TABLE 5.7: Cluster distribution with cells showing cluster centers sorted by within-cluster membership predictor importance

Cluster	**1**	**2**	**3**
Label	**Protective**	**Very Protective**	**Not Protective**
Description	Respondents' highest factor score was on Privacy but very low on Awareness, Cost_Benefit and Responsibilty	The respondents scored highly on all 6 factors especially on Awareness	Respondents in this cluster scored negatively on all six factors especially on Awareness
Size	57.9% (143)	23.9% (59)	18.2% (45)
Inputs (APD Factors and Mean Scores)	Cost-Benefit -0.15	Awareness 1.01	Awareness -1.17
	Responsibility -0.16	**Behaviour** **0.84**	**Behaviour** **-1.30**
	Privacy 0.11	Responsibility 0.97	Cost-Benefit -0.85
	Security 0.08	Cost-Benefit 1.00	Privacy -1.13
	Behaviour **0.06**	Security 0.66	Security -1.12
	Awareness -0.05	Privacy 0.58	Responsibility -0.77

The cluster centers presented in Table 5.7 are sorted to highlight the within-cluster predictor (APD Factors) importance while Figure 5.5 highlights the overall cluster membership predictor importance. A multivariate analysis conducted using the clusters as independent variable and the six factors as dependent variables shows significant differences in personal data attitudes across the segments $(Wilks'lambda = 0.196, p > 0.000)$. The results of a univariate F test revealed the clusters were significantly different on all APD segment predictor factors. The discriminant analysis conducted based on the three clusters indicated that the model could correctly classify 94.3% of respondents into groups.

5.5 Discussion

This study aimed to establish the dimensions required for the development of a reliable and valid APD measurement scale. An APD scale was successfully developed and verified based on the iterative scale development procedure adopted. Although the focus of this study was on attitude to personal data, the scale development process included an examination of both privacy and personal data literature and the related regulations. The research results show that six constructs (Protective Behavior/Interest, Privacy, Cost-Benefit, Awareness, Security, and Responsibility) are important components capable of differentiating individual's attitude towards personal data. The reliability

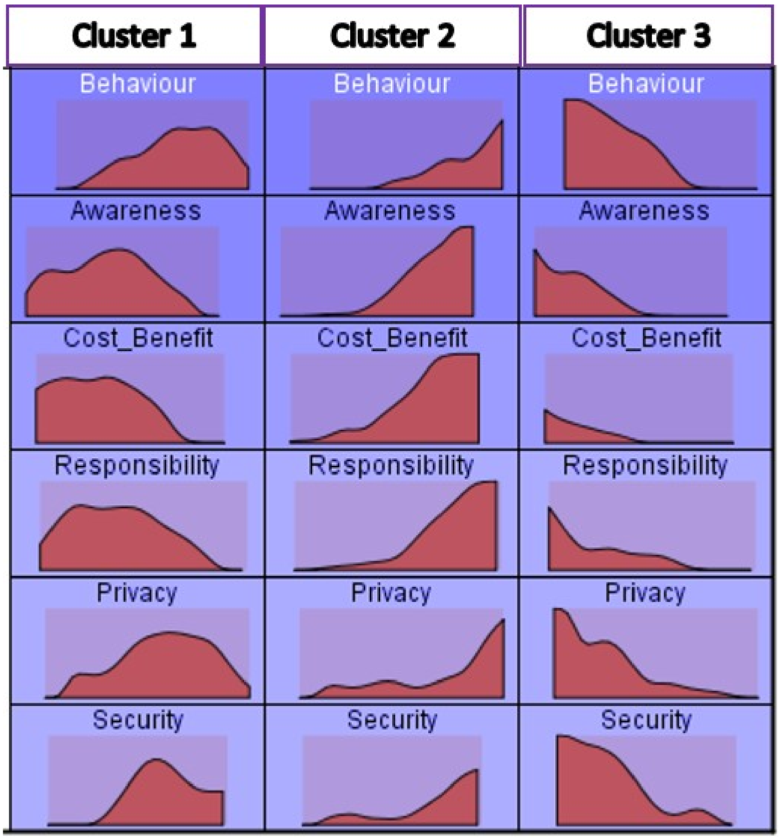


FIGURE 5.5: Comparison of the relative distribution of APD Factor Scores sorted by overall cluster membership predictor importance for the three clusters

analysis yields support for the APD scale's ability to reliably measure individual differences. The MANOVA results show that individuals' attitudes may vary based on the type of personal data. The results also suggest that participants who provided responses to the scale items based on health records generally viewed this data set as sensitive, and tended to score higher on the protective behavior construct. Conversely, those who provided responses in relation to their personal social media profile data mostly did not view it as sensitive and tended to score the lowest on both protective behavior and privacy concerns. Interestingly, there were a lot more social media participants who had had prior experience with personal data misuse (18) as compared to health data participants (4) – see Figure 5.3.

The study also examined the relationship between the six extracted factors. Overall, the strongest relationship existed between the construct of Privacy concerns and Awareness as well as Privacy and Security. Thus, Privacy correlates positively and reliably with both attitudes relating to Awareness and Security concerns. A possible interpretation here is that people who are more concerned about their privacy being breached tend to be more aware of the potential value of their personal data, and the risk factors associated with it. In general, all the constructs correlate significantly with each other. Notwithstanding the assumption that each construct measured completely different aspects of individuals' personal data attitude, the level of correlation between them is an indication of the conflicting conceptions people generally have on the subject.

The results from the cluster analysis show that, despite the diversity in attitudes towards personal data, there is a relatively small number of compatible groups of users sharing similar attitudes and behaviours. Research reported by Norberg et al. [239] and Sato [240] indicates that even though consumers express concerns for their personal data, they generally do not take enough protection measures towards it. Acquisti and Gross [241] also compared stated attitudes with actual behaviours of members of online social networks (OSNs) and found that reported privacy attitudes did not correlate with the probability of disclosing certain type of information on OSNs. Perhaps an exploration of the APD constructs may assist researchers in examining the relationships between individuals' personal data concerns and their claimed personal interest and protective behaviours. For example, 91% of the participants in the study conducted by Sato [240] indicated the need for a system that will enable them to control how their data is used. Meanwhile, researchers report fewer people actually adopting existing security and privacy mechanisms to protect their personal data online [242, 243]. The research findings by Shelton et al. [243], Rainie and Madden [244] highlight usability and lack of awareness of existing security mechanisms as the two main factors hindering people's ability to be more actively involved in the protection of their personal data and privacy. The usable security and privacy research community could, therefore, identify specific modifications of personal data attitudes, behaviours and skills that can foster a more positive appreciation for personal data through an in-depth exploration of the constructs identified.

The findings mostly reflect the underlying themes explored through studies that focused on personal data, rather than those centred on privacy concerns. Thus, whereas privacy measurement scales tend to focus on constructs such as collection, control, errors, authorized use and awareness of privacy practices, the personal data literature is more concerned with issues relating to security, availability, privacy, risk, and benefits. For instance, Kobsa [245] suggest that although consumers appreciate the benefits of user profiling and personalization, they are not willing to be profiled due to privacy concerns. Sato [240] on the other hand, surveyed about 3,000 people from six different countries and concluded that even though people are generally concerned about the privacy of their data, they are more positive about the potential benefits which they would normally weigh against the risk. Accordingly, when the benefits outweigh the perceived risk, cloud services users become more open to the data sharing concept. Although most people now accept that life in the digital age involves disclosure of personal data, concerns remain about the actual use of the data [242]. However, as Acquisti et al. [246] pointed out, because the experience individuals may have when their personal information is exposed may differ, their concerns about the use of their personal data also tend to vary. An APD scale will, therefore, be required to capture these individual differences to enable more representative user-models for the design of cybersecurity tools.

The findings of the study have implications for both research and design practices in the field of usable security and privacy. Since little prior research exists specifically on scale development for APD, this study signifies the first empirical examination of the concept. Existing instruments attempting to assess attitudes towards personal data are mainly based on a privacy-focused design which have produced a variety of attitudes ranging from one to six dimensions. Although there are significant similarities in the attitudes between privacy and personal data, privacy instruments tend not to relate specifically to attitudes towards what people may view as personal information. Information privacy, one of the most vital aspects of privacy, is concerned with protecting the personal data of individuals. However, the range of potential implications in relation to the collection and sharing of personal data goes beyond the issue of privacy and includes constructs related to responsibilities, security, risk, and benefits as explored in this study. All stakeholders within the digital economy, need to carefully consider these dynamics to ensure that they understand and are willing to accept the risk reward balance of personal data ecosystem [247].

The study makes a major contribution to the growing body of literature on user modelling in the field of information security by highlighting the potential of including APD as a determinant in predictive user models necessary for the design of adaptive cybersecurity. As indicated earlier, there is relatively little research literature on attitudes towards personal data that deal specifically with how individuals view the construct of personal data. There is therefore relatively little information available to guide designers in addressing personal data issues when designing new interfaces and technologies. A lot of new technologies and services have implications for how personal information is handled and how people react to them. Therefore, the existence of an instrument such as the APD scale has the potential for distinctively detecting attitude profiles of technology users that can be very useful for adaptive cybersecurity designs. Essentially, the six factors identified produced a framework around which personal data discussions and models might be developed by HCI researchers and information system designers. Thus, human factor engineers and designers may find such a tool very useful in looking to personalized interfaces where personal data issues are pertinent.

Although the findings presented in this report form an effective first draft of a personal data attitude instrument, several limitations of the study need to be highlighted. Notably, the convenience and accidental sampling methods adopted may limit the external validity of the findings. This preliminary data has however been used to provide empirical evidence in support of the APD scale's potential to be a valuable cybersecurity research and design tool. However, further research work need to be carried out with different types of populations, to establish the external validity of the APD instruments. An extended data collection is also necessary for the corroboration of the clusters that emerged. Nevertheless, the primary contribution of this work is to demonstrate the feasibility of segmenting users based on their attitude towards personal data among other determinants.

5.6 Chapter Summary

In this chapter, an initial development of an Attitude to Personal Data (APD) measurement instrument based on established psychometric principles is presented. The aim of the research was to develop a reliable measurement scale for quantifying and comparing attitudes towards personal data that can be incorporated into cybersecurity behavioral research models. Such a scale has become necessary for understanding individuals' attitudes towards specific sets of data as more technologies are being designed to harvest, collate, share and analyze personal data.

An initial set of 34 five-point Likert style items were developed with 8 sub-scales and administered to participants online. The data collected were subjected to Exploratory and Confirmatory factor analysis and MANOVA. The results are consistent with multi-dimensionality of attitude theories and suggest the adopted methodology for the study is appropriate for future research with a more representative sample. Factor analysis of 247 responses identified six constructs of individuals' attitude towards personal data: Protective Behavior, Privacy Concerns, Cost-Benefit, Awareness, Responsibility, and Security. The usefulness of the APD scale as a guide for information security research and design is also illustrated. Thus, the factor structure of the APD and related results are well discussed. Consequently, the study presented in this chapter addresses a genuine gap in the research by taking the first step towards establishing empirical evidence for dimensions underlying personal data attitudes. It also adds a significant benchmark to a growing body of literature on understanding and modelling computer users' security behaviours. In summary, the findings are believed to provide two major contributions to information security research and design practices:

1. a framework describing the primary dimensions of individuals' attitude towards personal data; and
2. an instrument that can easily be modified and used to measure those concerns and preferences for adaptive security designs.

The evaluation presented in this chapter is the first step toward developing a robust empirical evidence of the APD dimensions. Future research with more broader samples are required to replicate the factor structure and validate inferences that can be made based on the APD scores. Variables like, technology users' personal data attitude change overtime and the underlying factors such as local context and/or cultural differences, could then be examined within a single integrated analysis using machine learning techniques and structural equation modelling. The findings from this study are thus incorporated into the predictive modelling for personalized adaptive cybersecurity presented in Chapter 6.

CHAPTER 6

Modelling Behaviour for Adaptive Cybersecurity

Contents

6.1 Chapter Overview

This chapter describes the study conducted based on the research model proposed in Chapter 3. The study combines and applies behavioural science and machine learning techniques to better support user modelling in personalized adaptive cybersecurity applications. The integrated model of cybersecurity adoption proposed in chapter 3 is thus tested to determine influential factors which will impact on acceptability of web browser security controls (WBSC). Partial Least Squares Structural Equation Modelling (PLS-SEM) is applied to analyse empirical data collected using an online questionnaire-based survey. The empirical data and findings from the PLS-SEM model then serve as input for building the Bayesian-Network (BN) models for personalized adaptive cybersecurity (PAC). Thus the empirical experimentation with PLS-SEM assisted in determining which variables should be considered to support the personalization capability of the BN. The resulting components and structure of the Bayesian-network-based model illustrate how cybersecurity assistance can be intelligently provided.

6.2 Related Work

Factors affecting the acceptance of various computer technologies has been a central research focus on the implementation of computer systems. Davis et al. [248] determined that resistance to computer technologies aimed at increasing performance can be assessed and addressed with predictive behavioural models. This has led to the development of differing models aimed at verifying the effect of identified factors on the acceptance of different kinds of technologies. These factors can be broadly categorised as individual, contextual and system characteristics. In one of the earliest studies conducted to measure user acceptance of information technology, the functional and interface characteristics of an electronic mail and a text editor had a significant direct effect on attitude towards usage [249]. According to Calisir et al. [250], system characteristics such as security, reliability and speed as a measure of system quality influence expectation of quality user experience, hence increasing users' perceived ease of use. To determine factors influencing the use of decision support systems (DSS), Fuerst and Cheney [251] considered differing characteristics involving the decision maker (user demographics), the system itself (performance and quality of output) and contextual factors related to the organization within which the system is being implemented (e.g. management support, training, etc.). They found at least one variable from among the three characteristics mentioned mediated the use of DSS. To investigate the determinants of End-User Computing effectiveness in an organization, Igbaria [252] considered both individual and organizational (contextual) characteristics.

In the field of computer and information security, most studies focus on exploring factors influencing the acceptance of security policies and solutions within an organizational context. Topa and Karyda [253] recently reviewed the prevailing literature on employee security behaviour and classified the factors influencing them into individual, organizational and technical. Accordingly, organizations aiming to improve security policy compliance will need to adopt a holistic approach that addresses issues related to all three category of factors. Promoting the development of healthy security habits through training and awareness programs will help address individual factors influencing security compliance within organizations. Addressing organization factors entails the provision of appropriate support, deterrence and resources required to facilitate employees' access to information security policies and implementation through technical security mechanisms. Home computer users may, however, not be able to access these mitigating supports to enable them improve their information security behaviour. It is therefore critical to assess and ensure the usefulness as well as user friendliness of security tools developed for security inexpert users. In non-corporate environments, technical factors influencing security behaviour includes quality, performance and usability of the technological controls. Consequently, it is becoming increasingly important to focus on making the use of computer security tools effortless. The user model proposed and evaluated in this study for personalized adaptive cybersecurity, is geared towards this goal of effortlessness.

Recently, researchers have shown an increased interest in understanding users' security behaviour not only in the context of an organization, but within non-corporate settings as well. Omidosu and Ophoff [254] highlighted the need for more studies into the security behaviours of non-corporate computer users following a systematic review of the extant literature on information security behaviour in both organization and home context. Thus, far too little attention has been paid to the study of security behaviour of home computer users. As a result, a considerable knowledge gap exists where the security behaviour of individual cyber citizens operating within non-corporate context is concerned. Findings reported in this chapter fill some of that gap by incorporating empirical evidence for actual cybersecurity related attitudes and behaviours into the development of user models for personalized adaptive cybersecurity.

6.3 Theoretical Framework for Propositions

The Predictive Model of Cybersecurity Behaviour examined in this study is presented in Figure **??**) Two prominent models designed to predict specific security behaviour are the Technology Acceptance Model (TAM) and the Protection Motivation Theory (PMT) [255]. The proposed research model integrates components from both these theories, and includes other factors found to be possible determinants such as value for personalization and attitude to personal data. The model consists of three main components (External Variables, User Perception and Cybersecurity Behaviours), which are used to explore how the identified external variables may influence perceived ease of use (PEOU), perceived usefulness (PU), perceived risk (PR), value for personalization (VFP), and attitude to personal data (APD); and how these can then predict an individual's cybersecurity intentions (BI) and actual cybersecurity practiced and/or behavior (ACB). The ensuing paragraphs provide justification for the inclusion of these determinants in the research model and related propositions.

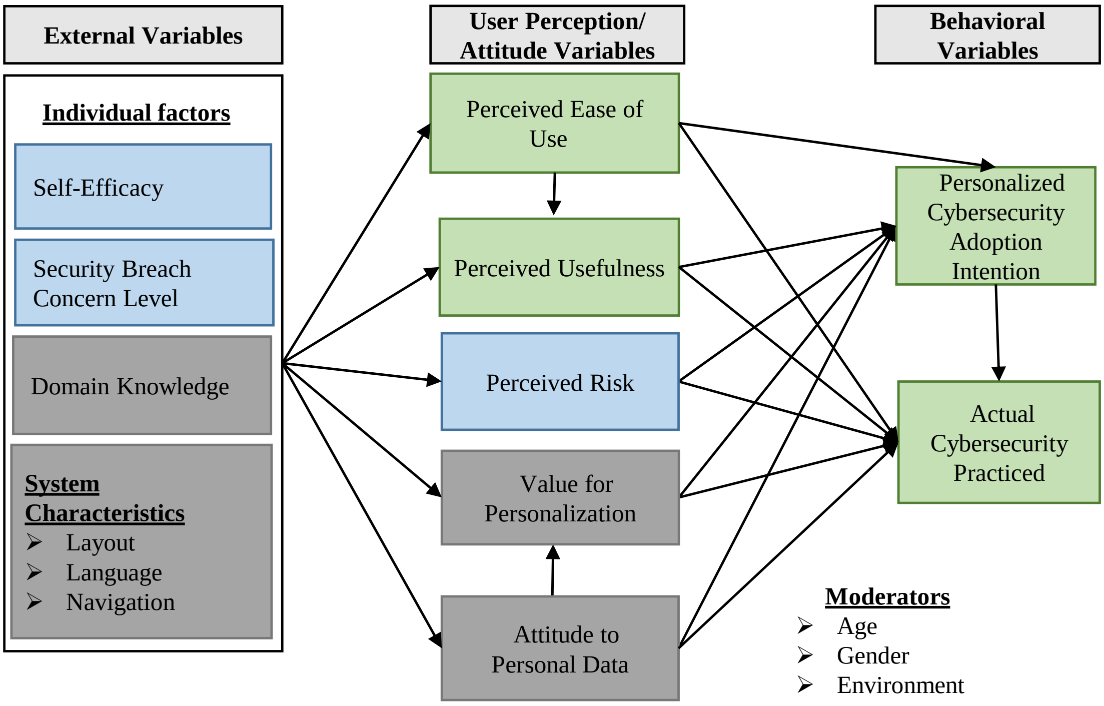


FIGURE 6.1: Predictive model for user cybersecurity behavioural Intentions

6.3.1 Proposition Set 1: User Perceptions

Beliefs that users have about the usefulness of systems and their ease of use affect intention to use and usage of the actual system. These perceptions have been extensively explored in previous technology acceptance research and provide support for the following propositions with regards to web browser security controls (WBSC).

6.3.1.1 Perceived Usefulness (PU)

- *H1: PU of WBSC is positively related to cybersecurity behaviour*

In the TAM, perceived usefulness refers to an individual's intrinsic belief about job related benefits such as productivity, effectiveness and performance associated with using a new technology. In the context of this research, PU refers to the degree to which a person believes web browser security settings would improve their protection against cyber-attacks. This definition captures both PU in the TAM model and response efficacy in the PMT model. Perceived usefulness has been reported to have positive impact on the adoption and usage of information systems [96, 256, 257]. Woon et al. [257] found response efficacy (similar to perceived usefulness) significantly impacted home computer users decision to protect their wireless network. Jeyaraj et al. [258] reviewed and analysed empirical studies conducted on IT innovation adoption in the past decade and found perceived usefulness to be the best predictor for behavioural intention. The proposition here is that, users are more likely to adopt security measures if they believe the security mechanism provided (in this case web browser security settings) are effective in making them cyber-secured.

6.3.1.2 Perceived Ease of Use (PEOU)

- *H2: PEOU of WBSC is positively related to cybersecurity behaviours*
- *H3: PEOU of WBSC is positively related to PU*

PEOU refers to an individual's perception of the cost in terms of time, mental and physical effort involved in using a system [96]. In previous studies, PEOU has been found to have both a direct and indirect effect on behaviour through its impact on PU of the technology being investigated. Suh and Han [24] also discovered that both security concerns and usability dimensions together have direct and indirect significant effects on the adoption of smartphones for internet banking. Thus PEOU can influence users attitudes towards a system application as well as their perception about the application's usefulness during use hence impacting on behaviour both explicitly and implicitly [96, 117, 259]. In the context of digital security, Ellis [260, p. 41] noted that *"if security systems are burdensome, people may avoid using them, preferring convenience and functionality to security"*. There is also empirical support for response cost (similar to PEOU) having a significant negative impact on intention to enable security settings on a wireless network [257]. It is therefore posited that security applications that are difficult to use and require a lot of effort to accomplish tasks efficiently will most likely be ignored and/or undervalued by users.

6.3.1.3 Perceived Risk (PR)

- *H4: PR about WBSC is negatively related to cybersecurity behaviour*

Threat appraisal is a key aspect of the PMT, and refers to the beliefs that individuals form about perceived risk when they become aware of security threats. Their perceived risk is then evaluated against the effectiveness of the coping mechanisms that are made available. PMT includes rewards, severity and vulnerability to explain how threats are perceived. In the model, rewards are considered similar to PU and PR as the degree to which a user feels the uncertainties and negative effects of configuring some web browser security settings in areas of functional, time, information, physical and social risks [112]. Perceived risk is considered to be a multi-dimensional construct in the literature consisting of different types of risk (e.g. physical, functional, social, etc.) [112, 261, 262]. This study examined only five types of risk that are considered to be most relevant in the context of security technology adoption. Functional or performance risk describes the potential ineffectiveness of a security mechanism, hence failure to achieve the desired security goals. Time risk refers to the perceived time lost that may occur due to difficulty in configuring some security settings correctly. Information risk is the likelihood that instructions regarding the correct use of the security mechanism is inadequate/unreliable (risk associated with information failure or asymmetric information). Physical risk means the extent to which an individual believes adopting the security technology can protect them against some form of loss, such as data, privacy or any component of the computer system (e.g. hard disk). Social risk describes the possibility that an individual may be worried about losing their reputation in a social group due to the adoption of a security control or technology.

Perceived risk has received considerable attention as a key predictor of consumer behaviour within the marketing literature (e.g.[263–265]). The construct has also been integrated into various predictive models and has been found to have significant impact on technology adoption behaviour (e.g. [266–269]). However, far too little attention has been paid to it as a possible predictor of cybersecurity behaviour. Lu et al. [112] examined perceived risk in their empirical study and found that it impacted on intention to adopt an Online Anti-Virus through PU and Attitude towards use. More recently, Chang [270] proposed an extended TAM model that includes risk-related factors for the prediction of managerial attitude towards the adoption of security technologies within an organisation. Based on findings of significant effects of PR in previous technology adoption studies, the proposition follows that, computer users perceiving high risk associated with WBSC will have a negative attitude towards cybersecurity in general.

6.3.1.4 Value for Personalization (VFP)

- *H5: High VFP will positively affect intention to adopt personalized adaptive cybersecurity*

Personalization is the adaptation of services or products to the needs and/or preferences of a user. Whereas adaptive systems can be built to suit a categorized group of users, personalization takes it further to a more individual level. A number of online vendors now provide personalized products and services through online profiles of their consumers (e.g. eBay, Dell, Amazon etc.). Different machine learning techniques are adopted in constructing these consumer profiles to facilitate the provision of personalized products and services [271–273]. In marketing/e-commerce, personalization has been recognized as a significant influential factor in various consumer behavioural models (e.g.[272, 274]). User-specific profiles allow online vendors to relate to their customers on individual basis, leading to improved customer satisfaction and loyalty. From the online users' point of view, however, the overall benefit of creating an online profile is the convenience of having different parts of their browsing experience personalized. Personalization can contribute to the effectiveness of technical security controls through improvement of user interactions and experience with the system. The nature of personalization may however differ for different types of user experience based on the context within which user profiles are defined and techniques used to create them. VFP in this study refers to the level of appreciation that a user has for all types of personalization possibilities within cyberspace. Because personalization is regarded as an important determinant of user experience and usage, assessing its significance within the structural model of a comprehensive set of other possible determinants of cybersecurity behaviours is imperative. The assumption here is that users who generally have positive attitudes towards the different types of personalized products and services available on-line are more likely to accept and use personalized adaptive cybersecurity.

6.3.1.5 Attitude to Personal Data (APD)

- *H6: APD is positively related to cybersecurity behaviours.*

The construct of personal data and how it is perceived by individuals are identified in this research as critical components in explaining and predicting individuals' attitudes towards cybersecurity. Security in the digital world is often argued to be concerned with three main goals: confidentiality, integrity and availability. The confidentiality aspect of security is a basic privacy goal, and is concerned with the prevention of unauthorised access to sensitive data [89]. Because personal data is a common factor underlying the constructs of both security and privacy [275], this thesis argues that, individuals' perception of it influences security related behaviour [276]. APD here refers to the value people place on their data, and their tendency to adopt measures to protect it. It appears that many people now recognize and accept that an increasing part of life in the digital age involves disclosure of personal data. This does not, however, void the concerns that people may have about the actual use of the provided data [277]. Haddadi et al. [278] highlighted the complex nature of personal data as a construct and how users' preferences and concerns differ based on context and sociological factors. To aid the inclusion of APD in cybersecurity behavioural research models such as ours, the study presented in Chapter 5 first explored APD dimensions to produce a measurement scale for personal data attitudes [279]. Based on findings from that study, it can be assumed that users who are generally protective towards their personal data are more likely to adopt cybersecurity measures.

6.3.2 Proposition Set 2: Moderating effects of external factors

Moderators are variables that modify the direction or strength of relationships between independent and dependent variables in a predictive model. Moderating variables alter relationships through interaction with either endogenous or exogenous variables, or by reallocating the error terms. Moderating factors have been shown to be very significant in various technology acceptance models as they can potentially improve the predictive validity of a model under investigation [118, 280]. Moderators may also account for inconsistent factor findings in various user technology acceptance models

[281]. Sun and Zhang [281] examined the moderating effects in technology acceptance models and concluded that the exclusion of important moderators reflecting individual and contextual differences may account for lower explanatory power (predictive validity) and factor inconsistencies in previous findings. Accordingly, models that are extended with moderators such as gender, experience and cultural background, are more able to capture the intricacy of complex contexts. Prior empirical studies have identified several moderating factors involving differences in individual, organisational, cultural, context and system characteristics. In this study moderating variables reflecting individual differences, contextual factors and system characteristics are examined.

6.3.2.1 Individual Differences

- *H7: Demographic profile of cybercitizens will moderate the relationship amongst the constructs of the proposed predictive model for cybersecurity behavioural intentions.*

The acceptance and adoption of cybersecurity technologies may vary from one individual to another depending on differences in their characteristics. Individuals differ in terms of personality, level of experience, cognitive characteristics, background, and other demographics. Various aspects of individual differences have been examined in previous research. The importance of understanding individual differences and how they impact on cybersecurity performance cannot be over emphasized. Most studies have only considered a limited number of the variables pertaining to individual differences. A need for a holistic approach to cybersecurity user modelling that examines the relations between various aspects of individual differences and cybersecurity related factors thus remains.

This study explores a wider variety of these individual characteristics and examines their impact on the perceived risk, usefulness, ease of use and attitude to personal data within the context of cybersecurity. As observed already, TAM is based on the fundamental principle that user perceptions mediate the influence of all other external factors that may influence technology acceptance and usage. Individual variables of interest that can be reliably measured alongside other variables are identified in this research model guided by a taxonomy of individual difference variables from previous research [282, 283]. Consequently, individual difference variables in the model both cover the categories of demographics (age, gender, and environment) and examine the descriptive characteristics of domain knowledge (DK), self-efficacy (SE) and users' security breach concern levels (SBCL) as external variables impacting on behavioral intentions towards cybersecurity.

Demographic Variables. Age has been found to moderate various factors in technology adoption and usage in the workplace [284]. In the area of cybersecurity, netizens between the ages of 18 and 25 were found to be more susceptible to phishing than other age groups [285, 286]. The existence of gender differences in perception attributes has also been confirmed with a variety of IS diffusion models including TAM [287]. Shin [288] also examined and found significant moderating effects of demographics variables, including income, on relationships in their Unified theory of acceptance and use of technology (UTAUT) model for mobile payment. More recently, Anwar et al. [289] observed gender differences in perceived computer security aptitudes and found that among employees from different organizations, men scored higher on self-reported cybersecurity behaviour than women. Consequently, three main demographic moderators (age, gender, and environment) are included in the study analysis to examine the moderating effects of internet users' demographics on cybersecurity behaviour.

Descriptive Characteristics SBCL and SE are PMT constructs adapted to examine the mediating effects of a participant's protection motivation on cybersecurity behaviour. In PMT, a person's protection motivation is derived from two cognitive appraisal processes — threat appraisal and coping mechanisms. Apart from PR, fear arousal (the level of concern invoked by the threat) also captures threat appraisal within PMT models. An Individual's assessment of the probability and consequences of a security threat is externalized as a security concern in this study. SBCL therefore refers to the degree of security threat an individual feels exist towards their personal safety online. The more convinced a user is about cybersecurity threats posing a significant damages to their personal digital assets, the more concerned they will be, resulting in a more positive attitude towards protection mechanisms. Hence we can assume that:

- *H8: High SCBL will positively influence attitude towards cybersecurity.*

Several studies have examined self-efficacy by integrating it with TAM (e.g.([132–134, 290]). Chau [131] for instance, incorporated computer attitude and self-efficacy into the original TAM as external variables affecting perceived usefulness and ease of use. Related research into security behaviours finds support for the prediction that high self-efficacy positively influence attitude towards security countermeasures [116, 257, 291, 292]. Self-efficacy has also been shown to influence adoption and usage of IT [292, 293]. In this study, cyber-citizens' self-efficacy influencing and/or predicting attitude towards cybersecurity behaviour is examined. The expectation is that individuals with high self-efficacy about their ability to optimise web browser security settings will have more positive attitude towards cybersecurity than those with low self-efficacy. Therefore:

- *H9: High SE about WBSC will positively influence attitude towards cybersecurity.*

6.3.2.2 System Characteristics - IC

- *H10: The quality of WBSC interface design will positively influence attitude towards cybersecurity.*

System Characteristics such as quality, interface design, speed/reaction time, etc., are some of the external factors proposed to have an indirect effect on the acceptance and usage of information systems through user perceptions [248, 294]. For instance, Pituch and Lee [295] included system characteristics as part of the external variables influencing e-learning use through perceived ease of use and usefulness. To do this, they solicited user ratings on three different aspects of e-learning system — functionality, interactivity and response time. System characteristics especially functionality and interactivity were found to have the strongest total effect on the dependent variables of their model. The role of system characteristics in predicting technology acceptance through user perceptions has been explored in different contexts with a variety of system-specific features. In this study, three interface characteristics (IC) — layout, terminology and navigation) are identified as critical for user interaction with WBSC in the study. The assumption made here is that, usability features such as clear, consistent layout and easy navigation will impact on a users' perception of WBSC, and hence the decision to accept or reject usage.

6.4 The Empirical Study

6.4.1 Research Design

The main research objective is to investigate influential factors which will impact on people's security behavioural intentions towards predictive analysis of a user's acceptance of personalized adaptive cybersecurity for web browsers. A quantitative data collection and analysis approach similar to those employed by [118, 296–298] in predicting behavioural intention was adopted. A field survey consisting of an online measurement instrument designed to collect data regarding factors influencing cybersecurity attitude and behaviours was conducted. The survey instrument was developed and administered using Qualtrics, an online survey tool. The measures were mostly adapted from previous studies that have explored various types of determinants of technology usage and specific computer security practices. For instance, the original measurement scales of TAM were adapted and modified to fit the context of WBSC usage. All construct measures were assessed with a 5-point Likert type scale ranging from "strongly agree" to "strongly disagree", except for the demographics and questions related to user preferences and/or experiences. Both positively and negatively worded items were included on the scales. Negatively worded items were reverse-coded during the data analysis to ensure that a higher numbered response on the Likert scale would represent higher positive attitude score, and vice versa.

The measurement instrument developed for the cybersecurity behavioural model has four main conceptual/ theoretical components consisting of individual differences, user perceptions/ attitudes, behavioural variables, and cybersecurity personalization components. The individual differences section consists of four exogenous driver constructs (i.e., IC, DN, SE, and SBCL) as well as basic demographics such as age, gender, and environment. Thus the section measures participants' experience with web browser security (DK), self-efficacy (SE), levels of concerns for security breaches (SBCL), personal preferences in terms of browser types and their respective user interfaces (IC). The second part of the instrument assessed participants' general attitudes towards cybersecurity from five main user perceptions: Ease of Use, Usefulness, Risk, Personalization and Personal Data. Hence the TAM and PMT items (PU, PEOU, and PR) together with value for personalization (VFP) and attitude to personal data (APD) items represent the key determinants of the endogenous target constructs.

To minimize respondent fatigue, the APD scale adopted from Addae et al. [279] was simplified by selecting only eight items based on overall cluster membership predictor importance of the APD factors as well as the reliability score of the measured items. Consequently, questions on Personal Data Awareness (PDA), Personal Data Protection (PDP) and Privacy Concerns (PC) measured reflectively, captured the major facets of the APD as a Type II second-order construct. This was to allow us to fully assess participants' attitudes to personal data in relation to cybersecurity intention and usage behavior. The third section (behavioral variables) consists of measures for the target constructs of interest (i.e., BI and ACB) and asked whether the respondents had ever used or attempted to use web browser security functionalities as well as intentions toward personalized web browser security assistance. In the final part, items adapted from Xu et al. [298] were used to collect participants' ratings on the personalization dimensions identified for the purposes of building a Bayesian-based network model for adaptive cybersecurity. All measured items included in the survey instruments are described along with references to where they were adapted from in Appendix C. Items are grouped into the factors represented on the research model (Figure 6.1) to ensure that a complete dataset is collected for hypothesis testing and data analysis.

6.4.2 Data Collection

A pilot test was first conducted with a mix of 50 university students and lecturers to ensure the survey instrument is comprehensible and valid. Feedback from the pilot was used to revise the final version. Since the research design is exploratory in nature, convenience sampling was sufficiently adopted. The questionnaire was mainly used to collect convenience samples on two main university campuses in China and UK through email distributions. The questionnaire was also distributed online using various social media platforms including Facebook, Twitter, WeChat and LinkedIn. A total of 421 participants took part in the survey however, 37 incomplete and invalid responses had to be removed resulting in 384 usable responses. Alluding to the "ten times" rule of thumb on minimum sample size, the 384 valid responses meets the requirement for a PLS-SEM analysis. Accordingly, the 384 sample size is more than ten times the largest number of structural paths (six) directed at the most targeted construct in the model (ACB) and also more than ten times the number of indicators (six) used to measure the most complex construct in the model (APD) [299]. The raw data were imported from Qualtrics and coded into the IBM SPSS statistic program for a descriptive analysis of respondent profiles.

6.4.3 Data Analysis

The settings and goals of this research favours the use of PLS-SEM based on the criterion identified by Hair et al. [299]. Using the SmartPLS 3 software, the Structural Equation Modelling (SEM) technique of Partial Least Squares (PLS) was employed to assess the theoretical model [300]. PLS-SEM has proven to be a very valuable approach to developing and testing models in behavioural research. The approach is particularly versatile for extending models and running complementary analysis such as nonlinear relationships and moderation alongside hierarchical component models allowing for more complex model relationships to be tested. The PLS-SEM technique also deals with data related threats such as sample size, unobserved heterogeneity and normality in the dataset, to the validity of standard predictive analytics. PLS-SEM computes parameter estimates from least square estimation hence minimizing the demands on required assumptions about the dataset including the measurement scale for the data collection, sample size and residual distributions [301]. The PLS-SEM approach also allows for formative and multi-level constructs making it favourable for exploring possible causal relationships while avoiding parameter estimation biases typical of regression analysis. With reference to the two-step analytical process described in Hair et al. [299], the measurement model was first evaluated for reliability and validity as the first step. The structural theory is then verified to determine the significant levels of the hypothesized relationships at the second step. The 2-step approach ensures inferences drawn from the structural relationship are based on validated measurement scales.

6.5 Results

6.5.1 Sample Characteristics

Table 6.1 summarizes the characteristic and demographic distribution of participants. 51.3% of respondents were female and 48.7% males. The majority of respondents were students (70.3%) and fall within the age group of 18-24 (62.0%). A total of 99% of the respondents were educated well above 12^{th} grade and 72.7% earned an income of 1,000 to 8,000 US Dollars per month and 27.3% earned less than $1,000.

TABLE 6.1: Respondent Profile

Demographic Variables		**Freq.**	**(%)**	**Σ %**
		N=384		
Age	18 - 24 years	238	62.0	62.0
	25 - 34 years	93	24.2	86.2
	35 - 44 years	42	10.9	97.1
	< 45 years	11	2.9	100.0
Education	12th grade or less	4	1.0	1.0
	High school diploma	118	30.7	31.8
	Some college (no degree)	61	15.9	47.7
	Associate degree	9	2.3	50.0
	Bachelor’s degree	86	22.4	72.4
	Graduate/ postgraduate	106	27.6	100.0
Employment	Employed for wages	74	19.3	19.3
	Self-employed	13	3.4	22.7
	Unemployed	22	5.8	26.8
	A homemaker	2	0.5	28.9
	A student	270	70.3	99.2
	Retired	3	0.8	100.0
Gender	Male	187	48.7	48.7
	Female	197	51.3	100.0
Ethnicity	Asian/ Pacific Islander	29	7.6	7.6
	African/ Black	52	13.5	21.1
	Caucasian/ White	67	17.4	38.6
	Chinese	193	50.3	88.9
	Hispanic/ Latino	14	3.7	92.6
	Other	29	7.5	100.0
Income per month	Less than $1,000	105	27.3	27.3
	$1,000 to $5,000	165	43.0	70.3
	$5,000 to $8,000	66	17.2	87.5
	$8,000 or more	48	12.5	100.0

6.5.2 Reliability and Validity of the Measurement Model

The outer measurement model was examined for reliability and convergent validity with the same PLS software. All variance inflation factor (VIF) values are below 5.0 which suggests multicollinearity is unlikely to be a problem in the data analysis. Following guidelines in Hair Jr et al. [302], VIF was further checked to determine if the first-order factors of APD were three distinct constructs. The VIF values of all constructs were below the conventional estimate of 5.0 with the highest being 3.195. Convergent validity for items in this study was assessed through their factor loadings in order to support the theory that sufficient convergent validity is achieved when the item measures the target latent construct. All the indicator items had significant path loadings at an alpha level of 0.01 and had high loading (> 0.5) on their respective parent constructs [302, 303]. All of the outer loadings in the measurement model were above the minimum recommended level of 0.708 with the exceptions of ACB_4 (0.622) and PU_3 (0.651). These two items were retained in the measurement model because they were very close to 0.70 and the criteria for reliability and convergent validity were met [302]. For the higher order construct (HOC) APD, all paths from the three exogenous driver constructs were meaningful (PDA=0.20, PDB=0.68 and PC=0.21). All the values of composite reliability (CR) and average variance extracted (AVE) were well within the recommended threshold [303, 304], with CR ranging from 0.81 to 0.95 and AVE from 0.62 to 0.86 (Table 6.2). The square root values of all the AVE shown in bold and placed diagonally in Table 6.3 show that discriminant validity is well established. The distinctiveness of the contents captured by the three individual first-order factors of APD is demonstrated by their correlations which are well below the 0.80 boundary for establishing discriminant validity. In summary, the results of the statistical analysis support the reliability, convergent and discriminant validity of the scales in the research model.

TABLE 6.2: Constructs Reliability and Validity

Latent Variables	**Scale Items**	**Loadings**	**CR**	**AVE**
Behaviour	ACB_1	0.90	0.90	0.69
	ACB_2	0.90		
	ACB_3	0.88		
	ACB_4	0.61		
Experience	DK_1	0.87	0.90	0.82
	DK_2	0.94		
Intention	BI_1	0.88	0.93	0.81
	BI_2	0.92		
	BI_3	0.91		
Interface	IC_1	0.82	0.90	0.70
	IC_2	0.84		
	IC_3	0.85		
	IC_4	0.82		
PD Awareness	PDA_1	0.79	0.87	0.69
	PDA_2	0.88		
	PDA_3	0.82		
PD Behaviour	PDB_1	0.79	0.83	0.62
	PDB_2	0.76		
	PDB_3	0.81		
Privacy Concern	PRI_1	0.93	0.92	0.86
	PRI_2	0.92		
Perceived Risk	PR_1	0.92	0.93	0.81
	PR_2	0.91		
	PR_3	0.88		

. . . continued

. . . continued

Latent Variables	Scale Items	Loadings	CR	AVE
Personalization	VFP_1	0.93	0.95	0.86
	VFP_2	0.95		
	VFP_3	0.91		
Security Concerns	SBCL_1	0.82	0.93	0.78
	SBCL_2	0.90		
	SBCL_3	0.91		
	SBCL_4	0.91		
Self-Efficacy	SE_1	0.71	0.85	0.65
	SE_2	0.83		
	SE_3	0.87		
Usability	PEOU_1	0.80	0.81	0.68
	PEOU_2	0.85		
Usefulness	PU_1	0.85	0.84	0.64
	PU_2	0.87		
	PU_3	0.65		

TABLE 6.3: Inter-construct correlations and Fornell-Larcker Criterion Analysis

	ACB	**DN**	**BI**	**IC**	**PDA**	**PDB**	**PR**	**VFP**	**PC**	**SBCL**	**SE**	**PEOU**	**PU**
ACB	**0.83**												
DN	0.67	**0.90**											
BI	0.29	0.05	**0.90**										
IC	0.07	-0.13	0.67	**0.84**									
PDA	0.59	0.52	0.21	0.13	**0.83**								
PDB	0.78	0.73	0.13	-0.04	0.66	**0.79**							
PC	-0.14	-0.12	0.07	0.13	-0.01	-0.14	**0.90**						
VFP	0.65	0.56	0.14	-0.05	0.68	0.62	-0.01	**0.93**					
PC	0.68	0.82	0.05	-0.20	0.51	0.76	-0.11	0.61	**0.93**				
SBCL	0.34	0.41	-0.06	-0.21	0.49	0.45	0.26	0.56	0.47	**0.88**			
SE	0.53	0.55	0.02	-0.16	0.70	0.66	-0.06	0.64	0.59	0.65	0.81		
PEOU	0.49	0.27	0.76	0.53	0.21	0.33	-0.08	0.14	0.24	-0.08	0.09	**0.83**	
PU	0.54	0.47	0.12	0.00	0.86	0.64	0.01	0.66	0.52	0.62	0.78	0.13	**0.80**

6.5.3 Structural Model

Results of the structural model analysis are displayed in Figure 6.2. Paths in a PLS structural model can be interpreted similarly to standardized regression betas hence the overall predictive strength of the model is assessed by the explained variance in the endogenous variables. Tests of significance of all paths were performed following the bootstrap resampling procedure outlined in Garson [305]. In the model, R^2 value indicates the total variance explained by the endogenous latent variables. R^2 values of 0.19, 0.33, or 0.67 for endogenous variables in the path model are described as weak, substantial or moderate respectively. A bootstrapping resampling procedure

(5000 samples) was used to determine the significance of the path coefficients. Here, a multi-stage approach is adopted to facilitate the assessment of the APD impact on the two main endogenous variables in the extended-TAM model. The first model consisted of only the TAM and PMT Latent Variables (LV) as mediators and explained 59% and 49% of the variances in the two target constructs BI and ACB respectively. The value for personalization (VFP) factor was included in the second stage which increased the variance explained in ACB to 64%. The effect size (f^2) was assessed with the following equation:

$$\mathrm{f}^2 = \frac{\mathrm{R}^2_{\text{included}} - \mathrm{R}^2_{\text{excluded}}}{1 - \mathrm{R}^2_{\text{included}}} \tag{6.1}$$

Where $\mathrm{R}^2{}_{included}$ and $\mathrm{R}^2{}_{excluded}$ are the R^2 values of the dependent LV when specific independent LV are included or excluded from the model. Values $\geq$0.02, $\leq$015, and $\leq$0.35 for f^2 respectively, represent small, medium and large effects of the exogenous LV [302]. The effect size of VFP on the endogenous construct ACB was large (0.40) and significant (p<0.001). Subsequently, the APD LV was added to the model and this second-order factor increased the R^2 of BI from 59% to 63%, and that of ACB from 64% to 74%. The effect size f^2 is large (0.47) and significant (p<0.001) for the predictive value of APD on ACB. There is also a small effect size (0.10) of APD on BI, which is significant at (p<0.005). Figure6.2 provides the R^2values for each endogenous variable in the full PLS model along with path coefficients and associated t-values of the paths. To simplify the structural model and make it more legible, only paths that have significant relationships (indicated with asterisk on the path coefficient) are included in Figure 6.2.

The results (Table 6.4) show all five behavioural attitude determinants PEOU, PU, PR, VFP and APD, have significant effects on the behavioural intention to accept adaptive personalized cybersecurity. The five constructs together explain 63% of the variance in behavioural intention (BI). However only three of them were found to predict actual previous adoption of cybersecurity tools as the hypothesized path from BI was not statistically significant. The relationship between PU and ACB was significant (β = -.10, p<0.05), but not in the predicted direction. In this study, PEOU had the highest of the five path coefficients and a significant positive relationship with BI (β = .84, t=51.5, p<0.001) while APD appears to be the most important variable in the model predicting ACB (β = .64, t=12.87, p<0.001). Value for Personalization was also found to have significant effect on BI and CAB hence justifying its importance in influencing users behavioural intention and attitude towards adaptive cybersecurity in a personal context.

In addition to evaluating the magnitude of the R^2 values as a criterion of predictive accuracy, the model's out-of-sample predictive power (Q^2) values were also examined. Here a sample re-use technique called blindfolding that omits part of the data matrix and uses the model estimates to predict the omitted part is applied to obtain the Q^2

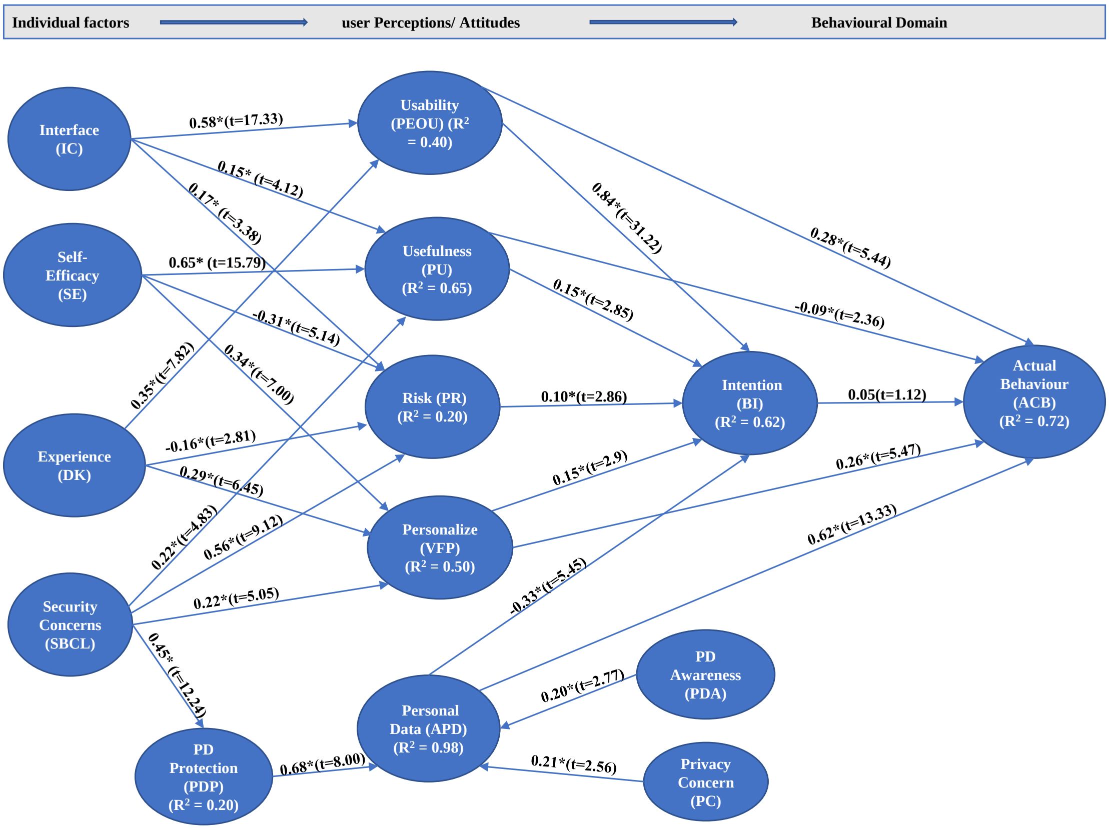


FIGURE 6.2: Path Model and PLS-SEM estimates

values for the endogenous constructs [302, 306]. Q^2 values greater than zero for specific reflective endogenous LV indicate the predictive relevance of the path model for that particular construct. Relatively values of 0.02, 0.15 and 0.35 indicate that the model respectively has a small, medium or large predictive relevance for the specified endogenous construct. Table 6.5 shows that all Q^2 values are considerably greater than zero, thus providing support for the cybersecurity behavioural model's predictive relevance for all the endogenous constructs especially having large predictive relevance ($Q^2 > 0.35$) for both of the two main target constructs (BI and ACB).

Further analysis was conducted to examine the moderating effects of demographic variables (Age, Gender) as well as the moderating influence of context of use (Home vs Corporate vs Public environments) on the hypothesized relationships in the model. When included in the model as control variables, age (β = 0.17, t=2.74, p<0.05), gender (β = 0.08, t=2.00, p<0.05) and environment (β = -0.23, t=3.71, p<0.001) were significantly associated with BI but none of them were significantly associated with ACB. Context of use (Environment) was negatively associated with BI, and it seems that users who more often access the web in public places are less interested in personalized adaptive cybersecurity. The income and education control variables were not statistically

TABLE 6.4: Summary of Findings

Hypothesized Paths	**Path Coefficients**	**t-values**	f^2	**Supported?**
Experience (DN) –> Perceived Risk (PR)	-0.16	2.81**	0.02	Yes
Experience (DN) –> Personalization (VFP)	0.29	6.49***	0.12**	Yes
Experience (DN) –> Usability (PEOU)	0.35	7.75***	0.20**	Yes
Intention (BI) –> Actual Usage (ACB)	-0.05	1.09	0	No
Interface (IC) –> Perceived Risk (PR)	0.17	3.37**	0.04	Yes
Interface (IC) –> Usability (PEOU)	0.58	17.38***	0.54***	Yes
Interface (IC) –> Usefulness (PU)	0.15	4.09***	0.06**	Yes
PD Attitude (APD) –> Actual Usage (ACB)	0.62	12.87***	0.47***	Yes
PD Attitude (APD) –> Intention (BI)	-0.33	5.51***	0.10**	Yes
Perceived Risk (PR) –> Intention (BI)	0.10	2.90**	0.03	Yes
Personalization (VFP) –> Actual Usage (ACB)	0.26	5.38***	0.12**	Yes
Personalization (VFP) –> Intention (BI)	0.15	2.92**	0.03	Yes
Security Concerns (SBCL) –> PD-Behaviour (PDB)	0.45	11.97***	0.25***	Yes
Security Concerns (SBCL) –> Perceived Risk (PR)	0.56	9.08***	0.22***	Yes
Security Concerns (SBCL) –> Personalization (VFP)	0.22	5.00***	0.05**	Yes
Security Concerns (SBCL) –> Usefulness (PU)	0.22	4.89***	0.08**	Yes
Self-Efficacy (SE) –> Perceived Risk (PR)	-0.31	5.09***	0.06**	Yes
Self-Efficacy (SE) –> Personalization (VFP)	0.34	6.95***	0.11***	Yes
Self-Efficacy (SE) –> Usefulness (PU)	0.65	15.77***	0.70***	Yes
Usability (PEOU) –> Actual Usage (ACB)	0.28	5.24***	0.10**	Yes
Usability (PEOU) –> Intention (BI)	0.84	31.50***	1.59***	Yes
Usefulness (PU) –> Actual Usage (ACB)	-0.09	2.38**	0.01	No
Usefulness (PU) –> Intention (BI)	0.15	2.90**	0.03	Yes

Note: *p $<$ 0.05. **p $<$ 0.01. ***p $<$ .001

TABLE 6.5: Predictive accuracy R^2 and out of sample predictive power Q^2 values

Endogenous LV	**R^2 Value**	**Q^2 Value**
Behaviour (ACB)	0.74	0.48
Intention (BI)	0.63	0.48
PD Attitude (APD)	0.98	0.48
PD Behaviour (PDB)	0.20	0.12
Perceived Risk (PR)	0.20	0.15
Personalization (VFP)	0.50	0.40
Usability (PEOU)	0.40	0.26
Usefulness (PU)	0.65	0.39

significant, hence they were not included in the results presented and further analysis. To further determine whether significant differences are present between coefficients for the observed heterogeneity (age, gender and environment), PLS-SEM multi-group analysis (PLS-MGA) was conducted following guidelines provided in Hair Jr et al. [302], Sarstedt et al. [307]. PLS-MGA is used for comparing PLS model estimates across groups of data when the groups pre-exist.

To explore the moderating influence of gender, the data was split into Male (n=184) and Female (n=200) subgroups and separate analyses were computed for each group with the full model. Three subgroups were created for age 18-34 (n=169), 35-44 (n=139) and <44 (n=76), as well as for environment and/or context of use Corporate (n=111), Home (n=205) and Public (n=68). As the maximum number of arrows pointing to an endogenous variable in the model is five, a minimum of 5*10=50 observations per group is

TABLE 6.6: Results of OTG for Age and Environment

Relationship	**Group**	**B**	**SS-Between**	**SS-Within**	**F$_R$**	**p**
Intention -> Behaviour	Environment 3	5000	206.64	0.10	2078.45	0.00
PD Attitude -> Behaviour	Environment 3	5000	614.86	0.17	3632.59	0.00
PD Attitude -> Intention	Environment 3	5000	544.58	0.06	8713.34	0.00
Perceived Risk -> Intention	Environment 3	5000	13.94	0.01	1277.02	0.00
Personalization -> Behaviour	Environment 3	5000	92.18	0.19	493.35	0.00
Personalization -> Intention	Environment 3	5000	11.93	0.02	669.01	0.00
Usability -> Behaviour	Environment 3	5000	253.81	0.12	2204.58	0.00
Usability -> Intention	Environment 3	5000	287.35	0.01	23289.54	0.00
Usefulness -> Behaviour	Environment 3	5000	419.16	0.05	8141.08	0.00
Usefulness -> Intention	Environment 3	5000	488.88	0.03	16709.36	0.00
Intention -> Behaviour	Age Group 3	5000	99.51	0.03	3627.87	0.00
PD Attitude -> Behaviour	Age Group 3	5000	20.39	0.02	1209.78	0.00
PD Attitude -> Intention	Age Group 3	5000	32.16	0.05	686.06	0.00
Perceived Risk -> Intention	Age Group 3	5000	28.84	0.02	1568.55	0.00
Personalization -> Behaviour	Age Group 3	5000	149.00	0.02	7804.65	0.00
Personalization -> Intention	Age Group 3	5000	87.93	0.03	2860.52	0.00
Usability -> Behaviour	Age Group 3	5000	59.70	0.04	1662.00	0.00
Usability -> Intention	Age Group 3	5000	500.49	0.05	9669.07	0.00
Usefulness -> Behaviour	Age Group 3	5000	32.01	0.01	3194.20	0.00
Usefulness -> Intention	Age Group 3	5000	265.61	0.03	10143.30	0.00

required according to the 10-times rule. The group-specific sample sizes for the three moderating variables can therefore be considered to be sufficient for the PLS-MGA. Since more than two groups are being compared in the case of age and environment, the Omnibus test of group differences (OTG) approach was applied as a first step to assess whether the path coefficients are equal across the three age and three environment groups. The analysis (Table 6.6) yields F_R values ranging from 493.35 to 23289.54 for paths between the mediating variables and the two target variables for the environment groups. F_R values ranging from 686.06 to 10143.30 were yielded for the age group differences on direct paths to the target variables. The null hypothesis that the path coefficients across the three groups of age and that of environment can therefore be rejected. Thus the test rendered all differences among the groups significant at $p \leq 0.01$ suggesting at least one path coefficient differs from the remaining two across the three groups both in the case of age and environment.

Table 6.7 shows the differences in the path coefficient estimates of the group comparisons with respect to all the direct paths to the two DVs in the model, and provides the results of multigroup comparisons based on PLS-MGA and Welch-Satterthwait (W-S) Test. While the PLS-MGA is a non-parametric test for difference of group-specific results based on PLS-SEM bootstrapping results, the W-S is a parametric test that assumes unequal variances across groups to determine the significance difference of group-specific PLS-SEM. As a one-tailed test, a typical cut-off level of significance for PLS-MGA results is >0.95 or <0.05, but the cut-off level can be set to >0.90 or <0.10 for smaller sample sizes. Slight differences between the PLS-MGA and W-S with respect to the significance of some of the group differences for specific relationships were observed. For instance, in the comparison of the Home and Public subsamples, the test rendered the relationship between Usefulness and Behaviour significant ($p \leq 0.10$) for PLS-MGA whereas this was insignificant in the W-S test (p=.15). In Table 6.7, significance levels <0.10 are highlighted in green while blue highlights indicates significance level determined at >0.90.

TABLE 6.7: Multigroup Comparison Test Results

Paths/Relationships	Comparison	PLS-MGA		Welch-Satterthwait Test	
		Path Coefficients - diff	p-Value	t-Value	p-Value
Intention -> Behaviour	Male vs Female	0.27	0.98	2.07	0.04
Usability -> Intention	Male vs Female	0.22	1.00	3.15	0.00
Usefulness -> Intention	Male vs Female	0.21	0.04	1.90	0.06
PD Attitude -> Intention	Home vs Corporate	0.44	0.94	2.15	0.03
Usability -> Intention	Home vs Corporate	0.15	0.02	2.02	0.05
Usefulness -> Intention	Home vs Corporate	0.20	0.05	1.75	0.08
Usefulness -> Behaviour	Corporate vs Public	0.38	0.04	1.75	0.08
Usefulness -> Intention	Corporate vs Public	0.43	0.99	2.59	0.01
Usability -> Intention	Home vs Public	0.27	0.00	3.12	0.00
Usefulness -> Behaviour	Home vs Public	0.26	0.07	1.47	0.15
Usefulness -> Intention	Home vs Public	0.22	0.95	1.59	0.12
Personalization -> Behaviour	Age <44 vs Age >34	0.21	0.97	1.88	0.06
Usability -> Intention	Age <44 vs Age >34	0.28	0.97	1.25	0.21
Usefulness -> Intention	Age <44 vs Age >34	0.23	0.04	1.71	0.09
Personalization -> Behaviour	Age 35-44 vs Age >34	0.15	0.92	1.43	0.16
Personalization -> Intention	Age 35-44 vs Age >34	0.13	0.91	1.30	0.19
Usefulness -> Intention	Age 35-44 vs Age >34	0.21	0.02	2.08	0.04
Intention -> Behaviour	Age 35-44 vs Age <45	0.19	0.07	1.44	0.15
Usability -> Intention	Age 35-44 vs Age <48	0.25	0.10	0.97	0.33

Table 6.8 summarizes the PLS-MGA results into a matrix to give a more simplified visual interpretation on determining significant effects based on demographics/ moderators. Although no specific hypothesis were declared for these moderating variables, the assumption that the effects of the attitudinal variables on the two target constructs may be dependent on them is reasonable. The results revealed significant differences in the group specific PLS path coefficients for the influences of the five mediating variables on ACB as well as BI on ACB. With regard to the age groups, there were significant differences between the groups for the relationship from BI to ACB, VFP to ACB, PEOU to BI, and PU to BI. In terms of Gender, the relationship between BI and ACB was negative and significant ($\beta = -0.25, t = 3.04, p < 0.05$) for Males while non-significant for the Females. This suggest that the unexpected negative relationship between BI and ACB that was found in the full sample results (Figure 6.2) seems to be largely based on the male respondents. Two other significant differences between Males and Females

subgroups are the relationships from PEOU to BI and from PU to BI. Although the relationship between PEOU and BI is positive and highly significant $(p < 0.001)$ for both groups, the MGA results shows that usability is somewhat more important in determining BI among females than males. Meanwhile, the relationship between PU and BI was positive and significant $(\beta = 0.22, t = 2.16, p < 0.05)$ for males while insignificant for females.

For the Environment subgroups, there were significant differences for relationships from APD to BI, PEOU to BI, PU to ACB and PU to BI. Interestingly, the path from PU to ACB was negative and moderately significant $(\beta = -0.31, t = 1.83, p < 0.10)$ for the public user group but insignificant for the corporate environment group. Thus usefulness in not important in predicting cybersecurity usage behaviour for those who mostly assess the internet within a corporate environment while most home and especially public users do not adopt cybersecurity tools though they may think they are useful. The differences in the environment groups for the relationship from PU to BI is also worth noting. Here PU seems to be more important in predicting positive BI of the public (β = .25, t=1.92, p<0.10) and home (β = 0.470.03, t=1.63, p>0.10) user groups than for the corporate group (β = -.0.17, t=1.73, p<0.10). The speculation here is that, due to availability of professional IT services in corporate environments, these user group feel more secured when assessing the internet, and hence may not see the need for an easier to use cybersecurity mechanism. Whereas, those who mostly assess the internet from non-corporate environments may have no access to cybersecurity experts, and may thus perceive personalized adaptive cybersecurity as an easier way of ensuring their security and privacy online. It should also be noted that the influence of attitude to personal data was relatively consistent across the different groups, except in the case of the home subgroup where APD did not seem to be influential in determining their BI, although it is important in predicting their actual cybersecurity usage (β = 0.47 t=7.57, p<0.001). Thus attitude towards personal data appears to have strong influence on cybersecurity behaviour and intentions across different user age and gender groups, and for both corporate and non-corporate users.

6.6 Framework for Personalized Adaptive Cybersecurity

Technology users differ in various ways in terms of goals, attitudes, and a host of individual characteristics and preferences that tends to influence their user experience. Design of user interaction for security and privacy technologies needs to accommodate different user goals and preferences. In the context of personal computing, web browsers provide a good platform to demonstrate the provision of adaptive and personalised cybersecurity configurations. Most current versions of web browsers allow users to sign in and synchronise their custom configurations across devices. This provides an opportunity to personalise default browser security settings as well as the

TABLE 6.8: Multigroup Analysis Matrix

Paths/ Relationships	**Age**	**Gender**	**Environment**
Intention -> Behavior		Male** vs Female	
PD Attitude -> Intention			Home vs Corporate*
Personalization -> Behavior	<44 vs >34** 35-44 vs >34*		
Usability -> Intention	<44 vs >34** 35-44* vs <44	Male vs Female***	Home** vs Corporate Home*** vs Public
Usefullness -> Behavior			Corporate** vs Public Home vs Public*
Usefullness -> Intention	35-44** vs >34	Male** vs Female	Home*** vs Corporate Corporate vs Public**

Notes: Significant levels are associated with the subgroups with the highest PLS path coefficients where *p < 0.10., **p < 0.05., ***p < 0.001

presentation of alerts to improve their acceptance rate and reduce cognitive loads associated with digital security on a personal level.

User model development is fundamental in an adaptive architecture for personalising user preferences. A user model consists of essential information and assumptions about users that can then be used to adapt the interaction of an application to specific individual users' needs. Building user models for adaptation and personalization often consists of two different approaches: one for the general user model and one for the personalised model. The general user model requires research and user experimentation to identify domain based generalization and classification of user interaction behaviours into specific user profiles. The personal model on the other hand will adapt new interactions based on observed data from an individual user session. An individualised profile for adaptive cybersecurity, for instance, will include background information on an identified user, goals, preferences as well as information on the target device and web application. Thus, the amalgamation of the user and personal model enables adaptation to be personalized through the classification of users based on demographic information and several other contextual and individual characteristics.

Research has shown that the cybersecurity field requires a multidisciplinary approach to identifying and translating the salient factors influencing specific privacy and security decisions into more effective user models. While Behavioural science techniques are useful to determine these salient factors and their dependencies, a lot of uncertainty remains in the attempt to recognize a user's goals from observations of behaviour. A powerful modelling technique developed by the artificial intelligence and machine learning community for effective reasoning in conditions of uncertainty in a sound mathematical manner is Bayesian Networks (BNs) [308]. BNs, also known as Belief Networks, provide a consistent way of replicating the essential features of plausible reasoning and have been successfully applied in the fields of medicine (e.g.[309]), marketing [310] and business management. BNs are known to be particularly useful in handling uncertainties in user modelling for different kinds of application domains. They are typically used in situations where variables characterise the existence or absence of a quantifiable outcome.

Nielsen and Jensen [311] described Bayesian networks as a directed acyclic graph (DAG) consisting of a set of variables and a set of directed edges between variables. The structure is mathematically referred to as a DAG whereby variables represents events and a link from event A to B represents a causal relation whereby A is a parent of B and B is a child of A. Each variable B with parents $A_1, \ldots\ A_n$ has the potential table $P(B|A_1, \ldots A_n)$ which holds conditional probability distributions. Consequently, a BN allows an identified joint distribution factorization to be represented graphically whereby the dependencies among variables are indicated with the directed arcs in the graph. The network of relationships in the BNs highlight how the various components interact with each other to influence the decision making process. A BN outputs generally reveals both the qualitative relationships between attributes and their quantitative measures in the form of conditional probability distributions of the factors' dependencies and interactions. Analysing the personalization components of cybersecurity (see Figure 6.3) with a Bayesian network is therefore expected to facilitate the characterization of various interactions between user context, profile, preferences and cybersecurity behaviour.

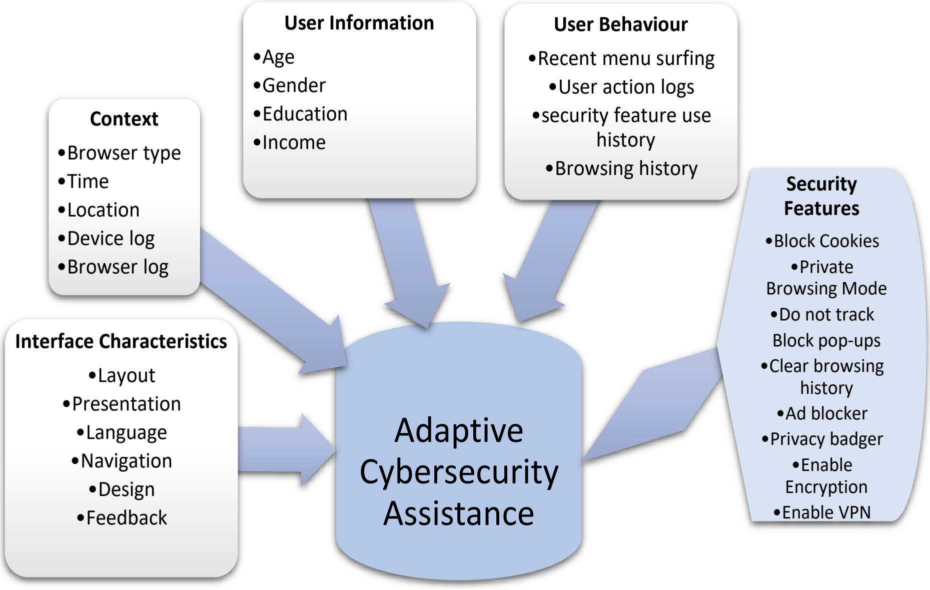


FIGURE 6.3: Proposed dimensions of personal adaptive cybersecurity assistance

For this thesis project, BNs serve as an important tool to compliment the user modelling process for adaptive cybersecurity. This is because the relationships between the many factors influencing a user's digital security decisions are mostly unclear. The empirical study conducted has led to the identification of these influential factors and for the directionality of their interactions to be determined. This makes directed edges in BNs more appropriate for the proposed model than undirected edges in Markov Random Fields [312]. The hidden states of these influential factors need to be intuitively inferred through observation of their effects using Bayes' rule. Thus BNs allows the inference problems to be formulated as a case of resolving the probability of an unknown variable from values of attributes observed. Apart from being able to describe uncertainty with BNs, there is the added advantage of being able to integrate different types of variables and related data within a single framework, and the flexibility of updating the models with new information at any given time.

The components of the framework (Figure 6.4) were extracted from the empirical study described in section 6.4. Following the validation of the behavioural research model, the statistical analysis of data on the personalization dimensions presented in Figure 6.3 is used to support the construction of the Bayesian network model. In summary, user profile constituting personal information and observed behaviour, system characteristic variables (e.g. browser type, security settings etc.), and context of use are the factors being considered for personalized or adaptive cybersecurity within web browsers.

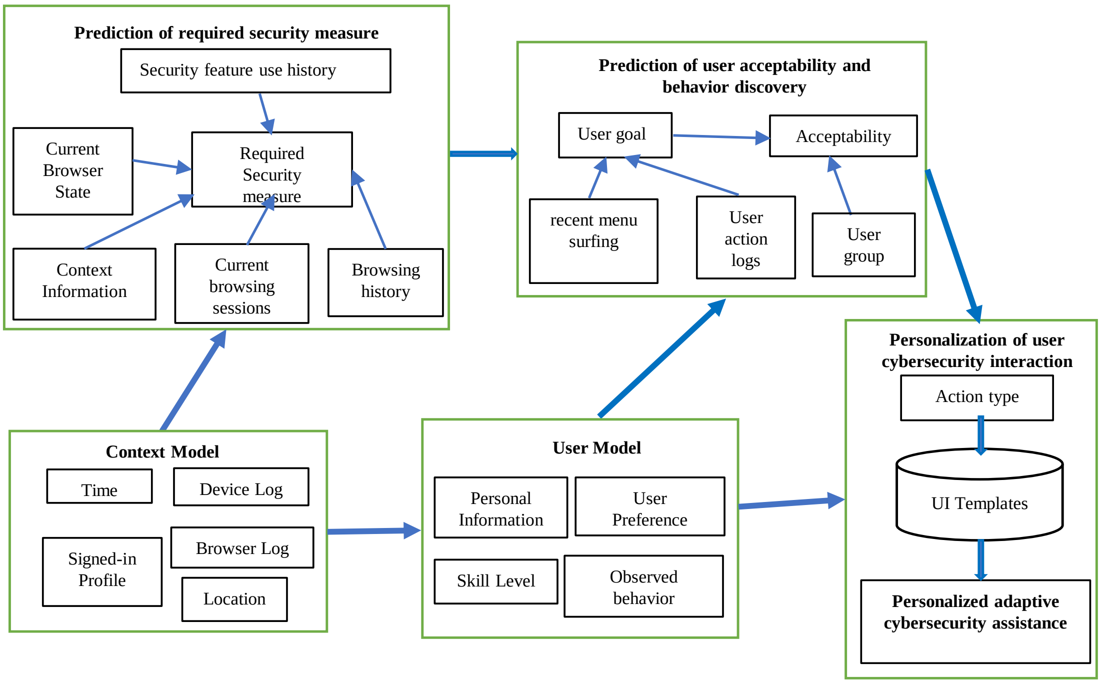


FIGURE 6.4: Bayesian Network framework to infer and provide personalized adaptive cybersecurity assistance

6.6.1 Structuring the Bayesian-Network-Based Model

Given the results from the empirical studies, the next practical steps involves building and assessing Bayesian models that can determine a user's security/privacy needs and likelihood to adopt available cybersecurity solutions. Defining appropriate variables and states of the identified variables are the building blocks of an effective user model. The objective here is to achieve quality inferences from the models by incorporating contextual information, user's actions including queries (both current and previous), as well as the user's background and personal preferences. It is important to define the states of the variables included in the model clearly so users can be monitored and the conditional probabilities assessed. To establish a database for the BN model, the impacts of attributes related to web browser security features are analysed together with individual characteristics and context of use factors. Information from the survey instrument is used to produce a table values for the personalization component variables and used to calculate the prior probabilities of the model.

To simplify the analysis, the levels within most of the variables were reduced. For instance the variable "location" was reclassified into three categories: home, public and private instead of the seven different locations measured with the survey scale (Home, School, Office, Public Transport, Cafes, Lecture rooms and Friend's house). Time of use was also set to peak and non-peak where peak time denotes periods where the user may normally be involved with official use of the internet for work or business related goals, and non-peak for pleasure or non-business related goals. Using a BN for analysis of responses to the cybersecurity personalization survey data can uncover and characterize the interaction of the personalization components and user's cybersecurity behaviour. This will yield both quantitative measures in the form of conditional probability distributions as well as qualitative relationships between the components of personalized cybersecurity.

BNs can be modelled based on priori domain knowledge and/or training datasest [313]. Since cybersecurity related datasets on HCUs was unavailable at this stage, the available dataset gathered from survey was augmented with domain knowledge to obtain the best combination of nodes for the BNs. Thus the cybersecurity personalization factors extracted from the data analysis along with models of the web browser security features was used to develop the initial BN models for several web browser security related tasks and subtasks. Eventually, the overall model resulted from the combination of several partial models developed from domain knowledge and simulated data generated with representative nodes. For instance, if we know a relation between user's security/privacy perceptions and expertise, these nodes can be connected by amending their Conditional Probability Table (CPT) bounds of states accordingly. Conditional probability distributions (CPDs) of the form — the probability of B given A ($p(\mathrm{B}|\mathrm{A})$), are then used to encode the relationships between variables in the BN. For each node B, the likelihood that the variable will be in each possible state given its parents' node A states is thus dependent on domain knowledge acquired from the empirical study as well as the frequency observed in both the measured variables and the simulated dataset (see Figure 6.6). This approach ensures a prior distribution is estimated for the model parameters and used alongside those learned from data. This helped in minimizing incorrect assignment of probabilities in cases where possible combinations were

TABLE 6.9: Cluster distribution of respondents showing cluster centres sorted by overall cluster membership predictor importance

Cluster	Cluster 1	Cluster 2	Cluster 3	Cluster 4
Description	Highest cluster group has high acceptability of PAC	2nd highest cluster group has high intention to adopt PAC	3rd highest cluster has moderate acceptability of PAC	The smallest cluster group has low acceptability of PAC
Size	31.8% (122)	26.8% (103)	23.4% (90)	18.0 (69)
Inputs	Acceptability 100%	Acceptability Intention(69.9%)	Acceptability 60%	Acceptability No intention (69%)
	Self-Efficacy µ=0.91	Self-Efficacy µ =-0.9	Self-Efficacy µ =0.02	Self-Efficacy µ =-0.16
	Age 25-34 (40.2%)	Age 18-24 (100%)	Age 25-34 (76.7%)	Age 18-24 (63.8%)
	Gender Male (94.3%)	Gender Female (100%)	Gender Female (75.6%)	Gender Male (91.3)
	Environment Corporate (56.6%)	Environment Home (100%)	Environment Home (83.3%)	Environment Corporate (39.1%)
Evaluation fields	ACB µ =0.84	ACB µ = -0.84	ACB µ = -0.24	ACB µ =0.07
	PEOU µ =0.45	PEOU µ = -0.16	PEOU µ =-0.26	PEOU µ =-0.23

not observed in the training data [314].

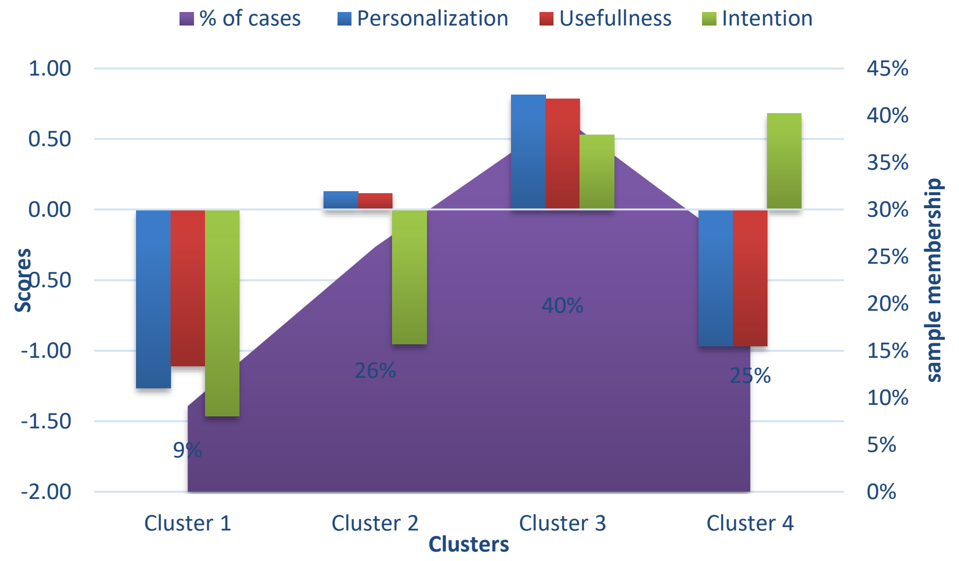
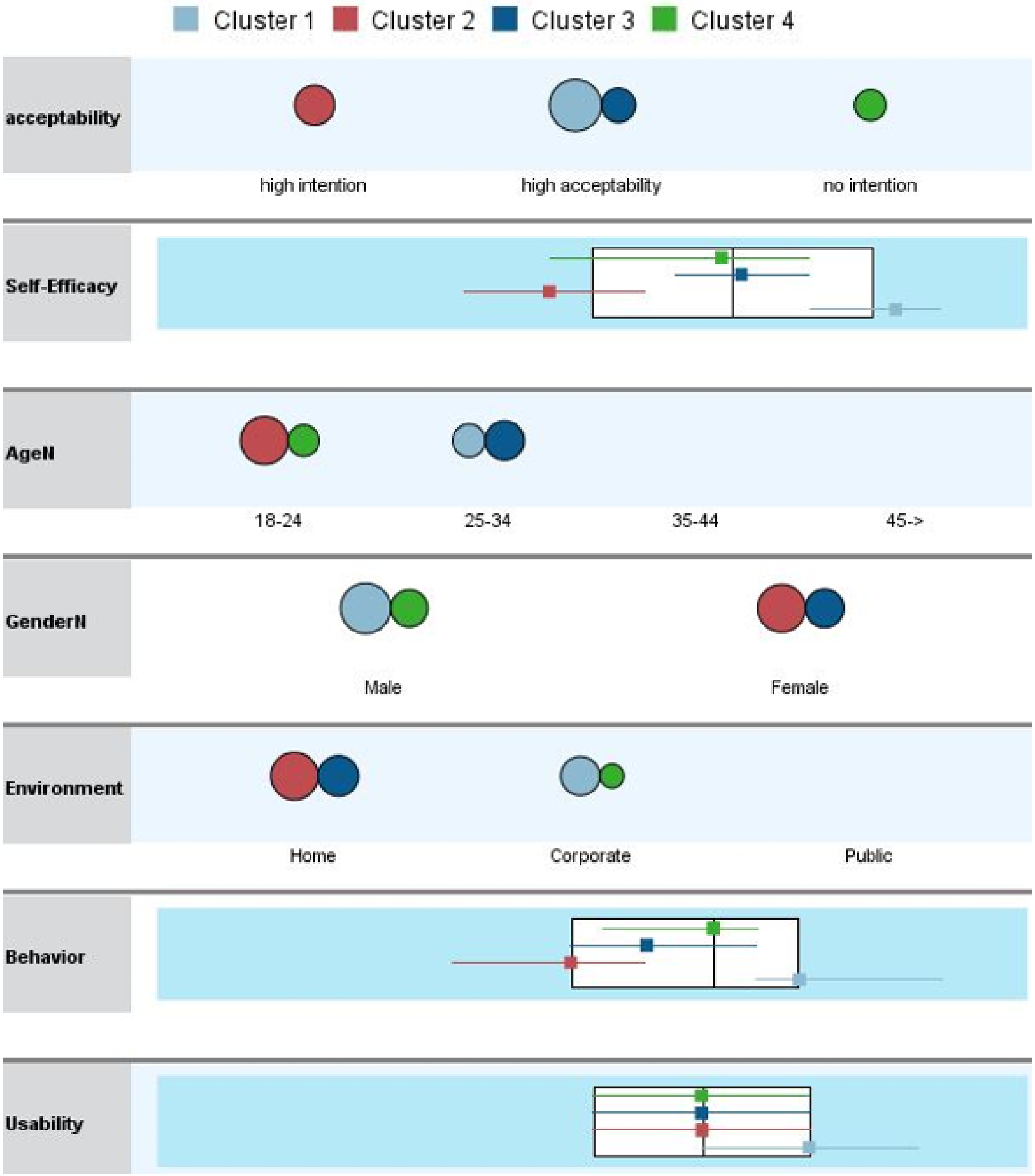


FIGURE 6.5: Cluster groups based on acceptability factors

As an example, I considered a simple scenario of inferring the likelihood that a user will welcome the automatic blocking of a third party cookie. Considering observation of recent actions taken by the user on the web browser, example assumptions and reasoning that can be made here are that there might be a 50% chance of a random user accepting to block 3^{rd} party cookies if the user is completing an online form requiring sensitive information, but if the user is on a university campus, that probability will become 62% based on observations of user behaviour in similar context. Moreover, in considering the user's profile information, if the user was female the likelihood might decrease to 43%. Prior probability can also be indicated for a user based on age and



a *Cluster 1 – high acceptability (100%) of PAC, score highest on self-efficacy and mostly access the web using corporate (56.5%) and public (43.3%) networks and more likely to have previously adopted a cybersecurity solution and found it user friendly.*

b *Cluster 2 – high intention to adopt PAC (69.9%) but scored the lowest on self-efficacy, mostly access the web using home network and less likely to have previously adopted a cybersecurity solution.*

c *Cluster 3 – Moderate acceptability (60%) with about 25% likelihood of rejection and 15% intention to adopt PAC. Moderate score on self-efficacy, mostly access the web with a home (83.3%) and sometimes corporate (16.7%) network and less likely to have previously adopted cybersecurity solutions.*

d *Cluster 4 – Low acceptability of PAC as 65.2% of these respondent group have no intention to adopt PAC and only 34.8% indicated high intention to adopt PAC. Low score on self-efficacy and access the web with all the three types of networks with about 39.1% likelihood for corporate, 33% likelihood for home and 27.9%. They are likely to have previously adopted a cybersecurity solution and not found it user friendly.*

FIGURE 6.6: Visualization of cluster comparison

frequency of using specific security features of the web browser. Qualitative inputs in terms of the variables and their dependencies are generated by domain knowledge and expert opinions. Quantitative data are subsequently generated using data analysis and model simulation.

To identify homogenous groups in the data set, a Two-Step clustering that is able to automatically determine the optimal number of clusters in a data set was adopted. Respondents were first clustered based on their factor scores on three acceptability variables determined from the PLS-SEM model (VFP, PU and BI) with k-means clustering. The results show that, majority of the participants have favourable consideration for PAC (Figure6.5). The acceptability cluster membership was then combined with other adaptive cybersecurity personalization variables (such as, context/environment, gender, age etc.) for the Two-Step clustering and evaluated on self-reported previous use of cybersecurity tool (ACB) and PEOU. The results are summarized in Table 6.9 and visualised with Figure 6.6.

The joint probabilities are then used to specify the CPTs. To make a prediction from the BN, the model propagates the information at any given instance based on its structure and prior/conditional probabilities and provides the post-probabilities associated with the acceptability status (high or low) for a particular cybersecurity task to be adapted to the user's preference. Consequently, the BN-based decision engine will take output probabilities from both the context and user models as causal factors, together with the web browser configuration log and security task models to make a prediction. A decision status (e.g. block cookies, send alert or not) with an associated probability is arrived at after information is propagated in the BN. If the "acceptability" and "security need" probabilities are higher than a preset threshold, an automated security assistance in this scenario (auto block 3^{rd} party cookies or a preferred form of user alert) is provided for the user (see Figure 6.7). Based on the evaluation of the level of satisfaction with the automated assistance provided, the user preference model is updated accordingly. Figure 6.7 illustrates a personalized cybersecurity adaptive task limited memory influence diagram (LMID) built using domain knowledge with records from the survey data analysis.

The preliminary results using simulated data provide shows the feasibility of the approach. However, since no real trial data was available for a full validation at this stage, the model is evaluated based on prediction accuracy. Thus considering real usage scenarios, are the levels of acceptability predicted satisfactory? The Hugin software [315][1] used for the BN modelling allows analysis about how well the predictions of the network match the cases in the dataset. Investigation shows that probability changes among specified scenarios for the proposed BN parameters, were similar to those obtained by the learned BN. Evaluation started with the BN built based on the proposed

[1] http://www.hugin.com

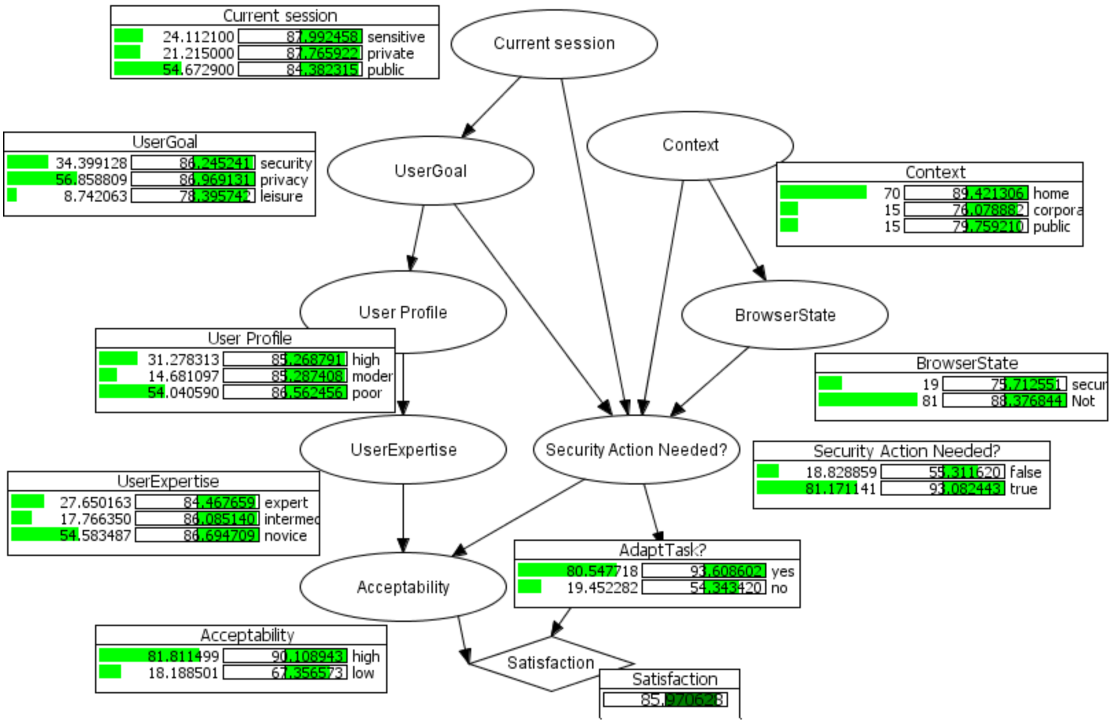
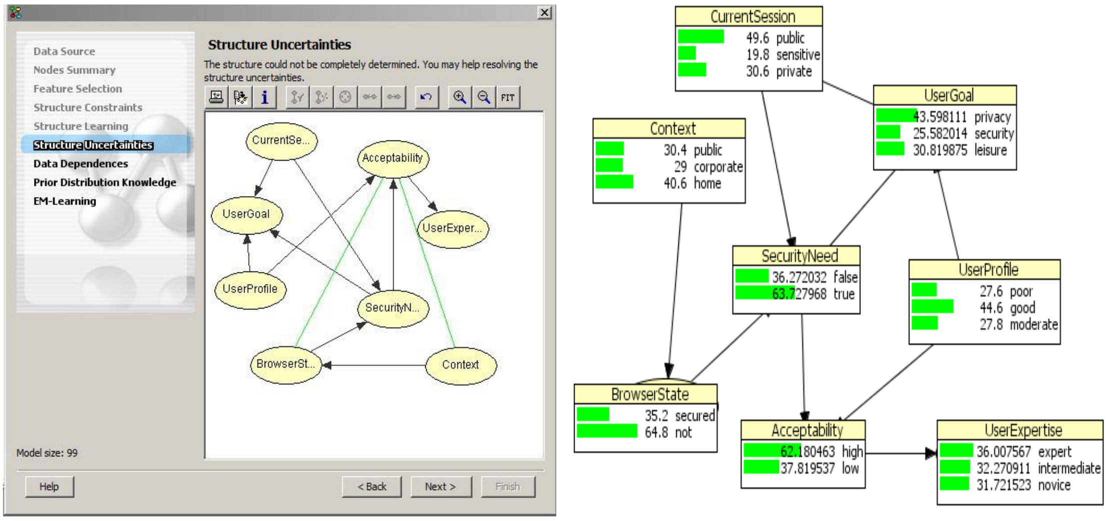


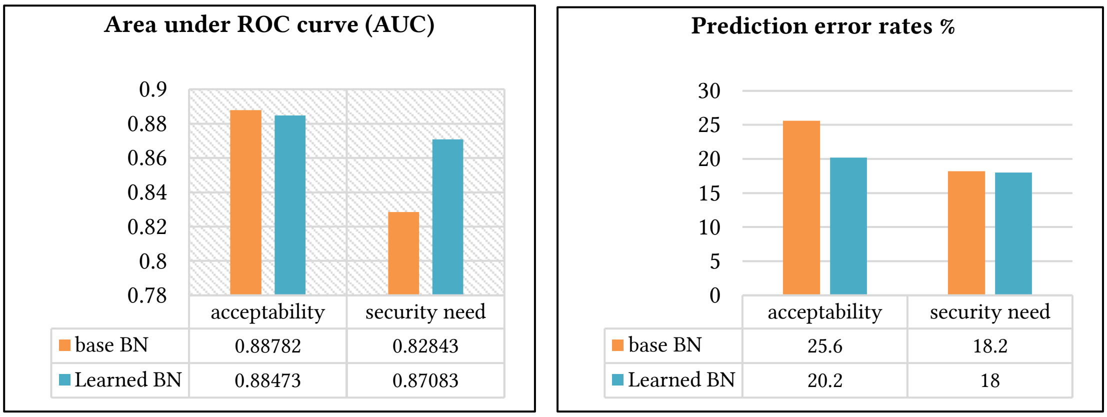
FIGURE 6.7: The qualitative representation of the LMID used for decision making in PAC with priors based on data analysis



The structure could not be completely determined. You may help resolving the structure uncertainties.

FIGURE 6.8: The intermediate structure and CPT estimates for the Learned BN

LMID referred to as the base BN. Next, data analysis was used to populate the CPT of the base BN which, is then used to generate a simulated data set. With the aid of the Learning Wizard a new network called intermediate BN was automatically generated from the simulated dataset (Figure 6.8). Prior domain knowledge was then applied to resolve any uncertainties that was present in the intermediate BN structure. With the discovered network and the generated database, parameter learning was carried out to specify a new CPT for the ensuing network called learned BN (Figure 6.8). Finally, the performance results (error rates and AUC) for the originally proposed BN structure are compared with corresponding BNs automatically discovered from both the survey and simulated data sets (Figure 6.9). A receiver operating characteristic (ROC) curve is a fundamental measure of a model's performance for predicting specific states and the area under the ROC curve (AUC) allows the quality of the model to be expressed using a single value.



	acceptability	security need
🟧 base BN	0.88782	0.82843
🟦 Learned BN	0.88473	0.87083

	acceptability	security need
🟧 base BN	25.6	18.2
🟦 Learned BN	20.2	18

FIGURE 6.9: Comparison of performance measures results for the base and learned BN structure

6.7 Discussions

The objectives of the study presented in this chapter are in two folds. One is to conduct an empirical study using a behavioural science approach to determine the factors influencing users' cybersecurity behavioural decisions. The second is to investigate the feasibility of integrating findings from the empirical studies into the machine learning approach of user and system modelling for cybersecurity. To this end, a cybersecurity behavioural model was first introduced and empirically tested. The effects of five attitudinal constructs on cybersecurity behavioural intentions and behaviour were examined and in doing so, (1) the original TAM was extended with additional dimensions – Perceived Risk, Value for Personalization and Attitude towards Personal Data, and (2) the influence of three sample demographic variables on cybersecurity behavioural intentions was examined. Although not all the hypothesized paths were found to be statistically significant, some interesting findings resulted from the study. The results suggest that both security-related perceptions and general external factors contribute to individual cybersecurity adoptive behaviour. The results also provide some evidence that these factors are moderated by the user's gender, age and the environment within which the internet is mostly accessed. Following the testing and verification of the behavioural model, those empirical findings were combined with the machine learning technique of Bayesian-network modelling for the development of a personalized adaptive cybersecurity framework.

The proposed behavioural model successfully explained most of the variance in the dataset. Similar to earlier studies [117, 259], TAM proved to be a useful theoretical framework to explore and explain factors influencing individuals' behavioural intentions towards technological innovations. Although the study confirmed the direct and indirect effects of some of the TAM constructs on cybersecurity behaviour, some of the results are inconsistent with prior research findings,and warrant further discussion. The results support prior empirical work that found a relationship between perceived ease of use, usefulness and behavioural intentions towards technological innovations (e.g.[268, 316]). However, contrary to suggestions from most prior studies that perceived usefulness is the main determinant of usage intentions in other IS research contexts (e.g. [96, 258, 317]), the results from this study show perceived ease of use has a greater influence in predicting behavioural intentions in the context of cybersecurity.

The experimental results are however consistent with some previous studies that applied the TAM to some online applications, finding a strong effect of perceived ease of use on usage intentions and behaviour (e.g. [269, 318–320]. The original TAM theorize PU have direct effect on behavioural intention while PEOU indirectly influences the intention through PU, hence depicting PEOU as a weak predictor of usage intentions. The model, however, supports a direct effect of PEOU on behavioural intentions and usage of cybersecurity, and points to a greater significance of the ease of use factor in the context of digital security. A possible explanation of this finding could be attributed to the assertion that the effect of PEOU is dependent upon whether the type of use is intrinsic or extrinsic to the technology [319]. Thus, as PEOU measured how easy the participant found it to learn and configure the security settings of their preferred web browser, the types of tasks involved here are intrinsic in that cybersecurity itself is an integrated component of the web browser with an interface that delivers the desired security and privacy control. Although the model did not support influence of PEOU on PU as theorized in the original TAM, PU did have a substantial impact on behavioural intention, which is consistent with extant findings in the TAM literature. The results confirms the direct relationship between PU and behavioural intention, though PEOU did not have a significant effect on PU and the proportion of the BI variance accounted for by PEOU far outweighed that of PU in the proposed cybersecurity behavioural model. Also, PEOU is a significant determinant of self-reported actual usage in this study, while PU is a non-significant determinant. PEOU therefore provides a considerable explanatory power in the context of cybersecurity usage among home computer users.

Another major conclusion from this study that differs from the classical TAM-related studies is the role of behavioural intention. Based on findings from previous behavioural models, behavioural intentions was originally hypothesised to predict actual self-reported adoption of cybersecurity mechanisms. However, contrary to what the extant literature suggests, the dataset collected in this study did not support this hypothesis. This revelation can however be considered reasonable when closely examined within the specific context of this research. This is because the behavioural intention construct in this study focused on PAC rather than general cybersecurity, and hence participants may not yet have been exposed to it. Moreover, in the context of cybersecurity it is generally logical to expect the inherent inexplicableness of security to impede actual usage though users may have intended to adopt available countermeasures. Thus factors such as complexity, inexperience and the secondary nature of security configuration to cyber browsing in general tend to deter adoption and usage of cybersecurity tools. The findings however highlight the moderating role of gender as the effect of BI on actual self-reported usage was significant for Males but not for females although the relationship was negative. Moreover, the effect of PEOU on BI was much stronger for the female subgroup, indicating that female netizens may be more hesitant to adopt difficult-to use cybersecurity controls. This is consistent with earlier findings from the user experience analysis in Chapter 4 whereby male participants generally had a lower usability expectation for security-related interfaces.

The results also suggest that the strongest predictor of self-reported actual usage of cybersecurity controls is the second order construct of attitude towards personal data. Thus, participants who showed higher concern for the collection and use of their personal data were more likely to have attempted to, or actually adopted a cybersecurity countermeasure to ensure their privacy/security online. Interestingly, the relationship between the APD construct and BI to adopt personalized adaptive cybersecurity was negative, indicating that users who are very privacy conscious are less likely to adopt cybersecurity mechanisms that rely on their personal data to provide adaptivity. The relevance of the proposed BN framework is clearly supported by this findings. The BN-based models complements available system records with domain knowledge data for the design of an intelligent cybersecurity mechanism. This minimizes the need to actively mine personal data to support prediction of acceptance of intended security task to be automated. The BN can also learn from real usage experience data to automatically update the probabilities when the inherent adaptability function is executed in practice. Users will be more satisfied if automated cybersecurity assistance provided is relevant to their primary cyber goals and delivered in a manner acceptable to them based on appropriate factors influencing their personal preferences. This requires a complex decision-making process involving predictive analysis of system and usage behaviour with a host of uncertainties. Building the predictive model with a BN which has the inherent facility to handle uncertainties will ensure a more effective provision of automated assistance that meets differing users' preferences compared to random automation of security tasks.

6.7.1 Implications for theory and practice

This study has implications for both researchers and practitioners of cybersecurity. From a research perspective, the extension of the TAM explained a significant amount of the variance in behavioural intention and adoption of web browser security controls. The study validates the significant role of user perceptions of ease of use, usefulness, risk, and personalization in predicting individual's intention to adopt PAC to achieve their security and privacy goals while accessing resources in the cyberworld with their web browsers. As discussed, the ease of use factor which is known to have weaker influence in the classic TAM literature, takes on a much more significant role when it comes to cybersecurity control usage and intentions. This implies that individuals who normally disregard cybersecurity countermeasures may have the intention of adopting PAC if they realize that it will be useful and easy to do so. The study introduced additional constructs from protection motivation theory and personal data research that better reflect the complex context of cybersecurity which encompasses digital security and privacy in its entirety. The findings from the PLS-SEM generally support the importance of the additional constructs, especially attitude towards personal data in predicting adoption behaviour in the domain of cybersecurity. Consequently the findings from the empirical behavioural study provide theoretical contributions in the area of cybersecurity acceptance and usage. This is with respects to both re-validation and extension of past theoretical framework as applied to the new context of security behaviour modelling. The findings from this research therefore add substantially to the knowledge base on predicting cybersecurity behavioural intentions and personalization dimensions for security design.

The findings also have implications for practice and design as it can inform several aspects of improving the usability of cybersecurity mechanisms. This study suggests that, cybersecurity mechanisms targeted at home computer users need to be very usable with minimal demand on cognitive resources. The study also endorses the value of incorporating data and privacy protection into system design right from the onset, which are the underlining principles of recent *privacy-by-design* projects. For instances both the new EU GDPR and PRIPARE projects [321–323] highlight the need for *privacy-by-design*. The proposed predictive model for providing personalization takes on individual's disposition to their personal data into account. This provides a framework for incorporating data privacy controls from the design stage. In so doing, personalization is provided at the preferred level for each individual. Thus, the design framework will facilitate the process of determining and limiting access to such data that a user might consider too sensitive in providing adaptive cybersecurity.

6.7.2 Limitations and future research

It is important to highlight the limitations of the studies presented in this chapter. Notably, generalization will need to be done with caution as the university students and staff were used as a convenience sample. The data set has however been successfully used to provide empirical evidence for the usefulness of predictive analytics with users' behavioural data for the design of adaptive cybersecurity. Further research work is also needed to fully evaluate the proposed BN-based models. This will require additional dataset and further optimisation and testing before implementation. Although some measured data sets (such as self-efficacy) were obtained, observation data such as the actual level of user's cybersecurity expertise and security state of the browser were not available during the development of the BN-based models. Nevertheless, the primary contribution of this work is to demonstrate how findings from behavioural empirical studies can be complemented with Bayesian-network modelling to better support prediction and decision-making for adaptive systems in the domain of cybersecurity. This represent a first-step towards the design and development of a user friendly adaptive cybersecurity which adheres to the concept of *privacy-by-design*.

Continuing with the combined approach of empirical studies and modelling technique, two future research directions can be determined. First, more broader samples are required to replicate the behavioural model and validate inferences that can be made based on either a PLS or Covariance-based SEM results. Secondly, more factors that will influence cybersecurity personalization need to be considered and their appropriate measure determined so they can be incorporated into the Bayesian network system.

6.8 Chapter Summary

An exploratoy investigation into the feasibility of pedictive analytics of behavioural data as a possible aid in developing effective user models for adaptive cybersecurity is reported in this chapter. The chapter describes the empirical study conducted to examine predictive analytics of individual behavioural data. Using a research model based on the integration of the Technology Acceptance Model (TAM) with PMT, a wide variety of constructs are explored in an attempt to explain and predict an individual's security behaviours. The integrated TAM and PMT model is further augmented by introducing Attitude to Personal Data (APD) as part of the key determinants of intention to practice cybersecurity.Partial Least Squares Structural Equation Modelling (PLS-SEM) is applied to the domain of cybersecurity by collecting data on users attitude towards digital security and analysing how that influence their adoption and usage of technological security controls such as web browser security functionalities. Initial results from the empirical study shows predictive analytics is feasible in the context of behavioural cybersecurity and can aid in generating usefull heuristics for the design and development of adaptive cybersecurity mechanisms. Predictive analytics can also aid in encoding digital security behavioural knowledge that can support the adaptation and/or automation of operations in the domain of cybersecurity. It can be used to identify cybersecurity issues that are susceptible to individual characteristics and provide a basis for the development of effective countermeasures for different user profiles.

CHAPTER 7

User-Centered Design and Evaluation of Security UI

Contents

7.1 Introduction

Web browsers are used to access contents within cyberspace. It is practically a user interface (UI) for accessing different types of contents including HTML documents, images, PDF etc. from remote web servers. As a UI, a browser's main function is to present web resources chosen by users within the browser window. This is achieved through a stateless and anonymous protocol called HyperText Transfer Protocol (HTTP) [324]. Most current web browsers employ an extensive architecture to augment the underlying web page technology of HyperText Markup Language (HTML) and provide other useful features such as private browsing, password management, bookmarking, syncing, accessibility features to accommodate users with disabilities etc. [6]. Accordingly, the basic architecture underlying a browser comprises of eight major interdependent sub-systems namely:

1. The UI which is the main browser display and settings pages
2. The Browser Engine for querying and handling actions between the UI and the rendering engine
3. The Rendering Engine is responsible for parsing and displaying HTML documents styled with CSS
4. The Networking sub-system for network calls such as HTTP etc.
5. JavaScript Interpreter for parsing and executing JavaScript codes
6. XML Parser

7. The UI Backend which uses operating system UI elements for drawing basic widgets and fonts

8. The Data Subsystem, a persistence layer that allows browsers to save all sorts of data locally on disk including cookies, bookmarks, and cache.

The added functionality offered by some of these subsystems exposes the browser to numerous vulnerabilities. For instance, the JavaScript interpreter allows client-side code execution within the browser for improved browsing experience but can equally be exploited for malicious purposes by attackers. Web browsers also gain the ability to deliver different types of web contents through plug-ins or add-ons such as the Adobe Flash Player for multimedia contents. Consequently, browsers are constantly evolving to accommodate more complex web applications including, emails, banking, television, virtual reality games etc. This increases the attack surface that can be exploited for security and privacy breaches. The importance of the security controls provided by web browsers can therefore not be overemphasized. Different kinds of cyber attacks through browser vulnerabilities publicly documented have been noted to render antivirus and firewalls ineffective [28, 325–328].

As highlighted in previous chapters of this thesis, non-expert users typically ignore these controls due to a number of usability and acceptability factors. While a growing number of studies continue to explore the human aspect of cyber security (e.g. [168, 170, 257, 329]), the question of how to make practical improvements to the usability and acceptability of technical security controls for non-expert users largely remain unanswered. This thesis seeks to address this gap by analysing user experience with these security controls (Chapter 4), studying and modelling user security behaviours (Chapters 5 and 6), designing alternative UIs and evaluating these designs.

This chapter describes the design and evaluation of the proposed SecAdapt browser which aims to improve the usability of browser security controls for non-expert users. The functions of usable browser security controls are addressed by identifying two primary goals. First is the need to improve the UI design of these controls. Second, to verify security functions that can be automated and adapted for individual preferences and their acceptable levels. Thus although the need for adaptive personalized security is identified, there is the need to gather requirements for acceptable levels of automated assistance through a user study. To achieve this goal, a user-centered design research is conducted.

7.2 Usable and Adaptive Cybersecurity Artefacts Instantiation

Vaishnavi and Kuechler [3] highlight the discovery and contribution of new knowledge as a key characteristic of Design Science Research (DSR) that distinguishes it from a routine design project. The general methodology of DSR framework for IS was applied to demonstrate relevance and rigour towards making contributions to the IS knowledge base by solving a persistent problem of usability and acceptability in the domain of cybersecurity. To address the research question of how to design cybersecurity controls to improve usability and acceptability among non-expert users, there is the need to instantiate prototype UIs as IS artefact to be evaluated. Vaishnavi and Kuechler [3] describes an IS artefact as not just an instantiation of the material artefact but equally important are the constructs, models and techniques applied in the design and development process.

Accordingly, a typical DSR goal can be realised through five main stages (see Figure 7.1). At Stage 1: Awareness of the problem — this thesis has identified the need to improve the usability of cybersecurity controls by building the case of their low adoption and correct use among non-expert users. At Stage 2: Suggestion — user experience with existing web browser security controls were analysed to gather requirements and preferences and the role of users' attitudes and behaviours in the adoption of cybersecurity tools were also assessed to envision new functionalities such as automated assistance and personalization. In Stages 3 and 4: Development and Evaluation — The findings from the studies presented in Chapters 4 to 6 were distilled into the design guidelines presented in Table 7.1 to produce alternative web browser security control UIs. This yielded two main artefacts as part of the DSR outcomes, namely SecAdapt V1 (SV1) and SecAdapt V2 (SV2) with minimal modern and user-centric designs as an instantiation of IS artefacts to be evaluated. For SV1, the focused was mainly to improve user's interaction with cybersecurity controls. The goal of the SV2 prototype design is to introduce and evaluate the concept of personalized adaptive security within web browsers for non-expert users. At Stage 5: Conclusion — the discussions of the research outcomes and contributions made to the knowledge base would be presented in Chapter 5.

7.3 User Experience and User-Centred Design Elements

The guidelines outlined in Table 7.1 were used in conjunction with user experience framework proposed by Garrett [4] for web application interface designs (see Figure 7.2). The framework provides industry-standard design guidelines right from the idea generation stage through to the implementation of software applications. Consequently, the two prototypes though not fully implemented as desktop applications were designed following the engineering guidelines described in the framework. The framework decomposes an interface design project into five main layers. The framework adopts a bottom-up approach to addressing user experience problems during design whereby issues move from abstraction in the lower layers to concrete solutions at the top of the layer. The layers are briefly described for the context of this thesis project as follows:

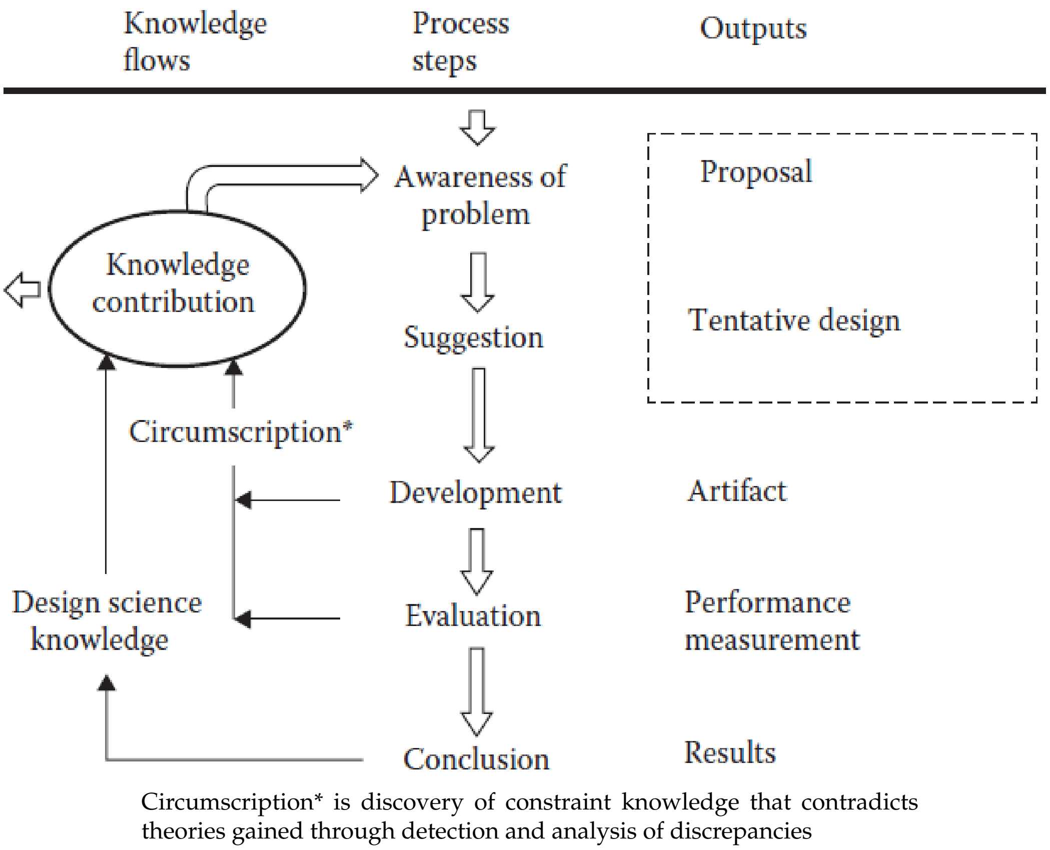


FIGURE 7.1: DSR process model [3]

- Surface — Make the visual designs concrete for users to interact with and simulate the performance of various security and privacy functions within the prototype.
- Skeleton — Design the skeleton taking into account the arrangement of interface components to achieve maximum efficiency and effectiveness during use. Finalize the design components, navigation options and how information would be presented on the screen for users.
- Structure — Define the user interaction steps and options based on the specifications identified in the Scope.
- Scope — Specify the functional requirements and features of the applications as well as resources required to support decision making.
- Strategy — Identify user needs and formulate the application objectives.

7.4 Aspects of the Proposed Prototype Designs

7.4.1 The Strategy

Two main design options emerged from devising the prototype development strategy. The first design option yielded the interactive prototype browser named SecAdapt

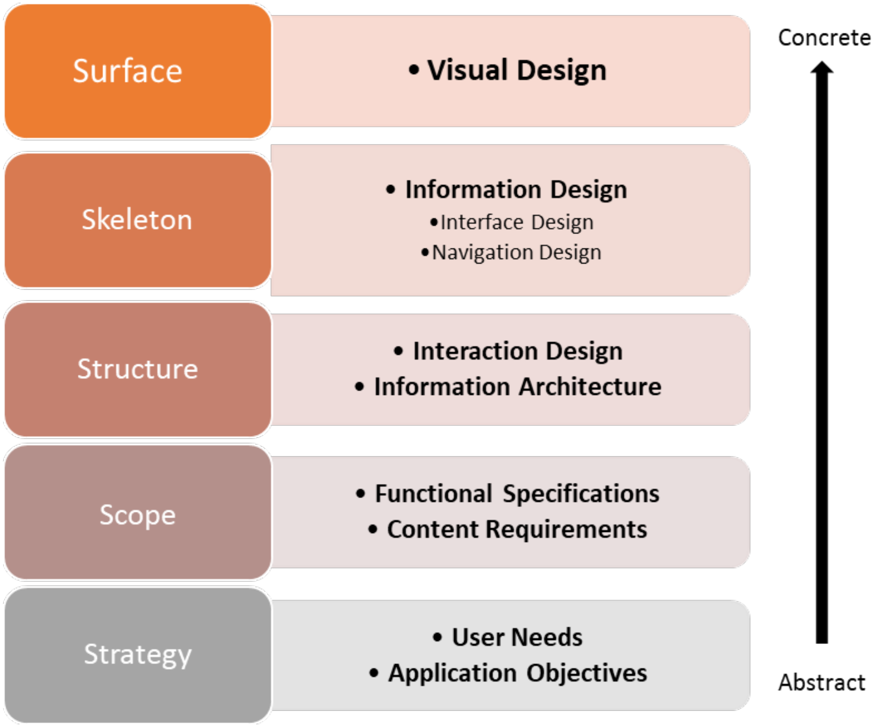


FIGURE 7.2: Elements of Good User Experience Design [4]

V1. This version of the prototype focused on addressing usability issues in the UI of browser security controls. The second option focused on the design of adaptive automation in browser security controls. In the past, decisions on Levels of automation (LOA) were determined with programmable logic at the design and development stage. With advances in machine learning and artificial intelligence, Adaptive Automation (AA) have emerged to replace the traditional approach to automation. AA allows the LOA to be controlled by both the user and the automated system to better maximise the benefits of automation and reduce its negative impact on human performance and cognition. Thus instead of allocating functions between humans and machines during system design (static function allocation), adaptive automation allows tasks to be reassigned based on the context within which the system is being used [5].

Feigh et al. [5] developed a two-part framework for characterizing AA during system design and development. The first part of the framework characterises adaptation triggers and methods used to determine actions that dictates the occurrence of adaption. The second part is a taxonomy of adaptation describing various ways and levels at which human-machine systems' interface and behaviour can be adapted. In this thesis, the AA framework is adapted for adaptive cybersecurity design which provided a design space for generating possible user interactions for the SV2 prototype. As shown in Figure 7.3, the first part of the frameworks substantially represent the Bayesian-based model for adaptive cybersecurity developed in Chapter 6. In so doing, a Bayesian matching engine designed for personalized adaptive cybersecurity would manage the adaptation triggers for the proposed prototype. The adaptive behaviour for SV2 would

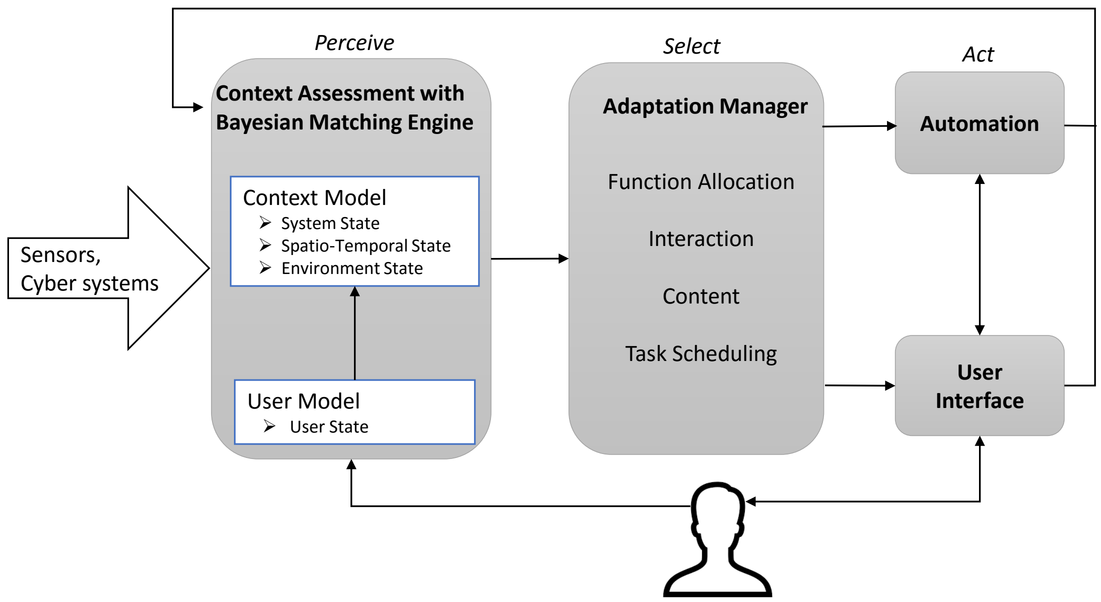


FIGURE 7.3: Adaptive Automation Depiction for Cyber Security Design [5]

thus be characterised by both the adaptation types available and Bayesian-based model supporting the decision of when and how adaptation will occur (adaptation triggers).

The adaptive component proposed for the second prototype SV2 is ultimately an agent that will assist users with cybersecurity-related tasks while working with a web browser. SV2 need to be designed to first display a small set of security-related interactions to the user with recommendations on which interaction to activate. SV2 can then use a set of quantitative measures of the users' interactions and other available metrics to determine the user's preferences in terms of the best security settings to optimize at a given time while using the web browser. Consequently, the following adaptations are anticipated to be provided to the user:

1. automatically generate personalized UI to improve user interaction with the in-built web browser security features.
2. automatically adapt web browser security and privacy settings to meet user security goals with personalized user interaction during active browsing session based on user behaviour and browsing data.
3. Unless very critical, the security recommender service will mostly be in standby mode with very limited notification message within a specified time-frame which can also be made adaptable to the user. This is to allow the user to work with the browser at a prolonged period of time with very minimal interruption from the browser's security engine to avoid annoyance with the system and possibly leading to it being disabled by the user.

7.4.2 The Scope

The design guidelines presented in Table 7.1 applied to standard modern browser security features, characterised the scope for SecAdapt V1. This scope is extended for SV2 to include adaptive features as outlined in subsection 7.4.2.1.

7.4.2.1 Core Features of SecAdapt V2

1. User Registration
   - Appears the first time the web browser is run
   - Allows the user to register with the SecAdapt application through the web browser sync settings
   - Enables the user to customize his/her profile account and preferences (e.g., e-mail and other personal information can be modified)
   - Enables the user to indicate/adjust their preferred level of privacy and secured interaction
   - Enables the user to indicate his/her feature preferences including interface options and type of data to be used for personalization
2. Show Security/Privacy Task Feedback
   - Enumerates all of a user's unresolved security/privacy warnings
   - Provide easy access to relevant security tips and tools
   - Offers the option to resolve previous warnings/alerts or recommendations
3. Help Menu
   - Displays a list of topics covering the different components of SecAdapt
   - Offers detailed information on each menu and feature
   - Accessible at any time on the settings menu
4. Push Notifications
   - Appear after any significant cybersecurity automation event occur in the web browser
   - Alert a user of new security features and updates
   - Remind users of unresolved security threats or recommended task
5. Context Aware
   - Stores contextual data (e.g. location, time, frequency of use etc.) associated with certain browser events and security tasks. For the prototype application we can demonstrate the adaptation capabilities using the following contextual parameters:

- Type of navigation label. Values: graphical or textual links
- Frequency of accessing a menu item
- Intensity of mouse movement
- Time and activity after login
- Device type. Values: desktop, laptop or mobile
- Location

The main component of both prototypes are the UI to be used in managing cybersecurity within the web browser application. The prototypes should be designed to run on Windows operating system relying on Firefox's built-in security controls accessible through its Application Programming Interface (API). Figure 7.4 provide an overview of the minimum implementation requirement of these core features in order to effectively evaluate adaptive automation functions in SecAdapt V2.

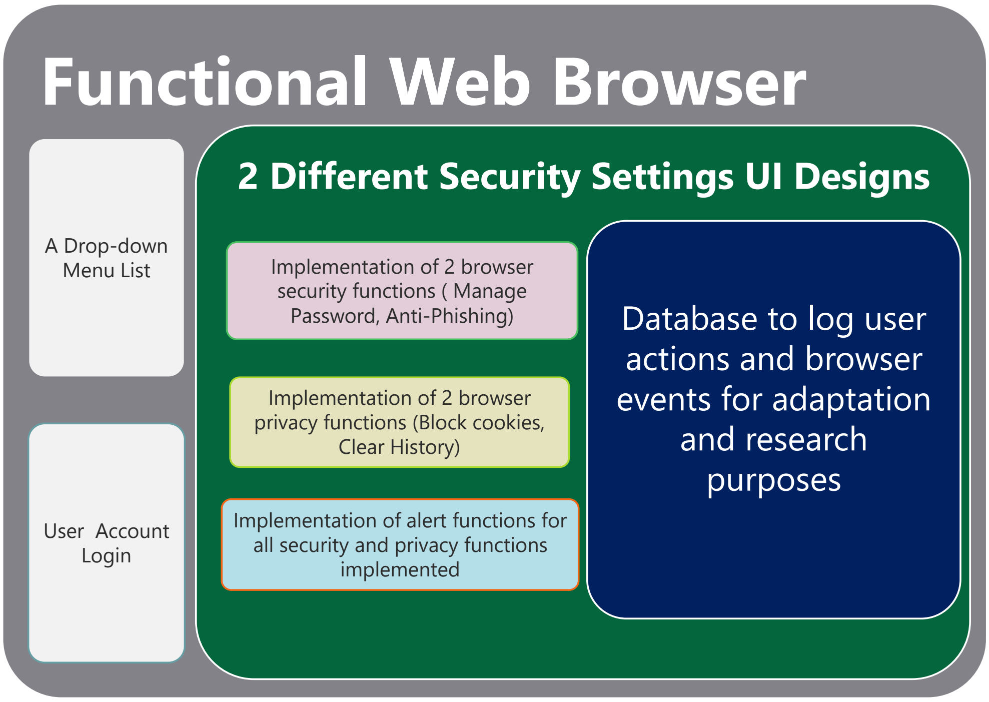

Functional Web Browser
A Drop-down Menu List
User Account Login
2 Different Security Settings UI Designs
Implementation of 2 browser security functions (Manage Password, Anti-Phishing)
Implementation of 2 browser privacy functions (Block cookies, Clear History)
Implementation of alert functions for all security and privacy functions implemented
Database to log user actions and browser events for adaptation and research purposes

FIGURE 7.4: Outline of the minimum implementation requirement for SecAdapt V2

7.4.3 The Structure

The features defined in the scope needs to be developed to allow for user interaction and evaluation. Here I considered four main security and privacy cases with scenarios that may require a user to interact with the proposed web browser security controls. These were later converted into a task sheet for the evaluation of the prototype designs (see Appendix D). Prototypes are generally used to assess the usability and user behaviour towards new application design concepts before moving towards actual development and implementation [330]. Walker et al. [331] defined an interface design

TABLE 7.1: Design guidelines for usable browser security UI

Design Indicators	**Description**
1. Language	Use plain language that even non-expert can understand to avoid confusion and minimize mental workload
2. Learnability	The interface should be intuitive enough for users to quickly determine what steps they need to take to achieve specific goals
3. Feedback	Provide visible feedback to clearly indicate outcome of user actions or non-actions
4. Error prevention or recovery	Users should be warned about some of the settings implications and critical actions need to be confirmed before execution.
5. Flexibility and efficiency	Organize interface items based on relevance or user preference to allow both experienced and novice users to quickly perform desired tasks and minimize delays.
6. Consistency	Provide consistent labelling and organization of controls throughout the application for consistency and clarity using colors, fonts and widgets.
7. Effectiveness	Users should be presented with help options to allow them complete not so obvious security case tasks such as back-up and encryption.
8. Visibility	Security and privacy controls should be clearly labelled and described to aid users understanding of their prevailing security and privacy status within the browser.
9. Aesthetic and minimalistic design	Focus on a simple uncluttered interface layout that meet modern design standards.

prototype as a working model of a software application that can be used to test design ideas. Prototypes allow software designers and engineers to examine content, aesthetics, and interaction techniques from the perspectives of all stakeholders.

Factors such as design constraints, application objectives, time pressure and financial liabilities need to be considered in choosing the level of fidelity required for usability testing of a proposed software application. For instance, low fidelity prototypes may be cheaper and take less time to be built but may not meet the requirement for usability testing depending on the application objectives. For this project, a high fidelity working prototype proved to be too time-consuming and expensive so I decided on a medium fidelity prototype designed to mimic a fully functional prototype that users can actually interact with. This is to ensure that the features are fully illustrated and tested for suitability through the UI prototype before moving towards the development of a functional prototype. Research has shown that reduced fidelity prototypes used in user testing are able to produce similar findings as their functional counterparts. [331–333]. Designing a medium fidelity prototype allowed us to focus on the architectural and interaction design with the added advantage of low cost and ease of iteration.

7.4.4 The Skeleton: Iterative Design

Following the identification of the main issues inhibiting the adoption of web browser security controls by non-expert users, a team was put together to explore the design space for more usable interfaces. This started with an ideation phase over the themes discussed in Chapter 4, brainstorming, and lightweight sketching of multiple designs to improve on the three browser UIs evaluated earlier on (see Appendix E for preliminary sketches and feedback used to improve them). The sketches were later converted into computer-based mock-ups using PowerPoint. The mock-ups were iterated several times and refined by feedback before settling on the final interaction design for the prototype. The final skeleton modified how security control objects are categorised and labelled. The SecAdapt home page itself is designed to **1**: promote cybersecurity awareness among users and **2**: minimise mental workload through a simplified menu for easy navigation to security controls (see Figure F.1 in Appendix F). The language used to describe the controls were also modified and made simpler eliminating most of technical terms users complained about in existing interfaces (e.g. cookies JavaScript etc.). The data protection functionality aspect was also redesigned to be more visible and fully integrated into the browser's security controls. A dashboard was introduced to provide a wholistic view of the browser security and privacy status to users – Figure 7.5.

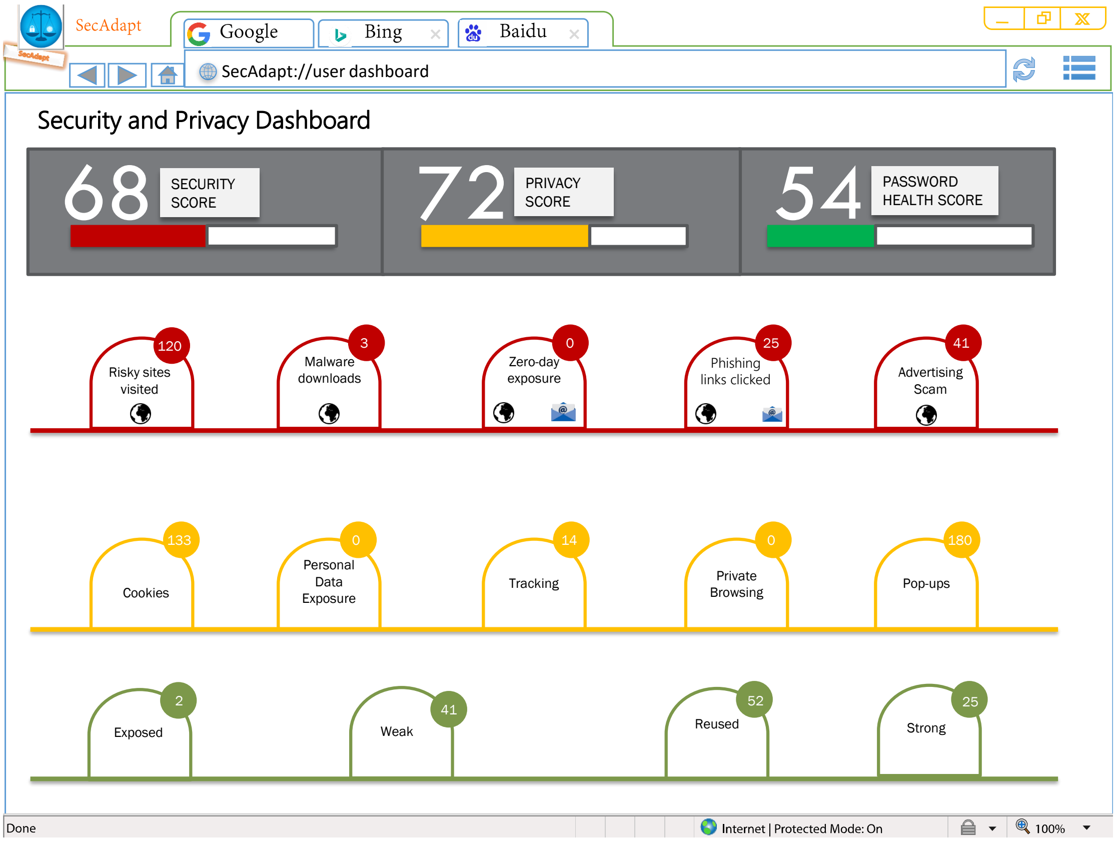
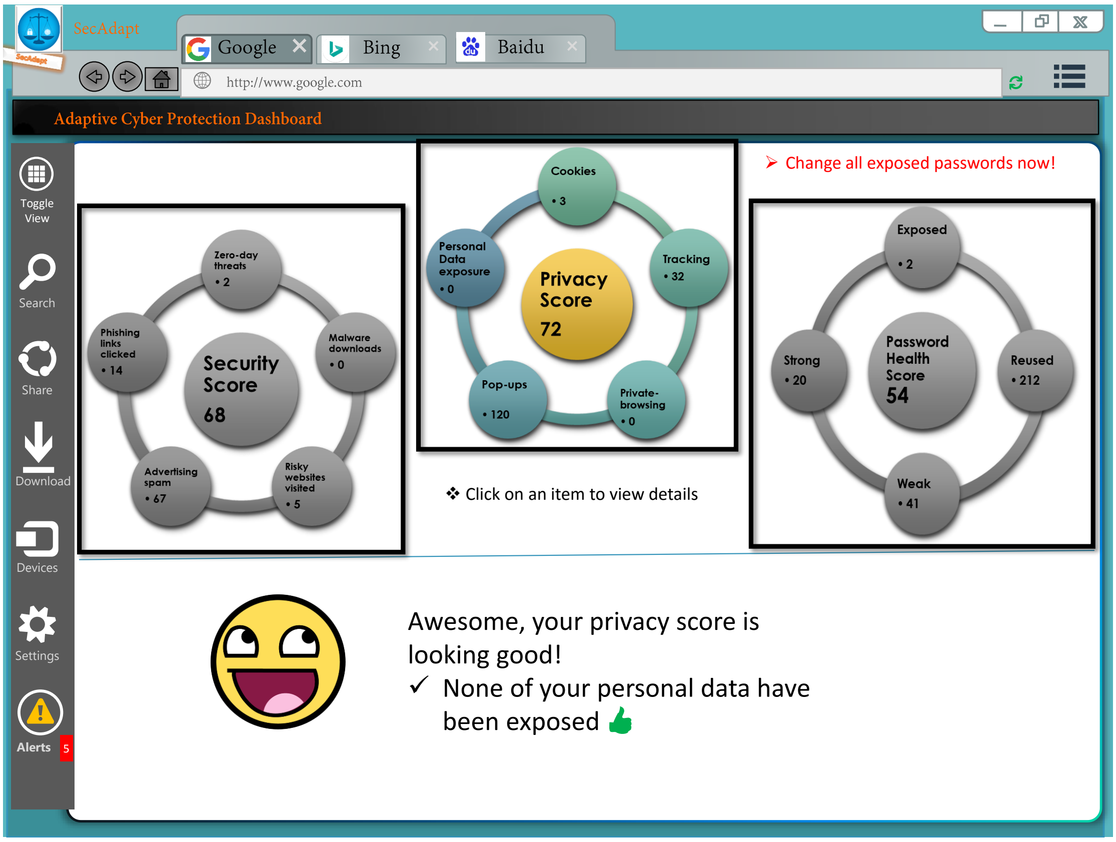


FIGURE 7.5: Screenshot of the user dashboard in SecAdapt V1

In SV2, the user dashboard was designed to illustrate the adaptive cybersecurity concept hence the interaction design was personalized for users whenever the adaptation manager is enabled (Figure 7.6). The dashboard in SV2 was also designed to be a one-stop interface for handling all of the user's cybersecurity and privacy goals following an initialization of the adaptive automation functions in the browser. Multiple designs were proposed for the modifications identified for both SV1 and SV2. The designs were discussed by the research team for validation before they were converted into the prototypes described in the following section.



➤ Change all exposed passwords now!

❖ Click on an item to view details

Awesome, your privacy score is looking good!

✓ None of your personal data have been exposed 👍

FIGURE 7.6: Screenshot of the adaptive user dashboard in SV2 highlighting the privacy score of the user

7.4.5 The Surface: Interactive Prototypes

Two medium-fidelity, interactive prototypes were created using Ms PowerPoint to improve how users perceive and interact with cybersecurity controls in web browsers. Visual Basics for Applications (VBA) was used to write macros for most of the controls in the prototype to simulate a functioning system. Several aspects of version two of the prototype were implemented using the Mozilla build virtual machine (VM)[1] as well as JavaFX WebView. JavaFX integrated into NetBeans IDE provided a platform to quickly design and implement the interface in Java simply by accessing the UI components in Scene Builder which is a visual layout tool. The JavaFX WebEngine class was used to

[1] https://developer.mozilla.org/en-US/docs/Mozilla/Developer_guide/Using_the_VM

support user interaction design implementation in SV2. Specifically, the JavaFX web components together with the Scene Builder was used to generate an FXML file for the prototypes. This can later be used to implement a fully functional SecAdapt by combining it with a Java project to bind the UI to the application's logic. The final designs were converted into PowerPoint Macro-Enabled Show (.ppsm files) and labelled as SecAdapt V1 and SecAdapt V2 accordingly. This prevented them from opening as a PowerPoint document to mimic a desktop application that can be run by the user from the desktop by double clicking on them like other desktop applications — see Appendix G for screenshots of some of the interaction implementation in SV2.

Apart from developing macros for the prototype functionalities, other PowerPoint features like action settings, animation, hyperlinks, embedded objects and add-ins were fully utilised to produce more realistic user interactions for the usability testing. Consequently, users were able to navigate through the two prototypes to explore the predefined features and react to the system design concepts. For the SV2, a fully functional password manager called Dashlane was integrated into the prototype to better simulate the concept of the adaptive automated functions. Thus the Dashlane interface was used to perform task 4 in SV2 rather than the UI designed for password manager in SV1. Figure 7.7 presents an example screenshot of the interface design in SV2 (See Appendix F for more screenshots of the medium-fidelity prototypes).

Overall, the proof of concept prototypes were purposely designed to have a non-technical and a modern aesthetic feel which were part of the main themes captured during the initial user experience analysis reported in Chapter 4.

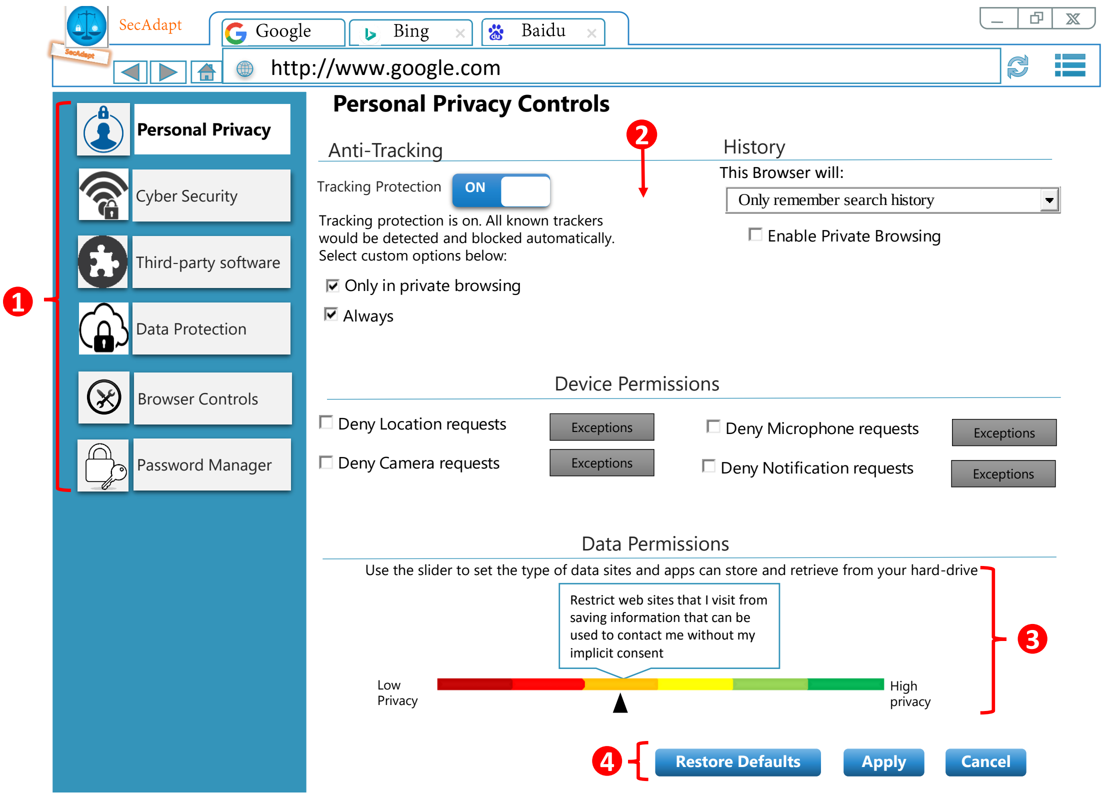
7.5 Evaluation

A usability study was conducted to evaluate the medium fidelity prototypes. The objectives of the evaluation are in two folds:

1. Measure and compare the usability of the prototype UI to existing interfaces designed for browser security controls.
2. Elicit users' feedback and reactions to the design concepts and the adaptive automation features to make recommendations for revisions if necessary.

7.5.1 Study Design

Although the objectives are slightly different, the study was designed to be identical to the user experience analysis study reported in Chapter 4. This was to allow for a similar dataset to be gathered for the comparison analysis. The main difference between the two set-ups has to do with the applications being evaluated which are the two prototypes — SV1 and SV2 and one fully functional browser – Firefox (FF). The



Personal Privacy Controls

Anti-Tracking

Tracking Protection ON

Tracking protection is on. All known trackers would be detected and blocked automatically. Select custom options below:

☑ Only in private browsing

☑ Always

History

This Browser will: Only remember search history

□ Enable Private Browsing

Device Permissions

□ Deny Location requests

□ Deny Camera requests

□ Deny Microphone requests

□ Deny Notification requests

Data Permissions

Use the slider to set the type of data sites and apps can store and retrieve from your hard-drive

Restrict web sites that I visit from saving information that can be used to contact me without my implicit consent

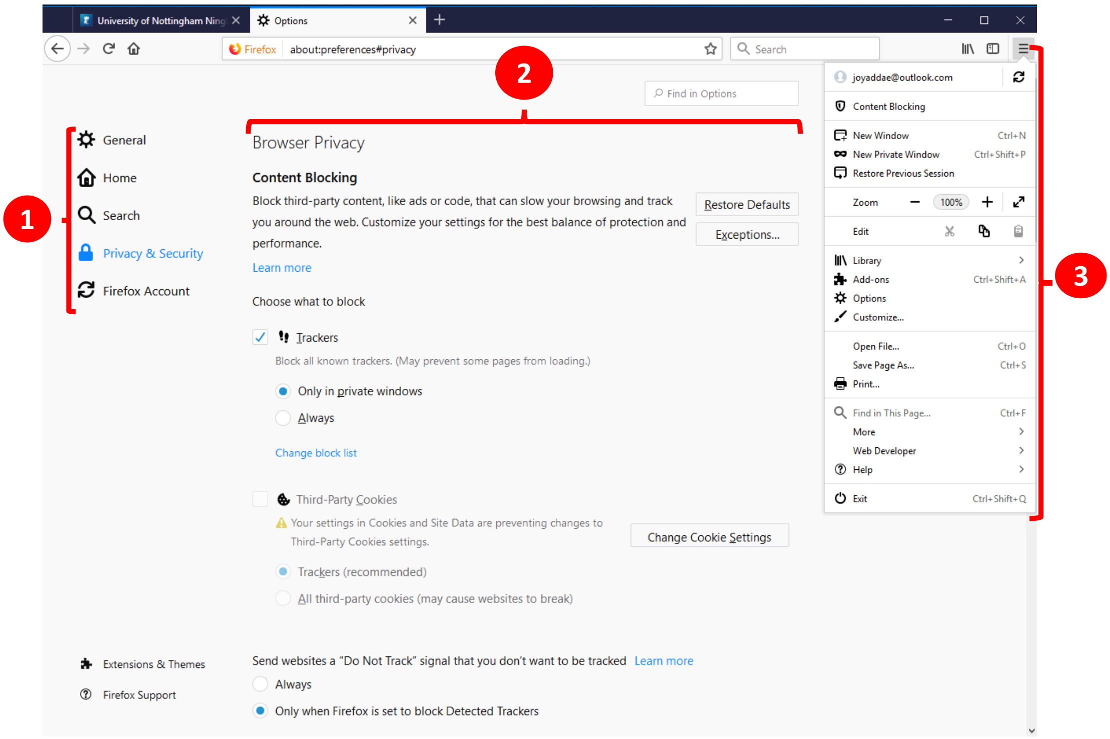
Low Privacy

High privacy

FIGURE 7.7: Screenshot of the main privacy interface for SecAdapt V1 – **1**: List of controls categorized and labelled with representative icons for consistency and clarity. **2**: The settings page reorganized to achieve an uncluttered design **3**: Privacy slider to help users visualize data permission options quickly with popup description provided for each level (colored block) and a lever that sets and shows the current permission/privacy level. **4**: Buttons provided to support undo and redo functions on all settings pages to aid error recovery and give the user enough control and freedom.

three browsers were setup on Windows 10 laptops with webcams and microphones in a room specifically booked for the experiment. A primary goal of this study is to test the prototypes against an existing browser with a security control interface. Firefox was selected because, its security interface had the highest usability score in the previous study. Consequently, Firefox's security UI and architecture served as the baseline for usability improvement during the design of the prototypes. Moreover, Firefox is an open-source browser which is relatively well-known among our target users. The latest version of Firefox (63.0.3) as at the time of this evaluation was thus chosen for the comparison study — see Figure 7.8.

Think-aloud protocols and the System Usability Scale (SUS) were used to evaluate the usability of the three UIs and to elicit feedback on the pros and cons of the design concepts and features. Think-aloud is a technique that is commonly employed in usability testing to elicit feedback on proof of concept designs. Thinking aloud while completing tasks is noted for providing more accurate accounts of behaviour as the need to rely on memory recall is eliminated. This also allowed for a better understanding of how the prototype performed from the user's perspective.



Browser Privacy

Content Blocking

Block third-party content, like ads or code, that can slow your browsing and track you around the web. Customize your settings for the best balance of protection and performance.

Learn more

Choose what to block

☑ Trackers

Block all known trackers. (May prevent some pages from loading.)

● Only in private windows

○ Always

Change block list

□ Third-Party Cookies

Your settings in Cookies and Site Data are preventing changes to Third-Party Cookies settings.

● Trackers (recommended)

○ All third-party cookies (may cause websites to break)

Send websites a "Do Not Track" signal that you don't want to be tracked Learn more

○ Always

● Only when Firefox is set to block Detected Trackers

1: Lack of adequate visibility of available security controls as some are hidden from the main interface e.g. password manager, backup and encryption. **2:** Cluttered interface combining both security and privacy controls with lots of text for users to sieve through **3:** The main drop-down menu list for accessing the browser's controls has too many items that could easily be grouped together to minimize mental workload when searching for specific options.

FIGURE 7.8: Screenshot of the version of Firefox security interface evaluated together with the prototypes with some of the usability issues participants encountered.

The four security case scenarios and corresponding tasks used in the previous study were also modified slightly to incorporate the adaptive feature use cases (see Appendix D). The first scenario involved protecting the browser against dangerous downloads and prevention of malware infestation. The second scenario is concerned with privacy requiring users to carefully consider and effect the necessary controls to elevate their personal privacy status. The third scenario required participants to take measures in protecting their personal and browsing data stored by the browser (backup and encryption). Finally, the fourth scenario involved the use of the password manager to manage login details saved by the browser. This resulted in a 4x3 within-subject (Repeated-Measures) study design, whereby each participant was required to perform the four study tasks using both prototypes and the Firefox web browser.

7.5.2 Procedure

After piloting the study tasks and making revisions, representative users were enlisted to test the 3 UIs. Participants were recruited through poster distribution on mailing lists and social media (WeChat, WhatsApp). The poster was designed with a barcode that volunteers can easily scan and sign-up as participants. The sign-up process involved choosing a time slot with a Doodle poll link used to schedule the study session for participants. A pre-study demographic survey was completed by each participant before commencing the study tasks. At the beginning of each session, the participant was instructed on how the experiment would be recorded and how to proceed through the tasks. Participants were asked to verbalize their thoughts as they perform the four security case tasks with the interactive prototypes and Firefox on a laptop configured specially for the study. The order in which the browsers were used was random but most participants preferred to start with the Firefox browser. Participants were given the SUS survey to complete after completing the four tasks with one browser. They would then complete the tasks and SUS survey for the other two browsers.

A semi-structured interview was conducted for each participant once the think-aloud task session is completed for the prototypes. In this interview, the adaptive automation mechanism is first explained to the participants, i.e., how certain features would be adapted and personalized for the user based on information voluntarily provided by the user and other metrics. Participants views were then sought out about the design concepts embodied by the prototype, what they liked and/or disliked, and how useful they found the features. Feedback was also gathered on how the design concept might be improved. The entire session involving the think-aloud protocol and post-interview lasted for approximately 45 minutes to an hour per participants. Each session was video recorded with the consent of the participant using the Morae software described in Chapter 4. Participants were compensated with 16GB customised USB drives after they complete the entire session.

7.5.3 Data Analysis

The data was analysed both qualitatively and quantitatively using inferential and descriptive statistical methods to measure and compare usability of the UIs evaluated. The three main usability metrics discussed in Chapter 3: effectiveness, efficiency and satisfaction defined by ANSI/ISO [153, 154] informed the overall analysis. Dependent variables such as task time, completion and error rates were used to measure the effectiveness and efficiency. Satisfaction, on the other hand, were measured based on participants feedback through the think-aloud protocol and the SUS survey. Specifically, statistical analysis was conducted on the security cases and individual task time metrics as well as the error counts to determine which of the security interface designs was more effective. Subsequently, the performance metrics of task time, error count, and satisfaction score were analysed together with the qualitative data gathered to assess the strength and weaknesses of the proof of concept design for personalized adaptive cybersecurity.

7.5.4 Participants

Table 7.2 summarizes the demographics of the participants. A total of 36 participants took part in the study of which 55.6% were male and 44.4% females. Participants age ranged from 18 to 44 years. About 80% of them had completed bachelors or masters degree, and either worked at, or near, or studied at the university where the study was conducted. Although the study participants were mostly Asians and/or Chinese (Figure 7.9), the pool of academic discipline and professional background reported was very diverse. Similar to the previous user study, most of the participants self-rated their general computer skills and cybersecurity experience level at 2 or 3 on a scale of 1 to 5 (see Figure 7.10).

TABLE 7.2: Summary of Participants' Demographics

Demographic	Frequency	Percent
Gender		
Female	16	44.4
Male	20	55.6
Total	36	100.0
Age Group		
18 - 24 years	9	25.0
25 - 34 years	22	61.1
35 - 44 years	5	13.9
Total	36	100.0
Education Level		
Graduate degree/ professional	19	52.8
Bachelor's degree	10	27.8
Some college, no degree	2	5.6
High school diploma or less	5	13.9
Total	36	100.0

7.6 Results

7.6.1 Efficiency and Effectiveness

The study produced quantifiable data to objectively measure and compare the usability of the three browser security UIs evaluated. The quantitative data were prepared for analysis using IBM SPSS Statistics 25 [334]. The main objective of the quantitative analysis of the dataset is to compare and determine which of the three browsers' security UI design concept is most effective and efficient.

Task Success Rate

Task completion and error rates constitute measures of effectiveness [160]. As shown in Figure 7.11, much higher success rates were recorded for task 1 to 3 with the two versions of the prototype compared to that of Firefox. The main failure rate for Firefox occurred in Task 1 (Malware prevention) and 3 (Data backup and protection). For

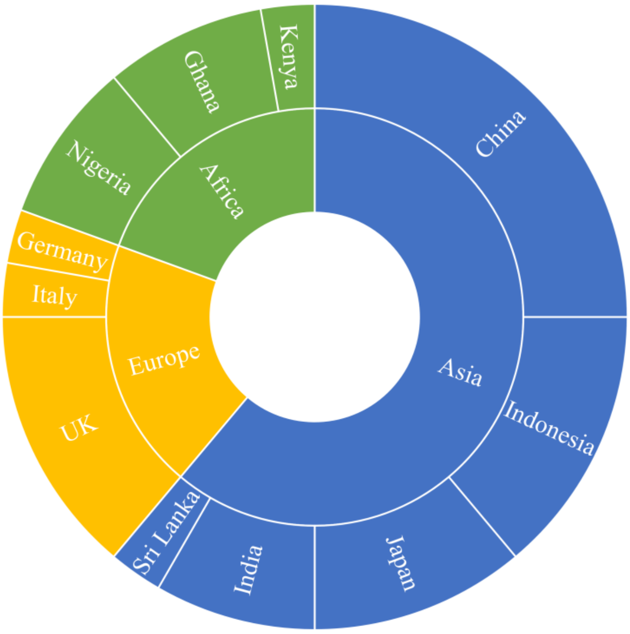


FIGURE 7.9: The pool of participants' nationality

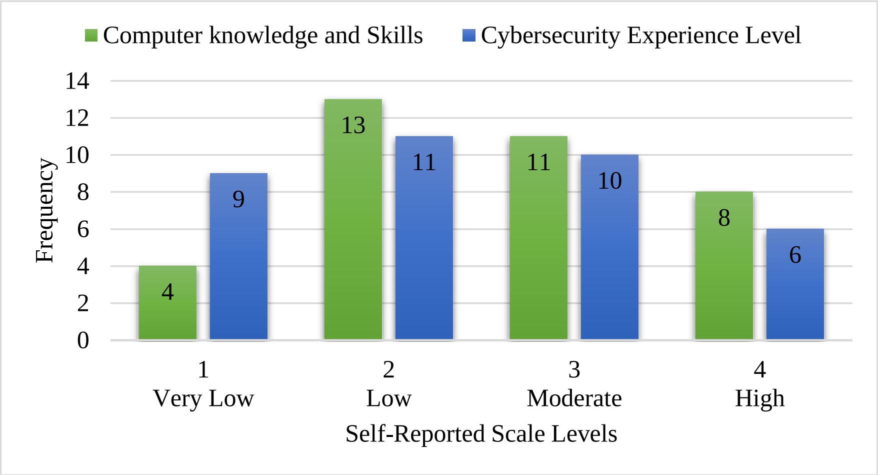
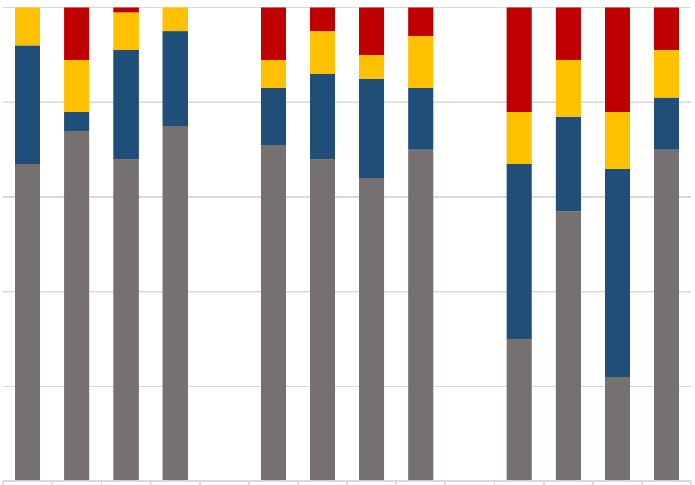


FIGURE 7.10: Participants' self-reported computer and cybersecurity experience levels

task 1, this was mainly because, the controls for security and privacy has been bundled up together and presented on a single page in the version of Firefox evaluated. Consequently, users found it difficult to locate the settings for security and malware prevention. Participants also struggled with Task 3 mainly due to the invisibility of the control for data backup in Firefox. Participants generally could not discover the configuration page without turning to search engines for the procedure which when found seemed too cumbersome. However, the success rate for task 4 is the same for Firefox and SV2. Overall, task success was consistently higher with SV1 followed by SV2.

Error Count

The distribution of errors counted by task is presented in Figure 7.12 with four levels of severity on usability. The importance of categorising the severity of identified



	Task 1	Task 2	Task 3	Task 4	Task 1	Task 2	Task 3	Task 4	Task 1	Task 2	Task 3	Task 4
	SecAdapt_V1				SecAdapt_V2				Firefox			
🟥 Failed to complete	0%	11%	1%	0%	11%	5%	10%	6%	22%	11%	22%	9%
🟨 False Completion	8%	11%	8%	5%	6%	9%	5%	11%	11%	12%	12%	10%
🟦 Completed with difficulty	25%	4%	23%	20%	12%	18%	21%	13%	37%	20%	44%	11%
■ Completed with ease	67%	74%	68%	75%	71%	68%	64%	70%	30%	57%	22%	70%

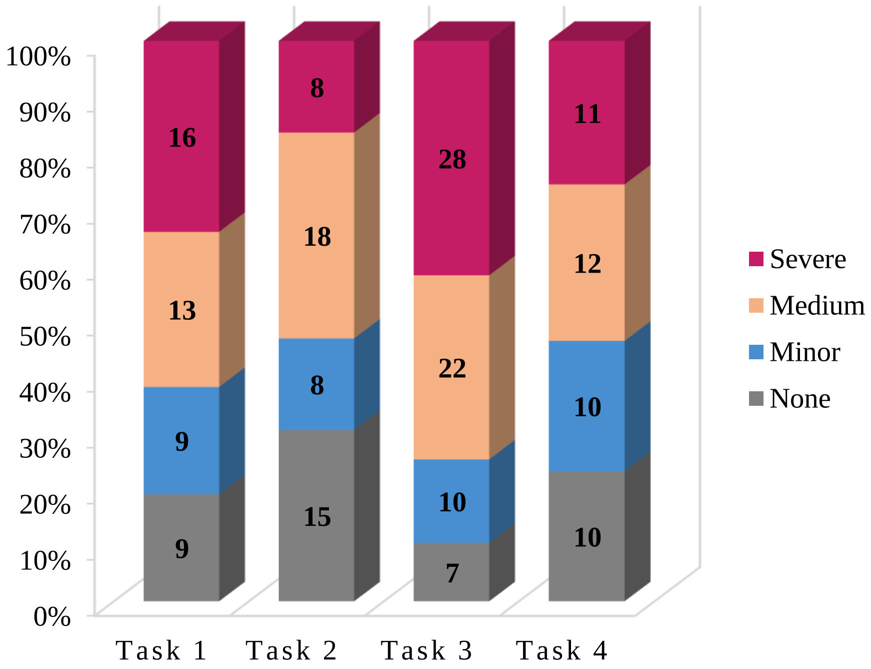
FIGURE 7.11: Task success distribution by browsers

usability problems has been emphasized in the literature as discussed in Chapter 4. Consequently, a combination of categorization approaches found in the literature was adapted and used in scoring each user and system error logged. The scoring was primarily based on the impact of the error on performance of the study task or emotional state of the participants.

TABLE 7.3: Error count summary by browsers

Browser	**T1_EC Sum**	**T2_EC Sum**	**T3_EC Sum**	**T4_EC Sum**	**Total** N=36
Firefox	24	17	32	19	92
SecAdapt V1	8	6	11	9	34
SecAdapt V2	11	4	8	16	39
Sum	43	27	51	44	165
Mean	14.33	9.00	17.00	14.67	55.00
Std. Deviation	0.55	0.43	0.67	0.57	

The error log appears to be consistently high on Task 1 – Malware Prevention, with a recorded error count of 17, 10 and 11 for Firefox, SV1 and SV2 respectively (see Table 7.3). As summarised in Table 7.4, Firefox logged a significantly higher number of errors on all the security use cases except for Task 4 where no significant difference was yielded by the Friedman test conducted. The most common error logs on Task 3 – Data Protection, had to do with participants mistaking saved logins on the password manager interface for the profile folder that they were required to backup. Instead of navigating to the application basics page to find their profile folder, most participants tried to complete the task on the main settings page in Firefox. This was captured as a



None: not a usability problem; **Minor**: causes some frustration and brief delay; **Medium**: causes moderate frustration and significantly delays user**; Severe**: causes severe frustration leading to task failure.

FIGURE 7.12: Severity of all errors logged with the three browsers by task

usability error because the interface design requires participant to leave the main options page to find the help icon on the browser's first menu list before they can navigate to where to find their profile folder. This error was severe enough causing participants to abandon the task and in some cases leading to false completion. A significant number of errors was also logged on Task 4 for Firefox and SV2, indicating a usability issue in the current interface design for password management in Firefox and Dashlane.

Task Completion Duration

The mean Task Time to complete each of the four Tasks for all three browsers is presented in Table 7.5, along with other descriptive statistics. Task time metrics are used to measure the efficiency of each browser's security interface design. Apart from security case 3, the mean task time durations for completing the study tasks are quite similar across the three UIs evaluated (Figure 7.13). A Friedman Test conducted to compare the actual time on task between the browsers however, revealed significant differences for all security cases except case 4 (see Table 7.6).

The task time values for SV1 was significantly lower across the four security cases with recorded 3.72, 3.07, 3.47 and 4.55 minutes as the mean time to complete task 1 to 4 respectively. For SV2, because of the added step of registering for the adaptive automation features, it was quite expected that participants would spend more time on task 1 in SV2 than in SV1. However, because the registration step is a one-time event it

TABLE 7.4: Friedman Test results for error count differences by browser

Task	Browser	Mean Rank[a]	N	Chi-Square	df	Asymp. Sig.
Task 1	**SecAdapt V1**	**1.81**	36	8.197	2	0.017
	SecAdapt V2	1.93				
	Firefox	2.26				
Task 2	**SecAdapt V2**	**1.83**	36	8.656	2	0.013
	SecAdapt V1	1.90				
	Firefox	2.26				
Task 3	**SecAdapt V2**	**1.75**	36	9.977	2	0.007
	SecAdapt V1	1.93				
	Firefox	2.32				
Task 4	**SecAdapt V1**	**1.81**	36	4.528	2	0.104
	SecAdapt V2	2.04				
	Firefox	2.15				

a. Mean rank of error count displayed in ascending order

did not impact on the remaining tasks. The results show that task time values for security case 2 was significantly lower for SV2 (Mean = 2.85 minutes) than SVI (Mean = 3.07 minutes) and FF (Mean = 4.36 minutes). In contrast, FF appeared to be significantly less efficient in completing the security case tasks except for Task 4 where the difference between the task time mean was not significant. Even though the difference for security case 4 task – Password Manager, was not statistically significant, participants generally took less time completing the task with the UI designed for SV1 as displayed in Figure 7.13.

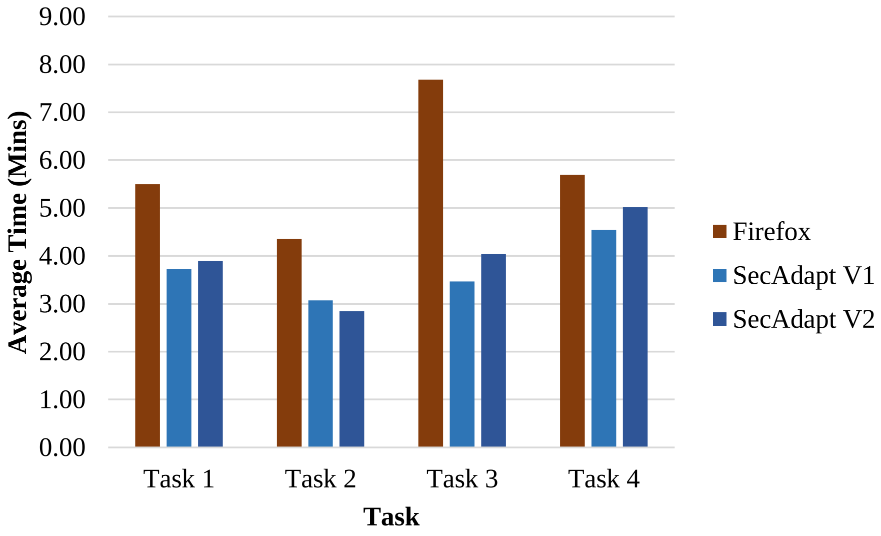
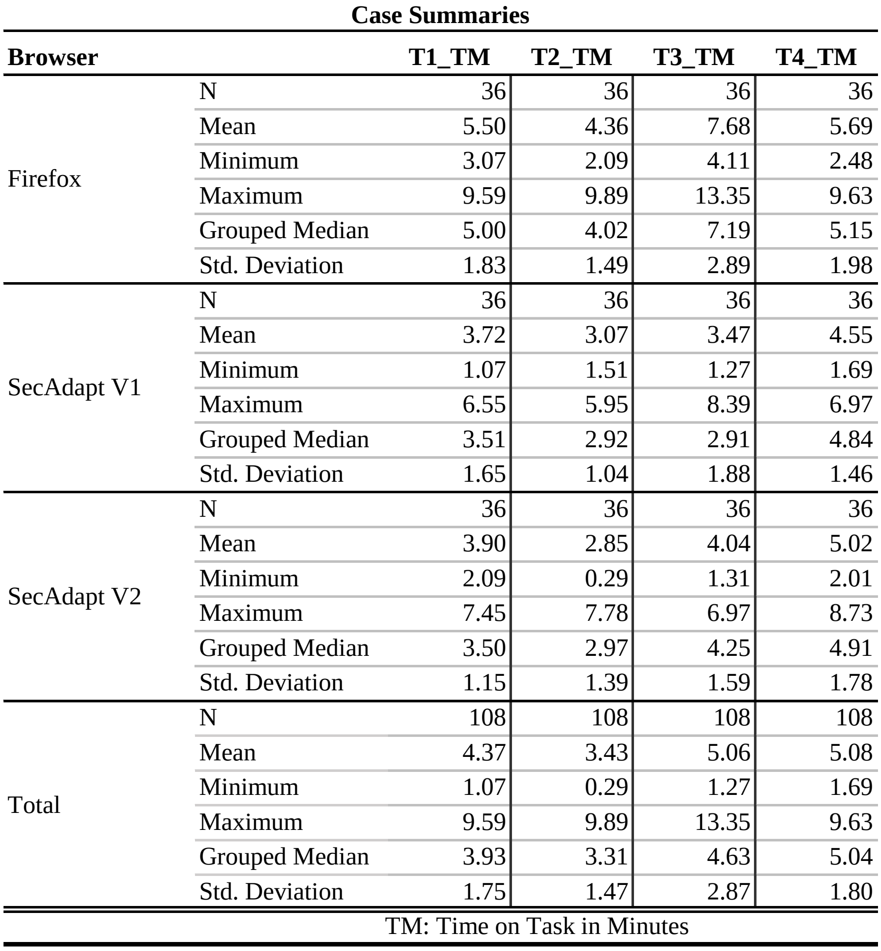


FIGURE 7.13: Average Time on Task by Browser

TABLE 7.5: Time on Task Summary by Browser

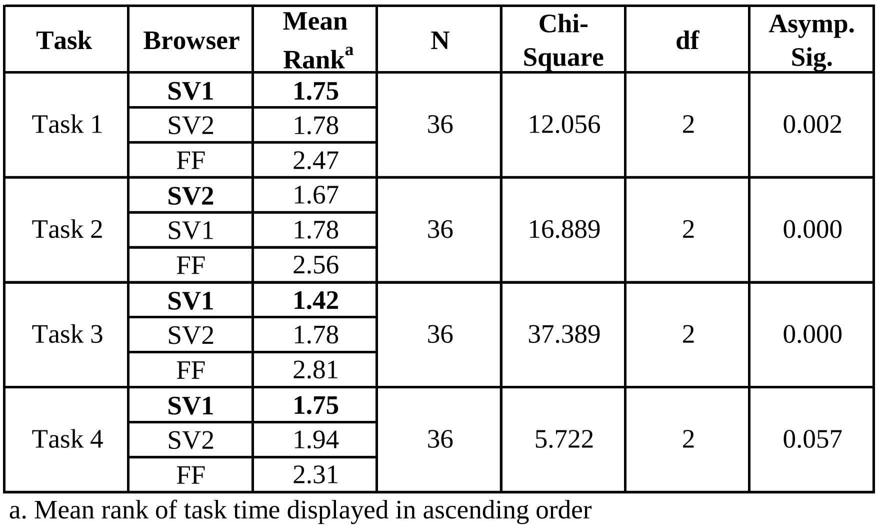


Case Summaries

Browser		**T1_TM**	**T2_TM**	**T3_TM**	**T4_TM**
Firefox	N	36	36	36	36
	Mean	5.50	4.36	7.68	5.69
	Minimum	3.07	2.09	4.11	2.48
	Maximum	9.59	9.89	13.35	9.63
	Grouped Median	5.00	4.02	7.19	5.15
	Std. Deviation	1.83	1.49	2.89	1.98
SecAdapt V1	N	36	36	36	36
	Mean	3.72	3.07	3.47	4.55
	Minimum	1.07	1.51	1.27	1.69
	Maximum	6.55	5.95	8.39	6.97
	Grouped Median	3.51	2.92	2.91	4.84
	Std. Deviation	1.65	1.04	1.88	1.46
SecAdapt V2	N	36	36	36	36
	Mean	3.90	2.85	4.04	5.02
	Minimum	2.09	0.29	1.31	2.01
	Maximum	7.45	7.78	6.97	8.73
	Grouped Median	3.50	2.97	4.25	4.91
	Std. Deviation	1.15	1.39	1.59	1.78
Total	N	108	108	108	108
	Mean	4.37	3.43	5.06	5.08
	Minimum	1.07	0.29	1.27	1.69
	Maximum	9.59	9.89	13.35	9.63
	Grouped Median	3.93	3.31	4.63	5.04
	Std. Deviation	1.75	1.47	2.87	1.80

TM: Time on Task in Minutes

TABLE 7.6: Friedman's Anova results for task time comparison by browser



Task	**Browser**	**Mean Rank[a]**	**N**	**Chi-Square**	**df**	**Asymp. Sig.**
Task 1	**SV1**	**1.75**	36	12.056	2	0.002
	SV2	1.78				
	FF	2.47				
Task 2	**SV2**	1.67	36	16.889	2	0.000
	SV1	1.78				
	FF	2.56				
Task 3	**SV1**	**1.42**	36	37.389	2	0.000
	SV2	1.78				
	FF	2.81				
Task 4	**SV1**	**1.75**	36	5.722	2	0.057
	SV2	1.94				
	FF	2.31				

a. Mean rank of task time displayed in ascending order

7.6.2 Satisfaction

The ten SUS statements modified to reflect web browser security controls was used to measure user satisfaction with the three browser UIs (see Figure 7.14). The SUS questionnaire items which were administered as part of the surveys included in the study, consisted of 10 alternating positive and negative statements to avoid response biases [172]. Statements numbered 1, 3, 5, 7 and 9 are positive hence were scored by subtracting 1 from the Likert scale position. Scoring for the negative statements (numbered 2, 4, 6, 8 and 10) on the other hand were done by subtracting the scale position from 5. A multiplication of the sum of all the individual scores by 2.5 would then yield the final SUS score in the range 0–100, for the application being assessed [158]. This section presents the comparative analysis of the SUS scores by browser as a measure of participants satisfaction with the design concepts of the three browsers.

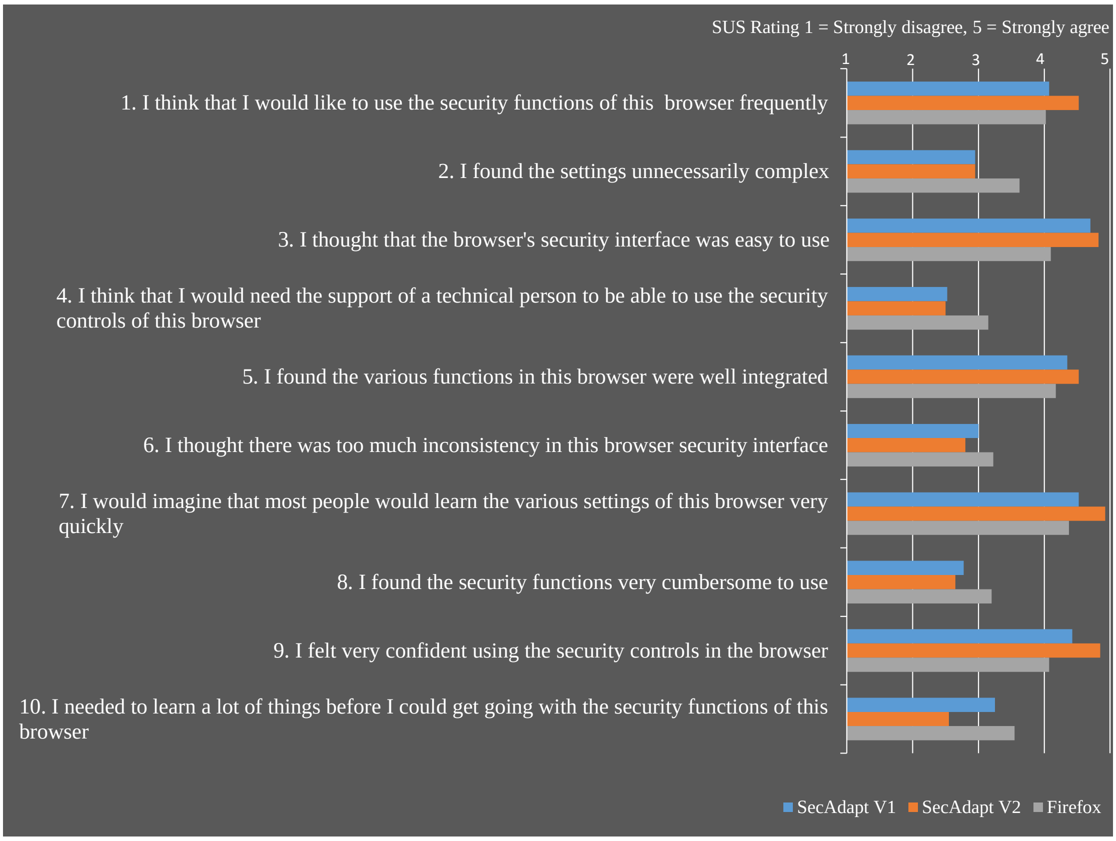


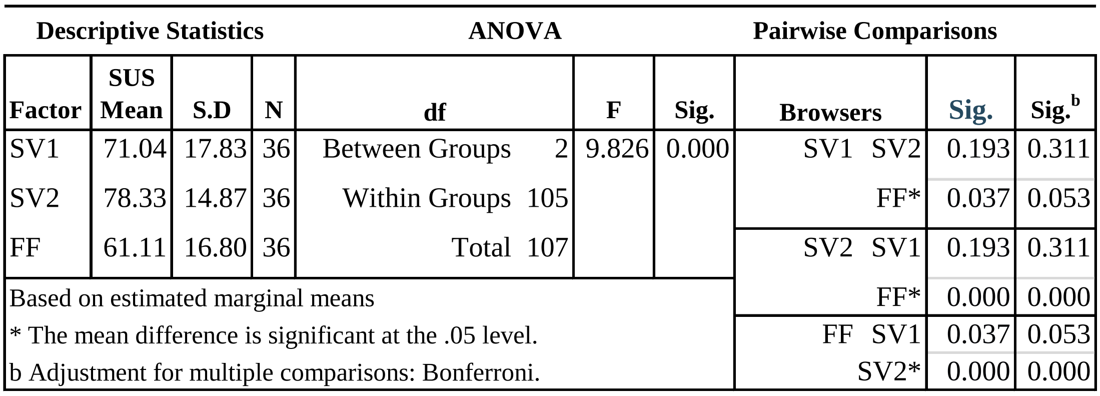
FIGURE 7.14: The 10 SUS statements used to measure and compare satisfaction ratings by browser

SUS by Browser

SV2 had the highest computed SUS score (78.33), followed by SV1 (71.04) which was slightly higher than that of FF (61.11). According to the SUS adjective ratings developed by Bangor et al. [172], the scores for SV1 and SV2 falls in the third quartile (70.5–77.8) and above the mean score of 69.5 (see Figure 4.16 in Chapter 4). Both prototypes therefore qualify for an adjective rating of "Excellent" and are considered "acceptable" in Bangor's acceptability range. FF's SUS score of 61.11 falls in the second quartile and below the mean of 69.5 hence can be rated as "Good" but ranked at "low marginal" according to Bangor's acceptability ranges.

A one-way ANOVA was performed to compare the SUS scores of the three browsers in order to determine whether the differences were statistically significant. The results are summarised in Table 7.7. There was a main effect of user interface type on the combined satisfaction ratings ($F = 9.826, p < 0.01$) explained by SV2 interface being generally rated higher than the others. Although the one-way ANOVA showed a statistically significant difference for the three browser's mean SUS scores ($p < 0.01$), the post-hoc tests (pairwise comparisons) revealed only the difference between SV2 and FF was highly significant ($p < 0.01$) after adjusting the significance values for multiple test using Bonferroni correction. The difference between SV1 and FF are however significant at an alpha level of 1 ($p = 0.053$). There was no significant difference between SV1 and SV2.

TABLE 7.7: One-way ANOVA of SUS scores by browsers



Descriptive Statistics				ANOVA				Pairwise Comparisons			
Factor	**SUS Mean**	**S.D**	**N**	**df**		**F**	**Sig.**	**Browsers**		**Sig.**	**Sig.**^{b}
SV1	71.04	17.83	36	Between Groups	2	9.826	0.000	SV1	SV2	0.193	0.311
SV2	78.33	14.87	36	Within Groups	105				FF*	0.037	0.053
FF	61.11	16.80	36	Total	107			SV2	SV1	0.193	0.311
									FF*	0.000	0.000
								FF	SV1	0.037	0.053
									SV2*	0.000	0.000

Based on estimated marginal means

* The mean difference is significant at the .05 level.

b Adjustment for multiple comparisons: Bonferroni.

7.6.3 Subjective Reactions and Feedback

The two prototypes elicited varying reactions from participants during the think-aloud sessions and the post-study interviews. NVivo 12 Pro [175] was used to integrate and thematically analyse all the qualitative data gathered from the process excluding those involving Firefox. The transcripts were coded with a specific focus on the study aims, i.e. elicit users' reactions and feedback on the design concepts and features. The transcripts were analysed using the same process described in Chapter 4, subsection 4.4.4. The themes that emerged from the qualitative data are summarised in Table 7.8 along with illustrative quotes for each sub-theme. A theme was considered important if it was supported by at least five participants.

7.6.3.1 Usability of the design concepts

A major sub-theme captured under usability is related to the UI control of choice for effecting changes to the settings in the prototype. Sliders were among the control elements used in the prototype to allow users set a value or range for specific sets of options involving privacy and/or security. When completing tasks to set permission levels using the slider provided on the interface for privacy settings and for adaptive security automation levels in SV2, participants were generally positive. 34/36 participants expressed their satisfaction with the slider as a control element for data permission typically commenting that: *"I think the slider for privacy levels is a good idea because*

TABLE 7.8: Summary of themes, sub-themes and example quotes

Themes	Sub-themes	Example Quotes
Usability of the design concepts	Effectiveness of features and control elements	"*I think the slider for privacy levels is a good idea because something like this would have been helpful in Firefox so I would definitely recommend this feature"*
	Content and Learnability	"*So this is quite an interesting interface straight away. It's quite clear and easy to understand"* *"This interface looks very clean and you're not burden with far too much text, it tells you exactly what it is. It's quite easy to follow"*
	Enjoyment of the aesthetics	"*Can I say it is not very refined and it looks like a piece of software in its very early stages."* *"I like how the interface itself is very visual. I like the big buttons, quite easy to turn on or off" I like these icons, they tell you what they are straight away"*
Effect of the user dashboard on cybersecurity acceptability	Awareness	*"This is interesting, I can now clearly distinguish between security and privacy issues when I look at this dashboard, I used to be confused about these things.*
	Relatability	*"This dashboard would be very useful, it makes it more real for me to easily pin-point my status and I like how I can click on each items for details."*
Impact of adaptive automation on attitude towards cybersecurity	Efficiency	*"Apart from the slight delay because I needed to register first, I can finish the remaining tasks faster just by turning on the adaptive button".*
	Mental Demand	*"...and it is quite overwhelming when I just click register for personalized adaptive cybersecurity then boom, I have to fill out all this forms..."*
	Privacy concerns	*"I don't think my ethnicity is relevant here..." or "Can I choose not to state my income level…"*
	Freedom of control	*"...I can still see all the different options, so it is good and I can choose to just set it myself when it starts misbehaving..."*

something like this would have been helpful in Firefox so I would definitely recommend this feature" They indicated that the descriptions provided through the pop-ups improved their understanding of the various permission levels and would help them to more easily make decisions about privacy options than in current interfaces.

Another feature design element that impacted on the usability of the prototype was the control for data backup and encryption. All participants indicated that they preferred the design concept for data protection in the prototype to those ones found in current browsers. In an example quote, one participant said: *"I still find Task 4 to be difficult but this interface is really helpful, it has made it easier"*.

Most of the participants liked using the toggle switches to set their preferences in the prototype. They typically remarked that: *"I like how I can just click on the buttons to either turn the safe-search mode on or off, very simple and straight forward."* However, 9/36 participants reacted negatively to the toggle switches for changing the state of some functionalities in the initial prototype design. They typically complained that: *"these on and off buttons are confusing, should I click on it to turn it on or it is already on, not sure."* . These participants wanted check-boxes with clear description of the options they can choose. The confusion associated with the toggle button was addressed in the final version of the prototype by indicating the state of the associated function in text.

Another sub-theme categorised under usability were comments and reactions to how contents are presented throughout the prototypes. Specifically, 28/36 participants indicated they were happy for not having to deal with technical terms like JavaScripts and Cookies. One participant explained: *"This is helpful, the description is very clear so I know exactly what am signing up for without now trying to guess or decode the terms"*

The third sub-theme captured reactions and feedback provided by participants on the overall attractiveness of the UI design. Almost all the participants commented that they liked the interface designs and thought it looked less cluttered and appeared user-friendly as captured in this example quote: *"This interface looks very clean and you're not burdened with far too much text, it tells you exactly what it is. It's quite easy to follow"* . A few reacted negatively to the aesthetics with remarks like: *"Can I say it is not very refined and it looks like a piece of software in its very early stages."* and *"I don't like the colours on the slider, maybe if you can tone it down a little bit"*. There were also positive reactions to the visual designs in the prototype with majority of the participants preferring it because it made their interaction much more enjoyable compared to other known security settings UI. This sentiment is captured in this example quote: *"I like how the interface itself is very visual and not boring. I like the big buttons, quite easy to turn on or off" I like these icons, they tell you what they are straight away"*. However, about a third reacted negatively to the visual designs in the prototype saying they would much prefer a clear layout of content with text rather than icons and buttons. In an example quote, a participant said: *"I think elderly people and kids would like this design but not me, I am used to just having text I can read on the interface."*

7.6.3.2 Effect of the user dashboard on cybersecurity acceptability

All participants reacted positively to the user dashboard design concept especially for the adaptive one in SV2 (see Figure 7.5 and 7.6). Typical comments indicated that the dashboard improved their awareness of cybersecurity controls and made the issues more relatable. For example, one participant explained that: *"This is interesting, I can now clearly distinguish between security and privacy issues when I look at this dashboard, I used to be confused about these things."* Another typical sentiment of relatability is captured in this comment: *"This dashboard would be very useful, it makes it more real for me to easily pin-point my status and I like how I can click on each item for details"*. In SV2, participants liked how emojis were used to communicate their privacy status with remarks like: *"I like the smiley, I can easily relate to it, I didn't feel the other icons like the emoji"*. Although all participants liked the idea of scoring their cybersecurity status on the dashboard, there were mixed feelings about the presentation style. About half of the participants said they would prefer adjective terms like low, medium or high while the other half liked the percentage scores provided typically saying: *"I am a numbered person so I prefer numbers and it is more exact"*. Overall, participants were generally very pleased with the user dashboard design concept and it impacted positively on their acceptability of web browser security controls as remarked by a participant: *"...this makes me feel like doing something to improve my cybersecurity status and I am more likely to check this more often rather than the other settings interfaces"*.

7.6.3.3 Impact of adaptive automation on attitude towards cybersecurity

Subjective responses to the adaptive interface design concept in SV2 was generally more positive than in the non-adaptive baseline version in SV1. Participants felt that the adaptation in SV2 helped them be more efficient than in SV1. One participant explained: *"Apart from the slight delay because I needed to register first, I can finish the remaining tasks faster just by turning on the adaptive button"*. In terms of mental demand, participants generally felt that it was less demanding performing the study task in SV2 than in SV1 remarking that: *"With this one I don't need to think or worry much, the ACP would adapt everything to my preference anyway"*. However, some participants asking questions like: *"Do I need to fill all this information at once?*, expressed dissatisfaction for the registration concept for adaptation. They felt it was too much information to spend time providing at a go and suggested this be split and collected gradually in subsequent versions of the application. *"...and it is quite overwhelming when I just click register for personalized adaptive cybersecurity then boom, I have to fill out all these forms..."*. Others expressed privacy concerns about some of the information that were required typically complaining that: *"I don't think my ethnicity is relevant here"*. Lastly, several participants liked the fact that all the controls in SV1 were available in SV2 too, letting them decide whether or not to take advantage of the adaptation hence giving them enough freedom and control. *"...I can still see all the different options, so it is good and I can choose to just set it myself when it starts misbehaving..."*

7.7 Discussion

The findings presented in this chapter shows that, improving usability remains a goal for enabling users who wish to adopt and use cybersecurity tools. The process of managing security and privacy settings in web browsers has proven to be a major challenge for home computer users. The problem is that, software developers rarely apply user-centered approach to the design and evaluation of security and privacy interfaces. Results from this study support the fact that a user-centered approach to the design of security interfaces can impact positively on their usability as well as acceptability.

The findings suggest three primary directions to improve the usability and acceptability of desktop web browser security interfaces: adaptive automation of cybersecurity functions, centralizing cybersecurity performance indicators, personalizing security interfaces.

Automation has been employed in several fields to improve task performance and decision-making. For example in healthcare, Manzey et al. [335] found that automated navigation support for surgeons minimized their physical effort requirement and increased patient safety during surgeries. Other areas where automation has been known to improve human interaction with systems include aviation [336], education [337] manufacturing [338, 339] etc. Application of automation for computer security has mainly focused on software testing, intrusion detection and analysis (e.g [340, 341]). The benefits offered by either full or partial automation need to be further leveraged towards improving other aspects of information security management beyond testing and analysis [342]. The usable security field has long recognised the important role automation can play in minimizing security failures commonly attributed to human factors. Previous studies have highlighted the need to balance user interaction with automation as most security decision making cannot be fully automated [87, 343]. This chapter illustrates how security designers can keep the human user in the loop with an adaptive automation framework proposed for personalized cybersecurity.

Another notable recommendation for improving cybersecurity usability and acceptability emerging from the user study conducted is to centralize the browser security and privacy status indicators users require to make critical decisions pertaining to their safety and privacy online. In any decision making, humans generally struggle with processing and understanding large volumes of data [344]. More and more security and privacy features are being integrated into web browsers due to their inherent vulnerabilities. It is imperative that the profusion of these features are managed to minimize complexity of the user interfaces. Progressive and staged disclosure are strategies used to manage options to minimize complexity in user interfaces [345]. In this instance, a dashboard with visualization is used to implement this technique in the design and development of the prototypes which were well received by participants. With the dashboard, users were able to view actionable and useful information related to their security and privacy at a glance. Previous research have also shown that visualization on dashboards greatly improve user performance with different kinds of software applications including cyber analytical tools [346, 347].

Finally, personalization is recommended for improving the usability of cybersecurity controls. The findings from the user study generally show that, although usability was maximised with the prototypes, there was still room for improvement. The findings clearly revealed that differences in user preferences could not be addressed in a single UI design concept hence the need for personalization. Already, the attitude to personal data (APD) scale developed in Chapter 5 has shown how differences in attitude towards personal data influence their interaction with cybersecurity controls [279]. The framework described in Chapter 6 also highlights several factors that could be considered for personalizing interfaces for cybersecurity controls. The various interfaces for manipulating security and privacy settings in the browser could be automatically personalized by profiling users based on these factors.

A key limitation of the prototype evaluation is that it was a short-term laboratory study hence the correct use of the prototype over an extended period of time could not be determined. Also, because of the medium-fidelity nature of the prototypes, their evaluation is primarily based on participants' opinions rather than their actual behaviours hence the results may not generalize to real-world settings. In the future, the prototype could be implemented and used in a long-term field study to address this limitation and determine if the findings carry over into the real world where users would use SecAdapt for adaptive cybersecurity.

7.8 Summary

In this chapter, the last study of this thesis was presented attempting to understand how cybersecurity controls could be designed for home computer users with an adaptive automation framework proposed and described in earlier chapters. The main object for the prototypes was to elicit user reactions to the different design concepts they illustrate as described in this chapter. As such, there was less focus on the implementation details such as how the information could be acquired and synthesized automatically to provide adaptive automation. Usability of cybersecurity tools has been a long unsolved problem. SecAdapt is a browser design concept proposed to improve cybersecurity usability through user-centred UI design and adaptive automation. SecAdapt addresses the problem of usability in web browser security controls by providing functionality transparent interfaces to minimize mental load of users when learning to use the system. Second, the prototype features adaptive controls that users can rely on for efficiency. An empirical investigation is carried out in a laboratory setting to verify the usability and acceptability of the proposed design concept. Overall, the evaluation confirmed that the participants in this study accepted and preferred to use improved design for cybersecurity controls in web browsers with adaptive automation than non-adaptive versions. This chapter also explored the limitations of using a medium-fidelity prototype as proof of concept for the design science research and future studies were proposed where the prototype should be implemented and used in a field study. The next chapter presents the overall conclusions of this thesis.

CHAPTER 8

Conclusion

8.1 Thesis Summary

The general research topic addressed by this thesis was whether the amalgamation of users' web browsing logs and behavioural data can be leveraged for personalized adaptive cybersecurity towards improving their usability and acceptability. This research thus focused on studying and understanding people's security behaviours and actions within cyberspace and how that knowledge can be leveraged towards improving the usability of cybersecurity mechanisms.The research tapped into techniques from multiple disciplines towards the achievement of this goal, by unlocking knowledge from web and behaviour data for the purposes of improving the adaptation of cybersecurity tools to users. The abundance of digital information streams and advances in predictive analytics and machine learning provide an opportunity to explore digital traces and behaviour to enrich the context parameters required for enhancing models for adaptation and/or personalisation. Consequently, this research moved forward current work on user models through further examination of contextual parameters required to adequately deduce user characteristics related to cybersecurity.

The core enquiry for this thesis was: *How can cybersecurity mechanisms be designed to increase the rate at which they are adopted and properly used by non-expert users?* The investigation of this question involved a mixed methods approach incorporating both quantitative and qualitative data analytics to identify existing problems and propose alternative solutions and/or recommendations. The scope of the core enquiry comprised four specific research objectives. The first research objective (OBJ1) was to identify and obtain user experiential data on existing cybersecurity tools and related usability problems. The second objective (OBJ2) was to identify and establish key user characteristics and security-related behaviour profiles. The third research goal (OBJ3) was to develop a machine-learning framework for personalised adaptive cybersecurity (PAC). The fourth research objective (OBJ5) was to develop and evaluate the usability and acceptability of prototype web browser security controls based on design concepts derived from the research findings. The first two objectives (OBJ1 and OBJ2) are both related to RQ1 and RQ2 while OBJ3 and OBJ4 are related to RQ3. To achieve the research objectives, the research methodology was applied over three phases consequently addressing the three sub-questions making up the main research query.

In phase one, exploratory and empirical studies were conducted to answer research questions one and two (RQ1 and RQ2). To identify the factors impacting on the adoption and use of cybersecurity tools, an extensive literature analysis was first performed in Chapters 2 and 3. During the review of the extant literature, two main attributes – usability and acceptability were identified as key factors impacting on the adoption and use of cybersecurity mechanisms. The dimensions of usability and acceptability identified partly answered RQ1 and RQ2. To fully address RQ1, the empirical user study reported in Chapter 4 is conducted to identify the specific usability issues encountered by users while interacting with cybersecurity controls in modern web browsers. Overall, the findings in phase one highlighted the need for more research efforts towards improving the usability and acceptability of cybersecurity tools to better protect the cyber ecosystem.

Phase two focused on the verification and validation of the cybersecurity acceptability dimensions identified in phase one towards addressing RQ2 and RQ3. To fully address RQ2, quantitative survey instruments were developed and administered on the web to collect and analyse data on the constructs and dimensions describing individual's security-related behaviours identified in phase one. Thus, findings from the user survey studies presented in Chapters 5 and 6 provided empirical evidence for the security-related behaviours identified and incorporated into the predictive modelling for personalized adaptive cybersecurity. Consequently, RQ3 was answered by applying Statistical modelling and Machine learning deductions (Bayesian-Networks) to the user survey dataset.

In phase three, two prototypes were developed and evaluated based on the findings from the studies conducted in Phase 1 and 2 which wholly answered the core enquiry of the thesis. Here, the principles of software engineering and user-centred design were applied to the concept formation, development and evaluation of the prototype web browsers. The objective of the prototype development was to illustrate how the proposed framework in phase 2 can be used to automatically adapt web browser security and privacy settings to meet user security goals with personalized user interaction. Using the interactive prototypes developed, representative users were recruited as study participants to test the usability and acceptability of the proposed design concepts. The SUS scores obtained from the usability study conducted provided a very useful metric for the overall usability maximised by the design concept for the prototypes as compared to existing web browser security controls. Table 8.1 provides an overview of the resources that were utilized in completing this research work.

TABLE 8.1: Summary of contributions, techniques and tools employed to achieve the research objectives

Achievements	**Techniques**	**Programs and Tools**
Measuring and predicting acceptability of cybersecurity controls	Behaviour Science • Quantitative survey instruments • User Modelling Data Science • Predictive Analytics	➢ Qualtrics ➢ IBM SPSS ➢ AMOS ➢ Smart-PLS ➢ Microsoft Excel
Identifying cybersecurity personalisation components for non-expert users	Machine Learning • User profiling • Bayesian-based decision support	➢ Hugin Lite ➢ Weka
Gathering requirement for usable and adaptive cybersecurity	Human Computer Interaction techniques • User experience analysis • User-centred design for security • Usability testing	➢ Microsoft PowerPoint ➢ CogTool ➢ Morae ➢ NVivo
Providing automated assistance in cybersecurity mechanisms for non-expert users	Software-Engineering • Prototype design, development, and evaluation	➢ NetBeans IDE ➢ JavaFX Scene Builder ➢ Visual Basics for Applications

8.2 Research Contributions

The contributions of this thesis are summarised as follows:

This thesis contributes to the measurement of users' cybersecurity behavioural attitudes towards the prediction of their intention to adopt cybersecurity tools. Chapters 2 and 3 present the extensive literature review conducted to identify critical cybersecurity behaviour and acceptance variables relevant for the provision of personalized adaptive cybersecurity. As part of meeting the research objective of obtaining data on security behaviours for predictive analysis, a quantitative Attitude to Personal Data (APD) measurement scale was then developed to be used in capturing attitudes towards personal data across groups, contexts, and datasets. The reliability and validity of the instrument was empirically verified and the results presented in Chapter 5. In summary, the results make two major contributions to information security research and design practices:

1. a novel framework describing the primary dimensions of individuals' attitude towards personal data; and
2. a practical measurement scale that can easily be modified and used to measure concerns and preferences for adaptive security designs.

This thesis further contributes to the growing body of literature on user modelling in the field of information security by:

1. conducting empirical experimentation incorporating APD as a determinant in predictive user models necessary for the design of adaptive cybersecurity;
2. validating the proposed model for adaptive cybersecurity that can be used in determining appropriate User Interfaces (UI) through pre-profiled user groups ('stereotypes');
3. proposing a new method of integrating behaviour science approach with machine learning technique to complement the user modelling process for adaptive cybersecurity.

   Specifically, a Bayesian-based framework is proposed for addressing issues of uncertainty in predicting user behaviour in the domain of cybersecurity as illustrated in Chapter 6.

The thesis also contributes to the Human-Centred Security literature by identifying the requirements for usable and adaptive cybersecurity design targeted at non-expert users. Here, HCI techniques were employed to investigate the usability issues inherent in modern web browser security controls. The study which is presented in Chapter 4, highlights the importance of testing security mechanisms with representative users and with realistic scenarios that provide contexts for security goals to be achieved.

The requirements for user-centric security presented in Chapter 4 was eventually incorporated into the design concepts for alternative cybersecurity UIs for web browsers described in Chapter 7. Specifically, the design concepts successfully addressed 8 usable security metrics as summarised below:

1. Awareness — an indication of the security configurations available in the prototype browser right from the onset provided through the home page design.
2. Intuitiveness — menu items clearly labelled and organized for users to easily determine the steps required to complete a task to achieve specific goals hence minimising mental workload for cybersecurity-related goals.
3. Feedback — informative feedback is offered throughout the design with dialogues to yield closure so users would know when a core task is completed.
4. Error prevention — critical actions like deleting password, ignoring security warnings, etc. are confirmed with the user before execution. Dialogues are used to indicate implications of the choices made visible in the interface so users can avoid making dangerous errors from which they may not be able to recover.

5. Error recovery — undo and redo functions are provided with clearly labelled buttons to help users recognise, diagnose and recover from non-critical errors.
6. Language — clear concise language is used for the contents of the prototype for non-expert users to easily understand and relate to.
7. Appearance/Aesthetics — an uncluttered interface is adopted with modern design elements to intentionally give the interface a non-technical look and feel.
8. Status indicators — a user dashboard design concept is introduced to provide a complete outlook of the critical cybersecurity indicators in the browser. This further enhanced users awareness of the browsers cybersecurity controls and how to manipulate them to meet their security and personal privacy needs.

The last contribution of this thesis, presented in Chapter 7, is exploring the design space for adaptive automation in browser security controls and their potential impact on the usability and acceptability of cybersecurity mechanisms. Consequently, the thesis produces novel and inspiring design implications for personalized adaptive cybersecurity and describes how users can be kept in the loop when automating specific security functionalities.

8.3 Limitations and Future Work

A limitation of this research is that convenience and accidental sampling was adopted for the survey data collection which may limit the external validity of the findings. However, the approach allowed enough dataset to be collected and provided empirical evidence in support of the propositions made. It should also be noted that, the laboratory studies were conducted with participants from one university hence generalization needs to be done with caution. Another limitation of this research is that the medium-fidelity nature of the prototype developed only allowed for short-term laboratory study to be conducted. Consequently, the correct use of the prototype over an extended period of time could not be determined. Also, because of the medium-fidelity nature of the prototypes, their evaluation is primarily based on participants' opinions rather than their actual behaviours hence the results may not generalize to real-world settings.

An exciting next step will be to fully implement the prototypes described in this thesis and deploy them for a field study to gather real-life data that can be used to further evaluate and optimize the performance of the proposed Bayesian-based framework for the adaptive automation and personalization. This would also make it possible to investigate other design dimensions like how accuracy and predictability affect the usability and acceptability of adaptive cybersecurity for non-expert users. A limitation of model-based personalization frameworks is the requirement of explicitly defined abstract interface models. However, since a standard design science process has already been followed to explore multiple low-fidelity concrete interface prototypes in this research, the functional specification can be inferred for the default user interfaces in the implementation. An important future work for the implementation of the prototypes would be to consider other metrics for adaptation other than the models of users' preferences, background knowledge and environment explored in this thesis. Other individual metrics like personality, motor abilities, and cognition can be explored in future research for adaptive cybersecurity.

This thesis focused on the security interfaces for desktop web browsers. Another promising research direction will be to pursue the usability and adaptation of security functionalities in mobile and cloud-based browsers. In recent times, cloud-based browsers have been proposed to alleviate the problems of web browser security vulnerabilities and minimise their use as the main vector of cyber attacks. It is important to study and understand the human component of the security infrastructure being provided in this new and emerging cloud environment. Web and data science techniques can be combined to study users' interactions with these security interfaces and ensure individuals from diverse backgrounds and capabilities can effectively adopt and use them for secure browsing.

A new trend of web data adoption in academic research is emerging with more and more studies being carried out on contents generated from social media (e.g. [348–352]. The examples listed were all aimed at promoting augmented user modelling techniques in enhancing existing user models with real-world context information that can be mined from a variety of sources which were not being considered previously. Thus web data mining is creating more and more possibilities of building user models that are enriched with a wider range of perspectives which cannot be achieved through just the analysis of user interactions with technology. The term 'big data' has been invented by computer scientist to describe the evolving technology of processing and converting huge digitally collected datasets into useful information and knowledge. Laney [353] differentiated big data from traditional technologies by highlighting the important attributes of velocity (the rate of data generation and transmission) and variety (the kinds of structured and unstructured data) in addition to volume (size of the data) which is commonly associated with big data definitions. More than ever, behavioural data analytic for predictions and decision making is rapidly advancing due to increasing availability of a great variety of structured, semi-structured or non-structured data from web sources (e.g., clickstreams and different kinds of logs).

Behavioural data analytics for security, however, has mostly been aimed at identifying anomalies by correlating long-term historical data and contextualising security events for forensic purposes [354, 355]. Consequently, the types of data collected for behavioural data analytics in the security field are mainly terabytes of network events, system logs, and audit trails of users within enterprises. It is generally very difficult for academic researchers to access these kinds of data streams as most enterprises withhold such data due to concerns about breach of privacy regulations and competitive access to data. The abundance of web data, however, means that researchers can now collect their own data directly from the web. Just like big data, web data presents an opportunity to develop theories and techniques to examine how systems are used but within the context of the web. Thus, the possibility to model users of cybersecurity mechanism based on their actions and behaviours on the web is highly feasible due to the varied amount of data that can be amassed from the web. This thesis has provided a novel way of looking at the problem, and a good starting point for more work in this area.

Bibliography

[1] J. Nielsen, *Usability engineering*. Elsevier, 1994.

[2] A. Dahanayake and B. Thalheim, “Enriching conceptual modelling practices through design science,” in *Enterprise, Business-Process and Information Systems Modeling*. Springer, 2011, pp. 497–510.

[3] V. K. Vaishnavi and W. Kuechler, *Design science research methods and patterns: innovating information and communication technology*. CRC Press, 2015.

[4] J. J. Garrett, *Elements of user experience, the: user-centered design for the web and beyond*. Pearson Education, 2010.

[5] K. M. Feigh, M. C. Dorneich, and C. C. Hayes, “Toward a characterization of adaptive systems: A framework for researchers and system designers,” *Human Factors*, vol. 54, no. 6, pp. 1008–1024, 2012.

[6] A. Grosskurth and M. W. Godfrey, “A reference architecture for web browsers,” in *null*. IEEE, 2005, pp. 661–664.

[7] R. Philip *et al.*, “Enabling distributed security in cyberspace,” *Departament of Homeland Security*, 2011.

[8] A. R. Beresford, “Location privacy in ubiquitous computing,” University of Cambridge, Computer Laboratory, Report, January 2005.

[9] M. Nadeau, “US state of cybercrime survey,” 2017. [Online]. Available: https://www.csoonline.com/article/3211491/security/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html?upd=1536825517075

[10] G. Grachis, “A look back at cybersecurity in 2017,” 2018. [Online]. Available: https://www.csoonline.com/article/3239405/data-breach/a-look-back-at-cybersecurity-in-2017.html

[11] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, “Guidelines for usable cybersecurity: Past and present,” in *Cyberspace Safety and Security (CSS), 2011 Third International Workshop on*. IEEE, 2011, pp. 21–26.

[12] D. Benyon and D. Murray, “Applying user modeling to human-computer interaction design,” *Artificial Intelligence Review*, vol. 7, no. 3-4, pp. 199–225, 1993.

[13] P. Biswas and P. Robinson, "A brief survey on user modelling in hci," in *Proc. of the International Conference on Intelligent Human Computer Interaction (IHCI) 2010*, 2010.

[14] D. Bollier, C. M. Firestone *et al.*, *The promise and peril of big data*. Aspen Institute, Communications and Society Program Washington, DC, 2010.

[15] D. Fisher, R. DeLine, M. Czerwinski, and S. Drucker, "Interactions with big data analytics," *interactions*, vol. 19, no. 3, pp. 50–59, 2012.

[16] W. O. Galitz, *The essential guide to user interface design: an introduction to GUI design principles and techniques*. John Wiley & Sons, 2007.

[17] D. Balfanz, G. Durfee, R. E. Grinter, and D. Smetters, "In search of usable security: Five lessons from the field," *IEEE Security and Privacy*, vol. 2, no. 5, pp. 19–24, 2004.

[18] Computing Research Association *et al.*, "Four grand challenges in trustworthy computing," in *Second in a Series of Conferences on Gran d Research Challenges in Computer Science and Engineering*, 2003.

[19] Sage Publishing. (2018) Human factors: The journal of the human factors and ergonomics society. [Online]. Available: https://us.sagepub.com/en-us/nam/human-factors/journal201912#description

[20] M. A. Rodriguez, J. Bell, M. Brown, and D. Carter, "Integrating behavioral science with human factors to address process safety," *Journal of Organizational Behavior Management*, vol. 37, no. 3–4, pp. 301–315, 2017. [Online]. Available: https://doi.org/10.1080/01608061.2017.1340924

[21] Internet Live Stats, "Number of internet users," 2018. [Online]. Available: http://www.internetlivestats.com/internet-users/#trend

[22] N. MCDONALD, "Digital in 2018: World's internet users pass the 4 billion mark," 2018. [Online]. Available: https://wearesocial.com/us/blog/2018/01/global-digital-report-2018

[23] M. Aliyu, M. Mahmud, A. O. M. Tap, and R. M. Nassr, "Evaluating design features of islamic websites: a muslim user perception," in *5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*. IEEE, 2013, pp. 1–5.

[24] B. Suh and I. Han, "The impact of customer trust and perception of security control on the acceptance of electronic commerce," *International Journal of electronic commerce*, vol. 7, no. 3, pp. 135–161, 2003.

[25] C. Flavián and M. Guinalíu, "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site," *Industrial Management & Data Systems*, vol. 106, no. 5, pp. 601–620, 2006.

[26] Russ Harvey Consulting, "Web security: Vulnerabilities in internet software," 2018. [Online]. Available: https://www.russharvey.bc.ca/resources/websecurity.html

[27] NSS Labs, "Web browser group test: Which web browser offers best malware protection?" 2014. [Online]. Available: https://www.nsslabs.com/company/news/press-releases

[28] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, N. Modadugu *et al.*, "The ghost in the browser: Analysis of web-based malware." *HotBots*, vol. 7, pp. 4–4, 2007.

[29] A. Hackworth, "Spyware," Carnegie Mellon University, Tech. Rep., 2005. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50317

[30] AOL/NCSA. (2005) AOL/NCSA online safety study. America Online and the National Cyber Security Alliance. [Online]. Available: http://www.uoltj.ca/artwork/2005-2006.2.2.uoltj.Cover.pdf

[31] P. Gühring, "Concepts against man-in-the-browser attacks," 2006.

[32] H. Shahriar, K. Weldemariam, M. Zulkernine, and T. Lutellier, "Effective detection of vulnerable and malicious browser extensions," *Computers & Security*, vol. 47, pp. 66–84, 2014.

[33] Y.-M. Wang, R. Roussev, C. Verbowski, A. Johnson, M.-W. Wu, Y. Huang, and S.-Y. Kuo, "Gatekeeper: Monitoring auto-start extensibility points (aseps) for spyware management." in *LISA*, vol. 4, 2004, pp. 33–46.

[34] E. Kirda, C. Kruegel, G. Banks, G. Vigna, and R. Kemmerer, "Behavior-based spyware detection." in *Usenix Security Symposium*, 2006, p. 694.

[35] E. Abgrall, Y. Le Traon, S. Gombault, and M. Monperrus, "Empirical investigation of the web browser attack surface under cross-site scripting: an urgent need for systematic security regression testing," in *Software Testing, Verification and Validation Workshops (ICSTW), 2014 IEEE Seventh International Conference on*. IEEE, 2014, pp. 34–41.

[36] I. Hydara, A. B. M. Sultan, H. Zulzalil, and N. Admodisastro, "Current state of research on cross-site scripting (XSS) – a systematic literature review," *Information and Software Technology*, vol. 58, pp. 170–186, 2015.

[37] M. Kumar, "Google developer discovers a critical bug in modern web browsers," 2018. [Online]. Available: https://thehackernews.com/2018/06/browser-cross-origin-vulnerability.html

[38] B. PwC UK. (2017) Operation cloud hopper. [Online]. Available: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

[39] Internet Live Stats, "Internet usage & social media statistics," 2018. [Online]. Available: http://www.internetlivestats.com/internet-users/#trend

[40] E. Amoroso, *Cyber Security*. Silicon Press, 2006.

[41] R. A. Kemmerer, "Cybersecurity," in *Software Engineering, 2003. Proceedings. 25th International Conference on*. IEEE, 2003, pp. 705–715.

[42] C. Canongia and R. Mandarino Jr, "Cybersecurity: The new challenge of the information society," *Crisis Management: Concepts, Methodologies, Tools, and Applications*, p. 60, 2013.

[43] M. D. Cavelty, "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities," *Science and engineering ethics*, vol. 20, no. 3, pp. 701–715, 2014.

[44] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014.

[45] R. S. Ross and L. A. Johnson, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*. National Institute of Standards and Technology, 2010. [Online]. Available: https://www.nist.gov/node/561981

[46] R. Kainda, I. Flechais, and A. Roscoe, "Security and usability: Analysis and evaluation," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, 2010, pp. 275–282.

[47] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *European Symposium on Research in Computer Security*. Springer, 2007, pp. 359–374.

[48] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 581–590.

[49] S. L. Garfinkel and R. C. Miller, "Johnny 2: a user test of key continuity management with S/MIME and Outlook Express," in *Proceedings of the 2005 symposium on Usable privacy and security*. ACM, 2005, pp. 13–24.

[50] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, ser. SSYM'99. Berkeley, CA, USA: USENIX Association, 1999, pp. 14–14. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251421.1251435

[51] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: effects of tolerance and image choice," in *Proceedings of the 2005 symposium on Usable privacy and security*. ACM, 2005, pp. 1–12.

[52] B. Al Fayyadh, M. AlZomai, and A. Josang, "Firewalls usability: An experiment investigating the usability of personal firewalls," 2013.

[53] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth, "It's too complicated, so i turned it off!: expectations, perceptions, and misconceptions of personal firewalls," in *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*. ACM, 2010, pp. 53–62.

[54] T. Wong, "On the usability of firewall configuration," in *Symposium on usable privacy and security*, 2008.

[55] W. Geng, S. Flinn, and J. M. DeDourek, "Usable firewall configuration," in *PST*, vol. 5. Citeseer, 2005, p. 11.

[56] A. Wool, "A quantitative study of firewall configuration errors," *Computer*, vol. 37, no. 6, pp. 62–67, 2004.

[57] A. Herzog and N. Shahmehri, "Usability and security of personal firewalls," in *IFIP International Information Security Conference*. Springer, 2007, pp. 37–48.

[58] J. Johnston, J. H. Eloff, and L. Labuschagne, "Security and human computer interfaces," *Computers & Security*, vol. 22, no. 8, pp. 675–684, 2003.

[59] F. Raja, K. Hawkey, and K. Beznosov, "Revealing hidden context: improving mental models of personal firewall users," in *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009, p. 1.

[60] B. Alfayyadh, J. Ponting, M. Alzomai, and A. Jøsang, "Vulnerabilities in personal firewalls caused by poor security usability," in *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*. IEEE, 2010, pp. 682–688.

[61] G. Post and A. Kagan, "The use and effectiveness of anti-virus software," *Computers & Security*, vol. 17, no. 7, pp. 589–599, 1998.

[62] J. Cheung, S. Li, A. Totolici, and P. Zheng, "Usability analysis of sophos antivirus," academia.edu, 2001. [Online]. Available: http://courses.ece.ubc.ca/412/term_project/reports/2008/09-

usability_study_of_sophos_antivirus.pdfhttps://www.academia.edu/6748995/Usability_Analysis_of_Sophos_Antivirus

[63] Enex TestLab, "Usability of endpoint security," 2014. [Online]. Available: https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosenexreportendpointusability.pdf?la=en

[64] S. Furnell and N. Clarke, "Power to the people? the evolving recognition of human aspects of security," *computers & security*, vol. 31, no. 8, pp. 983–988, 2012.

[65] M.-u.-R. Khan and M. H. Abbas, "Security and usability of anti-virus software," 2007.

[66] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 601–610.

[67] D. Zissis and D. Lekkas, "Trust coercion in the name of usable public key infrastructure," *Security and Communication Networks*, vol. 7, no. 11, pp. 1734–1745, 2014.

[68] M. Wood, "Want my autograph? the use and abuse of digital signatures by malware," in *Virus Bulletin Conference*, 2010.

[69] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication." in *USENIX Security Symposium*, vol. 9, 2000, pp. 4–4.

[70] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[71] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 657–666.

[72] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5–14.

[73] T. Müller, T. Latzo, and F. C. Freiling, "Self-encrypting disks pose self-decrypting risks," in *Annual Computer Security Applications Conference (ACSAC), Orlando, Florida, USA*, 2011.

[74] J. Hietala, "Hardware versus software: A usability comparison of software-based encryption with seagate secure hardware-based encryption," SANS Institute, A SANS Whitepaper, 2007.

[75] M. Ahmed, R. Pal, M. M. Hossain, M. A. N. Bikas, and M. K. Hasan, "A comparative study on the currently existing intrusion detection systems," in *Computer*

Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of. IEEE, 2009, pp. 151–154.

[76] P. Kabiri and A. A. Ghorbani, "Research on intrusion detection and response: A survey." *IJ Network Security*, vol. 1, no. 2, pp. 84–102, 2005.

[77] SANS Institute, "Host- vs. network-based intrusion detection systems," Global Information Assurance Certification, Tech. Rep., 2005.

[78] T. Patil, G. Bhutkar, and N. Tarapore, "Usability evaluation using specialized heuristics with qualitative indicators for intrusion detection system," in *Advances in Computing and Information Technology*. Springer, 2012, pp. 317–328.

[79] CERT-MU, *Guideline For Securing Your Web Browser*. National Computer Board – Mauritius, 2011. [Online]. Available: http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20For%20Securing%20Your%20Web%20Browser.pdf

[80] Chromium Developers, "Software architecture - the chromium projects," 2009. [Online]. Available: http://www.chromium.org/chromium-os/chromiumos-design-docs/software-architecture

[81] M. Dhanraj and L. Rojo, "Web browser security comparative report," 2017. [Online]. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=54773

[82] A. Mylonas, N. Tsalis, and D. Gritzalis, "Evaluating the manageability of web browsers controls," in *International Workshop on Security and Trust Management*. Springer, 2013, pp. 82–98.

[83] ——, "Hide and seek: On the disparity of browser security settings," in *Poster: 9th Symposium on Usable Privacy and Security, UK.* Citeseer, 2013.

[84] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Computers & Security*, vol. 28, no. 3-4, pp. 130–137, 2009.

[85] J. Clark, P. C. Van Oorschot, and C. Adams, "Usability of anonymous web browsing: an examination of tor interfaces and deployability," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007, pp. 41–51.

[86] T. Whalen and K. M. Inkpen, "Gathering evidence: use of visual security cues in web browsers," in *Proceedings of Graphics Interface 2005*. Canadian Human-Computer Communications Society, 2005, pp. 137–144.

[87] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13)*. USENIX, 2013, pp. 257–272.

[88] R. Von Solms, “Information security management: why standards are important,” *Information Management & Computer Security*, vol. 7, no. 1, pp. 50–58, 1999.

[89] B. Schneier, *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2011.

[90] L. Coventry, P. Briggs, J. Blythe, and M. Tran, “Using behavioural insights to improve the public’s use of cyber security best practices,” University of Northumbria, Department of Psychology, PaCT Lab, Tech. Rep., 2014.

[91] W. H. Dutton, “Fostering a cybersecurity mindset,” *Available at SSRN 2490010*, 2014.

[92] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.

[93] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, “The psychology of security for the home computer user,” in *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012, Conference Proceedings, pp. 209–223.

[94] R. Crossler and F. Bélanger, “An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (usp) instrument,” *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 45, no. 4, pp. 51–71, 2014.

[95] NIST and A. M. Schwartz, “Cybersecurity, innovation, and the internet economy,” National Institute of Standards and Technology, Report, 2011. [Online]. Available: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf

[96] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” *MIS quarterly*, pp. 319–340, 1989.

[97] T. Kunert, *User-centered interaction design patterns for interactive digital television applications*. Springer Science & Business Media, 2009.

[98] A. Dillon, “User acceptance of information technology,” *Encyclopedia of human factors and ergonomics*, 2001.

[99] H. Holden and R. Rada, “Understanding the influence of perceived usability and technology self-efficacy on teachers? technology acceptance,” *Journal of Research on Technology in Education*, vol. 43, no. 4, pp. 343–367, 2011.

[100] S. K. Dubey and A. Rana, “Analytical roadmap to usability definitions and decompositions,” *International Journal of Engineering Science and Technology*, vol. 2, no. 9, pp. 4723–4729, 2010.

[101] R. Agarwal and V. Venkatesh, "Assessing a firm's web presence: a heuristic evaluation procedure for the measurement of usability," *Information Systems Research*, vol. 13, no. 2, pp. 168–186, 2002.

[102] C. Wilson, *User experience re-mastered: your guide to getting the right design*. Morgan Kaufmann, 2009.

[103] B. Shneiderman, *Designing the user interface: strategies for effective human-computer interaction*. Pearson Education India, 2010.

[104] ——, "Universal usability," *Communications of the ACM*, vol. 43, no. 5, pp. 84–91, 2000.

[105] J. Nielsen, "10 usability heuristics for user interface design," *Fremont: Nielsen Norman Group.[Consult. 20 maio 2014]. Disponível na Internet*, 1995.

[106] M. E. Zurko and R. T. Simon, "User-centered security," in *Proceedings of the 1996 Workshop on New Security Paradigms*, ser. NSPW '96. New York, NY, USA: ACM, 1996, pp. 27–33. [Online]. Available: http://doi.acm.org/10.1145/304851.304859

[107] V. Cambazoglu and N. Thota, "Computer science students' perception of computer network security," in *Learning and Teaching in Computing and Engineering (LaTiCE)*. IEEE, 2013, pp. 204–207.

[108] H.-J. Hof, "User-centric IT security-how to design usable security mechanisms," *arXiv preprint arXiv:1506.07167*, 2015.

[109] L. Church, "End user security: The democratisation of security usability," *Security and Human Behaviour*, 2008.

[110] M. Scott, S. Gudea, W. Golden, and T. Acton, "Usability and acceptance in small-screen information systems," *information technology*, vol. 18, no. 4, pp. 277–297, 2004.

[111] V. Bordo, "Overview of User Acceptance Testing (UAT) for Business Analysts (BAs)," 2010.

[112] H.-P. Lu, C.-L. Hsu, and H.-Y. Hsu, "An empirical study of the effect of perceived risk upon intention to use online applications," *Information Management & Computer Security*, vol. 13, no. 2, pp. 106–120, 2005.

[113] B.-Y. Ng and M. Rahim, "A socio-behavioral study of home computer users' intention to practice security," *PACIS 2005 Proceedings*, p. 20, 2005.

[114] W. Conklin, *Computer security behaviors of home pc users: a diffusion of innovation approach*. The University of Texas at San Antonio, 2006.

[115] R. LaRose, N. Rifon, S. Liu, and D. Lee, "Understanding online safety behavior: A multivariate model," in *The 55th annual conference of the international communication association, New York city*, 2005.

[116] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an understanding of the online consumer's risky behavior and protection practices," *Journal of Consumer Affairs*, vol. 43, no. 3, pp. 449–473, 2009.

[117] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management science*, vol. 46, no. 2, pp. 186–204, 2000.

[118] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS quarterly*, pp. 425–478, 2003.

[119] J. Lu, C.-S. Yu, C. Liu, and J. E. Yao, "Technology acceptance model for wireless internet," *Internet Research*, vol. 13, no. 3, pp. 206–222, 2003.

[120] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of experimental social psychology*, vol. 19, no. 5, pp. 469–479, 1983.

[121] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your attention please: Designing security-decision uis to make genuine risks harder to ignore," *In Proceedings of the Ninth Symposium on Usable Privacy and Security*, p. 6, 2013.

[122] C. Brodie, C. M. Karat, J. Karat, and J. Feng, "Usable security and privacy: a case study of developing privacy management tools," *In Proceedings of the 2005 symposium on Usable privacy and security*, pp. 35–43, 2005.

[123] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Computers & security*, vol. 31, no. 4, pp. 597–611, 2012.

[124] H. J. Asghar, "Design and analysis of human identification protocols," Ph.D. dissertation, Macquarie University, 2012.

[125] J. Stanton, P. Mastrangelo, K. Stam, and J. Jolton, "Behavioral information security: two end user survey studies of motivation and security practices," *AMCIS 2004 Proceedings*, p. 175, 2004.

[126] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, 2005.

[127] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & Security*, vol. 23, no. 3, pp. 191–198, 2004.

[128] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the ?weakest link??a human/computer interaction approach to usable and effective security," *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001.

[129] M. A. Sasse and I. Flechais, "Usable security: Why do we need it? how do we get it?" *Security and Usability*, pp. 13–30, 2005.

[130] J. Y. Thong, W. Hong, and K. Y. Tam, "What leads to user acceptance of digital libraries?" *Communications of the ACM*, vol. 47, no. 11, pp. 78–83, 2004.

[131] P. Y. Chau, "Influence of computer attitude and self-efficacy on it usage behavior," *Journal of organizational and end user computing*, vol. 13, no. 1, p. 26, 2001.

[132] H. Amin, "Internet banking adoption among young intellectuals," *Journal of Internet Banking and Commerce*, vol. 12, no. 3, pp. 1–13, 2007.

[133] B. Hasan, "Delineating the effects of general and system-specific computer self-efficacy beliefs on IS acceptance," *Information & Management*, vol. 43, no. 5, pp. 565–571, 2006.

[134] W. Hong, J. Y. Thong, and K.-Y. T. Wai-Man Wong, "Determinants of user acceptance of digital libraries: an empirical examination of individual differences and system characteristics," *Journal of Management Information Systems*, vol. 18, no. 3, pp. 97–124, 2002.

[135] T. Ramayah, "Doing e-research with e-library: Determinants of perceived ease of use of e-library," *International Journal of Technology, Knowledge and Society*, vol. 1, no. 4, pp. 71–82, 2006.

[136] J. Y. Thong, W. Hong, and K.-Y. Tam, "Understanding user acceptance of digital libraries: what are the roles of interface characteristics, organizational context, and individual differences?" *International journal of human-computer studies*, vol. 57, no. 3, pp. 215–242, 2002.

[137] N. M. Aykin and T. Aykin, "Individual differences in human-computer interaction," *Computers & industrial engineering*, vol. 20, no. 3, pp. 373–379, 1991.

[138] A. Dillon and C. Watson, "User analysis in hci?the historical lessons from individual differences research," *International Journal of Human-Computer Studies*, vol. 45, no. 6, pp. 619–637, 1996.

[139] C. Chen, M. Czerwinski, and R. Macredie, "Individual differences in virtual environments?introduction and overview," *Journal of the American Society for Information Science*, vol. 51, no. 6, pp. 499–507, 2000.

[140] D. E. Egan, "Individual differences in human-computer interaction," *Handbook of human-computer interaction*, pp. 543–568, 1988.

[141] G. Pare and J. J. Elam, "Discretionary use of personal computers by knowledge workers: testing of a social psychology theoretical model," *Behaviour & Information Technology*, vol. 14, no. 4, pp. 215–228, 1995.

[142] D. Banisar, S. Davies *et al.*, "Privacy and human rights: an international survey of privacy laws and practice," *Global Internet Liberty Campaign*, 1999.

[143] R. Clarke, "Introduction to dataveillance and information privacy, and definitions of terms," *Roger Clarke's Dataveillance and Information Privacy Pages*, 1999.

[144] J. Carlos Roca, J. José García, and J. José de la Vega, "The importance of perceived trust, security and privacy in online trading systems," *Information Management & Computer Security*, vol. 17, no. 2, pp. 96–113, 2009.

[145] L. V. Casalo, C. Flavián, and M. Guinalíu, "The role of security, privacy, usability and reputation in the development of online banking," *Online Information Review*, vol. 31, no. 5, pp. 583–603, 2007.

[146] National Research Council, *Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop*. Washington, DC: The National Academies Press, 2010.

[147] S. Pearson, *Privacy, security and trust in cloud computing*. Springer, 2013, book section 1, pp. 9–13.

[148] G. Iachello and J. Hong, "End-user privacy in human-computer interaction," *Foundations and Trends in Human-Computer Interaction*, vol. 1, no. 1, pp. 1–137, 2007.

[149] M. S. Ackerman and L. Cranor, "Privacy critics: Ui components to safeguard users' privacy," in *CHI'99 Extended Abstracts on Human Factors in Computing Systems*. ACM, 1999, pp. 258–259.

[150] A. Collins, D. Joseph, and K. Bielaczyc, "Design research: Theoretical and methodological issues," *The Journal of the learning sciences*, vol. 13, no. 1, pp. 15–42, 2004.

[151] V. Vaishnavi and W. Kuechler, "Design research in information systems," *Association for Information Systems*, 2004.

[152] A. R. Hevner, "A three cycle view of design science research," *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4, 2007.

[153] F. L. Greitzer, "Situated usability testing for security systems," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2011.

[154] C. Birge, "Enhancing research into usable privacy and security," in *Proceedings of the 27th ACM international conference on Design of communication*. ACM, 2009, pp. 221–226.

[155] StatCounter.com, "Desktop browser market share worldwide – 2016," 2016. [Online]. Available: http://gs.statcounter.com/#desktop-browser-CN-monthly-201511-201610-bar

[156] C. Buckler, "Browser trends may 2016: Firefox finally overtakes ie," 2016. [Online]. Available: https://www.sitepoint.com/browser-trends-may-2016-firefox-finally-overtakes-ie/

[157] J. Brooke *et al.*, "SUS – A quick and dirty usability scale," *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996.

[158] J. Brooke, "SUS: a retrospective," *Journal of usability studies*, vol. 8, no. 2, pp. 29–40, 2013.

[159] T. Zhao and S. McDonald, "Keep talking: an analysis of participant utterances gathered using two concurrent think-aloud methods," in *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*. ACM, 2010, pp. 581–590.

[160] ANSI, "Common industry format for usability test reports," 2001.

[161] ISO, "Ergonomic requirements for office work with visual display terminals (vdts): Part 11: Guidance on usability," *International Organization for Standardization ISO*, vol. 9241, 1998.

[162] J. Nielsen, "Severity ratings for usability problems (2007)," *Retrieved March*, vol. 4, 2010.

[163] J. S. Dumas, J. S. Dumas, and J. Redish, *A practical guide to usability testing*. Intellect books, 1999.

[164] J. Rubin and D. Chisnell, *Handbook of usability testing: how to plan, design and conduct effective tests*. John Wiley & Sons, 2008.

[165] R. Molich and J. S. Dumas, "Comparative usability evaluation (cue-4)," *Behaviour & Information Technology*, vol. 27, no. 3, pp. 263–281, 2008.

[166] D. M. Hilbert and D. F. Redmiles, "Extracting usability information from user interface events," *ACM Computing Surveys (CSUR)*, vol. 32, no. 4, pp. 384–421, 2000.

[167] P. Kortum and C. Z. Acemyan, "The relationship between user mouse-based performance and subjective usability assessments," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 60, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 2016, pp. 1174–1178.

[168] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons, "Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client," *arXiv preprint arXiv:1510.08555*, 2015.

[169] J. Sauro, "Measuring usability with the system usability scale (SUS)," 2011.

[170] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, and K. Seamons, "Confused johnny: when automatic encryption leads to confusion and mistakes," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 5.

[171] T. S. Tullis and J. N. Stetson, "A comparison of questionnaires for assessing website usability," in *Usability professional association conference*, vol. 1, 2004.

[172] A. Bangor, P. Kortum, and J. Miller, "Determining what individual SUS scores mean: Adding an adjective rating scale," *Journal of usability studies*, vol. 4, no. 3, pp. 114–123, 2009.

[173] J. Sauro, *A practical guide to the system usability scale: Background, benchmarks & best practices*. Measuring Usability LLC Denver, CO, 2011.

[174] S. McDonald, H. M. Edwards, and T. Zhao, "Exploring think-alouds in usability testing: An international survey," *IEEE Transactions on Professional Communication*, vol. 55, no. 1, pp. 2–19, 2012.

[175] QSR International Pty Ltd, "NVivo qualitative data analysis software," *Version 12 Pro*, 2018.

[176] S. C. Yang, "Reconceptualizing think-aloud methodology: Refining the encoding and categorizing techniques via contextualized perspectives," *Computers in Human Behavior*, vol. 19, no. 1, pp. 95–115, 2003.

[177] W. Quesenbery, "What does usability mean: Looking beyondease of use'," in *Annual conference-society for technical communication*, vol. 48. Citeseer, 2001, pp. 432–436.

[178] S. Ruoti, B. Roberts, and K. Seamons, "Authentication melee: A usability analysis of seven web authentication systems," in *Proceedings of the 24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2015, pp. 916–926.

[179] P. A. Akiki, A. K. Bandara, and Y. Yu, "Adaptive model-driven user interface development systems," *ACM Computing Surveys*, vol. 47, no. 1, 2015.

[180] N. Mezhoudi, J. L. Perez Medina, I. Khaddam *et al.*, "Context-awareness metamodel for user interface runtime adaptation," *International Journal of Software Engineering*, vol. 2, 2015.

[181] S. Stille, S. Minocha, and R. Ernst, "A 2 dl-an adaptive automatic display layout system," in *Human Interaction with Complex Systems, 1996. HICS'96. Proceedings., Third Annual Symposium on*. IEEE, 1996, pp. 243–250.

[182] A. Bunt, C. Conati, and J. McGrenere, "What role can adaptive support play in an adaptable system?" in *Proceedings of the 9th international conference on Intelligent user interfaces*. ACM, 2004, pp. 117–124.

[183] B. Jason, A. Calitz, and J. Greyling, "The evaluation of an adaptive user interface model," in *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*. ACM, 2010, pp. 132–143.

[184] V. Alvarez-Cortes, B. E. Zayas-Perez, V. H. Zarate-Silva, and J. A. R. Uresti, "Current trends in adaptive user interfaces: Challenges and applications," in *Electronics, Robotics and Automotive Mechanics Conference (CERMA 2007)*. IEEE, 2007, pp. 312–317.

[185] M. Chignell and P. Hancock, "Intelligent interface design," *Handbook of human-computer interaction*, pp. 969–995, 1988.

[186] C. Stephanidis, A. Paramythis, M. Sfyrakis, A. Stergiou, N. Maou, A. Leventis, G. Paparoulis, and C. Karagiannidis, "Adaptable and adaptive user interfaces for disabled users in the avanti project," *In Intelligence in Services and Networks: Technology for Ubiquitous Telecom Services*, pp. 153–166, 1998.

[187] M. Bisignano, G. Di Modica, and O. Tomarchio, "Dynamically adaptable user interface generation for heterogeneous computing devices," in *International Conference on High Performance Computing and Communications*. Springer, 2005, pp. 1000–1010.

[188] L. Strachan, J. Anderson, M. Sneesby, and M. Evans, "Minimalist user modelling in a complex commercial software system," *User Modeling and User-Adapted Interaction*, vol. 10, no. 2-3, pp. 109–146, 2000.

[189] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers, "Big data: The next frontier for innovation, competition, and productivity. 2011," McKinsey Global Institute, Report, 2015.

[190] F. Zhu, S. Carpenter, A. Kulkarni, C. Chidambaram, and S. Pathak, "Understanding and minimizing identity exposure in ubiquitous computing environments,"

In Mobile and Ubiquitous Systems: Networking Services, MobiQuitous, 2009. MobiQuitous' 09. 6th Annual International. IEEE, pp. 1–10, 2009.

[191] G. Iachello and J. Hong, "End-user privacy in human-computer interaction," *Foundations and Trends in Human-Computer Interaction*, vol. 1, no. 1, pp. 1–137, 2007.

[192] S. Lederer, J. I. Hong, A. K. Dey, and J. A. Landay, "Personal privacy through understanding and action: five pitfalls for designers," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 440–454, 2004.

[193] A. Joinson, C. Paine, T. Buchanan, and U. Reips, "Measuring internet privacy attitudes and behavior: A multi-dimensional approach," *Journal of Information Science*, vol. 32, no. 4, pp. 334–343, 2006.

[194] M. C. Brown, "Exploring interpretations of data from the internet of things in the home," *Interacting with Computers*, vol. 3, p. 25, 2013.

[195] S. Sharples, M. Brown, J. Harding, and M. Jackson, "Usability, human factors and geographic information (editorial)," *Applied ergonomics*, vol. 44, no. 6, pp. 853–854, 2013.

[196] Information Commissioner's Office, "Key definitions of the data protection act," 2015. [Online]. Available: http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#personal-data

[197] Australian Government, "Privacy amendment (enhancing privacy protection) act 2012," Australian Government, 2014. [Online]. Available: https://www.legislation.gov.au/Details/C2012A00197

[198] C. Millard and W. K. Hon, "Defining ?personal data?in e-social science," *Information, Communication & Society*, vol. 15, no. 1, pp. 66–84, 2012.

[199] 2015.

[200] E. McCallister, *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing, 2010.

[201] T. C. Rindfleisch, "Privacy, information technology, and health care," *Communications of the ACM*, vol. 40, no. 8, pp. 92–100, 1997.

[202] Wellcome Trust, "Summary report of qualitative research into public attitudes to personal data and linking personal data," The Wellcome Trust Limited, Report, 2013. [Online]. Available: http://www.wellcome.ac.uk/About-us/Publications/Reports/Public-engagement/WTP053206.htm

[203] United States: PPSC, *Personal privacy in an information society: the report of the Privacy Protection Study Commission*. The Commission: for sale by the Supt. of Docs., US Govt. Print. Off., 1977, vol. 1.

[204] O. for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD, 2002.

[205] J. B. Earp and F. C. Payton, "Information privacy in the service sector: An exploratory study of health care and banking professionals," *Journal of Organizational Computing and Electronic Commerce*, vol. 16, no. 2, pp. 105–122, 2006.

[206] A. F. Westin, *Privacy and freedom*. New York: Atheneum, 1967, vol. 25.

[207] W. E. Forum, "Unlocking the value of personal data: From collection to usage," WEF, Report, 2013. [Online]. Available: http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage

[208] J. H. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: Measuring individuals concerns about organizational practices," *Management Information Systems Quarterly*, vol. 20, no. 2, pp. 167–196, 1996.

[209] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale and a causal model," *Information Systems Research*, vol. 5, pp. 336–355, 2004.

[210] W. Hong and J. Y. Thong, "Internet privacy concerns: an integrated conceptualization and four empirical studies," *MIS Quarterly*, vol. 37, no. 1, pp. 275–298, 2013.

[211] L. F. Chen and R. Ismail, "Information technology program students' awareness and perceptions towards personal data protection and privacy," in *Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on*. IEEE, 2013, pp. 434–438.

[212] M. Robling, K. Hood, H. Houston, R. Pill, J. Fay, and H. Evans, "Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study," *Journal of Medical Ethics*, vol. 30, no. 1, pp. 104–109, 2004.

[213] P. Singleton, N. Lea, A. Tapuria, and D. Kalra, "Public and professional attitudes to privacy of healthcare data: a survey of the literature," Cambridge Health Informatics Ltd, Report, 2008. [Online]. Available: http://www.gmc-uk.org/GMC_Privacy_Attitudes_Final_Report_with_Addendum.pdf_27007284.pdf

[214] Z. Wang and Q. Yu, "Privacy trust crisis of personal data in china in the era of big data: The survey and countermeasures," *Computer Law Security Review*, vol. 31, no. 6, pp. 782–792, 2015.

[215] H. Sheng, F. F.-H. Nah, and K. Siau, "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns," *Journal of the Association for Information Systems*, vol. 9, no. 6, p. 344, 2008.

[216] W. K. Hon, C. Millard, and I. Walden, "Who is responsible for ?personal data?in cloud computing??the cloud of unknowing, part 2," *International Data Privacy Law*, vol. 2, no. 1, pp. 3–18, 2012.

[217] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006.

[218] F. Belanger, J. S. Hiller, and W. J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The journal of strategic Information Systems*, vol. 11, no. 3, pp. 245–270, 2002.

[219] M. Lang, J. Devitt, S. Kelly, A. Kinneen, J. O'Malley, and D. Prunty, "Social networking and personal data security: a study of attitudes and public awareness in ireland," *In Management of e-Commerce and e-Government, ICMECG'09*, 2009.

[220] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS quarterly*, pp. 13–28, 2006.

[221] K.-L. Hui, H. H. Teo, and S.-Y. T. Lee, "The value of privacy assurance: an exploratory field experiment," *Mis Quarterly*, pp. 19–33, 2007.

[222] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of measures of online privacy concern and protection for use on the internet," *Journal of the American society for information science and technology*, vol. 58, no. 2, pp. 157–165, 2007.

[223] M. Pattinson, K. Parsons, M. Butavicius, A. McCormac, D. Calic, S. Furnell, and S. Furnell, "Assessing information security attitudes: A comparison of two studies," *Information Computer Security*, vol. 24, no. 2, 2016.

[224] OPM, "Review of public and professional attitudes towards confidentiality of healthcare data," General Medical Council, Report, June 2015.

[225] G. Bansal and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, vol. 49, no. 2, pp. 138–150, 2010.

[226] S. Pearson, *Privacy, security and trust in cloud computing*. Springer, 2013.

[227] T. R. Hinkin, "A review of scale development practices in the study of organizations," *Journal of management*, vol. 21, no. 5, pp. 967–988, 1995.

[228] E. C. Papanastasiou, "Factor structure of the attitudes toward research scale," *Statistics Education Research Journal*, vol. 4, no. 1, pp. 16–26, 2005.

[229] A. Field, *Discovering statistics using IBM SPSS statistics*. sage, 2013.

[230] J. Rattray and M. Jones, "Essential elements of questionnaire design and development," *Journal of Clinical Nursing*, vol. 16, pp. 234–243, 2007.

[231] H. Van der Heijden and L. S. Sørensen, *Measuring attitudes towards mobile information services: an empirical validation of the HED/UT scale*. Technical University of Denmark, Center for Tele-Information, 2002.

[232] D. Child, *The essentials of factor analysis*. London: Continuum, 2006.

[233] S. P. Reise, N. G. Waller, and A. L. Comrey, "Factor analysis and scale revision," *Psychological Assessment*, vol. 12, no. 3, p. 287, 2000.

[234] H. B. Lee and A. L. Comrey, "Distortions in a commonly used factor analytic procedure," *Multivariate Behavioral Research*, vol. 14, no. 3, pp. 301–321, 1979.

[235] D. Hooper, J. Coughlan, and M. Mullen, "Structural equation modelling: Guidelines for determining model fit," *Articles*, p. 2, 2008.

[236] P. Bertea and A. Zait, "Methods for testing discriminant validity," *Management Marketing-Craiova*, no. 2, pp. 217–224, 2011.

[237] B. S. Everitt and D. C. Howell, *Encyclopedia of statistics in behavioral science*. John Wiley Sons Ltd, 2005.

[238] E. Mooi and M. Sarstedt, *Cluster analysis*. Springer, 2010.

[239] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[240] M. Sato, "Personal data in the cloud: A global survey of consumer attitudes," *Minato-u, To yo*, pp. 105–7123, 2010.

[241] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *International workshop on privacy enhancing technologies*. Springer, 2006, pp. 36–58.

[242] EU Commission, "Attitudes on data protection and electronic identity in the european union," *Eurobarometer Special Surveys*, vol. 359, 2011.

[243] M. Shelton, L. Rainie, M. Madden, M. Anderson, M. Duggan, A. Perrin, and D. Page, "Americans? privacy strategies post-snowden," *Pew Research Center*, 2015.

[244] L. Rainie and M. Madden, “Americans? privacy strategies post-snowden,” *Pew Research Center*, vol. 16, 2015.

[245] A. Kobsa, *Privacy-enhanced web personalization*. Springer, 2007, pp. 628–670.

[246] A. Acquisti, C. Taylor, and L. Wagman, “The economics of privacy,” *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492, 2016.

[247] 2013.

[248] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, “User acceptance of computer technology: A comparison of two theoretical models,” *Management Science*, vol. 35, no. 8, pp. 982–1003, 1989.

[249] F. D. Davis, “User acceptance of information technology: system characteristics, user perceptions and behavioral impacts,” *International journal of man-machine studies*, vol. 38, no. 3, pp. 475–487, 1993.

[250] F. Calisir, C. Altin Gumussoy, A. E. Bayraktaroglu, and D. Karaali, “Predicting the intention to use a web-based learning system: Perceived content quality, anxiety, perceived system quality, image, and the technology acceptance model,” *Human Factors and Ergonomics in Manufacturing & Service Industries*, vol. 24, no. 5, pp. 515–531, 2014.

[251] W. L. Fuerst and P. H. Cheney, “Concepts, theory, and techniques: Factors affecting the perceived utilization of computer-based decision support systems in the oil industry,” *Decision Sciences*, vol. 13, no. 4, pp. 554–569, 1982.

[252] M. Igbaria, “End-user computing effectiveness: A structural equation model,” *Omega*, vol. 18, no. 6, pp. 637–652, 1990. [Online]. Available: http://www.sciencedirect.com/science/article/pii/030504839090055E

[253] I. Topa and M. Karyda, “Identifying factors that influence employees’ security behavior for enhancing isp compliance,” in *International Conference on Trust and Privacy in Digital Business*. Springer, 2015, pp. 169–179.

[254] J. Omidosu and J. Ophoff, “A theory-based review of information security behavior in the organization and home context,” in *Advances in Computing and Communication Engineering (ICACCE), 2016 International Conference on*. IEEE, 2016, pp. 225–231.

[255] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, “The psychology of security for the home computer user,” in *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012, pp. 209–223.

[256] M. Igbaria, N. Zinatelli, P. Cragg, and A. L. Cavaye, "Personal computing acceptance factors in small firms: a structural equation model," *MIS quarterly*, pp. 279–305, 1997.

[257] I. Woon, G.-W. Tan, and R. Low, "A protection motivation theory approach to home wireless security," *ICIS 2005 proceedings*, p. 31, 2005.

[258] A. Jeyaraj, J. W. Rottman, and M. C. Lacity, "A review of the predictors, linkages, and biases in it innovation adoption research," *Journal of Information Technology*, vol. 21, no. 1, pp. 1–23, 2006.

[259] S. Alharbi and S. Drew, "Using the technology acceptance model in understanding academics' behavioural intention to use learning management systems," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, pp. 143–155, 2014.

[260] G. Ellis, "NAE grand challenges for engineering," *IEEE Engineering Management Review*, vol. 1, no. 37, p. 3, 2009. [Online]. Available: http://www.engineeringchallenges.org/File.aspx?id=11574&v=ba24e2ed

[261] J. Jacoby and L. B. Kaplan, "The components of perceived risk," in *SV-Proceedings of the third annual conference of the association for consumer research*, 1972.

[262] L. B. Kaplan, G. J. Szybillo, and J. Jacoby, "Components of perceived risk in product purchase: A cross-validation." *Journal of applied Psychology*, vol. 59, no. 3, p. 287, 1974.

[263] B. Dai, S. Forsythe, and W.-S. Kwon, "The impact of online shopping experience on risk perceptions and online purchase intentions: does product category matter?" *Journal of Electronic Commerce Research*, vol. 15, no. 1, p. 13, 2014.

[264] S. Forsythe, C. Liu, D. Shannon, and L. C. Gardner, "Development of a scale to measure the perceived benefits and risks of online shopping," *Journal of interactive marketing*, vol. 20, no. 2, pp. 55–75, 2006.

[265] S. M. Forsythe and B. Shi, "Consumer patronage and risk perceptions in internet shopping," *journal of Business research*, vol. 56, no. 11, pp. 867–875, 2003.

[266] F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems*, vol. 17, no. 2, pp. 165–176, 2008.

[267] M. S. Featherman and P. A. Pavlou, "Predicting e-services adoption: a perceived risk facets perspective," *International journal of human-computer studies*, vol. 59, no. 4, pp. 451–474, 2003.

[268] M.-C. Lee, “Factors influencing the adoption of internet banking: An integration of tam and tpb with perceived risk and perceived benefit,” *Electronic commerce research and applications*, vol. 8, no. 3, pp. 130–141, 2009.

[269] S. Özkan, G. Bindusara, and R. Hackney, “Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis,” *Journal of enterprise information management*, vol. 23, no. 3, pp. 305–325, 2010.

[270] A. J.-T. Chang, “Roles of perceived risk and usefulness in information system security adoption,” in *Management of Innovation and Technology (ICMIT), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1264–1269.

[271] A. Izquierdo-Yusta, C. Olarte-Pascual, and E. Reinares-Lara, “Attitudes toward mobile advertising among users versus non-users of the mobile internet,” *Telematics and Informatics*, vol. 32, no. 2, pp. 355–366, 2015.

[272] J. W. Kim, B. H. Lee, M. J. Shaw, H.-L. Chang, and M. Nelson, “Application of decision-tree induction techniques to personalized advertisements on internet storefronts,” *International Journal of Electronic Commerce*, vol. 5, no. 3, pp. 45–62, 2001.

[273] T. Raghu, P. Kannan, H. R. Rao, and A. B. Whinston, “Dynamic profiling of consumers for customized offerings over the internet: A model and analysis,” *Decision Support Systems*, vol. 32, no. 2, pp. 117–134, 2001.

[274] D. J. Xu, “The influence of personalization in affecting consumer attitudes toward mobile advertising in china,” *Journal of Computer Information Systems*, vol. 47, no. 2, pp. 9–19, 2006.

[275] S. Pearson, *Privacy, security and trust in cloud computing*. Springer, 2013, book section 1, pp. 9–13.

[276] J. Addae, M. Radenkovic, X. Sun, and D. Towey, “An augmented cybersecurity behavioral research model,” in *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*. IEEE, 2016, pp. 602–603.

[277] EU, “Attitudes on data protection and electronic identity in the european union,” *Eurobarometer Special Surveys*, vol. 359, 2011.

[278] H. Haddadi, H. Howard, A. Chaudhry, J. Crowcroft, A. Madhavapeddy, and R. Mortier, “Personal data: Thinking inside the box,” *arXiv preprint arXiv:1501.04737*, 2015.

[279] J. H. Addae, M. Brown, X. Sun, D. Towey, and M. Radenkovic, “Measuring attitude towards personal data for adaptive cybersecurity,” *Information & Computer Security*, vol. 25, no. 5, pp. 560–579, 2017.

[280] W. W. Chin, B. L. Marcolin, and P. R. Newsted, "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion/adoption study," *Information systems research*, vol. 14, no. 2, pp. 189–217, 2003.

[281] H. Sun and P. Zhang, "The role of moderating factors in user technology acceptance," *International journal of human-computer studies*, vol. 64, no. 2, pp. 53–78, 2006.

[282] M. Alavi and E. A. Joachimsthaler, "Revisiting dss implementation research: A meta-analysis of the literature and suggestions for researchers," *Mis Quarterly*, pp. 95–116, 1992.

[283] R. P. Bostrom, L. Olfman, and M. K. Sein, "The importance of learning style in end-user training," *MIS Quarterly*, pp. 101–119, 1990.

[284] M. G. Morris and V. Venkatesh, "Age differences in technology adoption decisions: Implications for a changing work force," *Personnel psychology*, vol. 53, no. 2, pp. 375–403, 2000.

[285] P. Kumaraguru, J. Cranshaw, R. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, "A real-word evaluation of anti-phishing training," *Citeseer*, 2009.

[286] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 373–382.

[287] V. Venkatesh and M. G. Morris, "Why don't men ever stop to ask for directions? gender, social influence, and their role in technology acceptance and usage behavior," *MIS quarterly*, pp. 115–139, 2000.

[288] D.-H. Shin, "Towards an understanding of the consumer acceptance of mobile wallet," *Computers in Human Behavior*, vol. 25, no. 6, pp. 1343–1354, 2009.

[289] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, pp. 437–443, 2017.

[290] T. Ramayah, "Doing e-research with e-library: Determinants of perceived ease of use of e-library," *International Journal of Technology, Knowledge and Society*, vol. 1, no. 4, pp. 71–82, 2006.

[291] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, 2009.

[292] R. LaRose, N. J. Rifon, and R. Enbody, “Promoting personal responsibility for internet safety,” *Communications of the ACM*, vol. 51, no. 3, pp. 71–76, 2008.

[293] D. Compeau, C. A. Higgins, and S. Huff, “Social cognitive theory and individual reactions to computing technology: A longitudinal study,” *MIS quarterly*, pp. 145–158, 1999.

[294] J. C.-C. Lin and H. Lu, “Towards an understanding of the behavioural intention to use a web site,” *International journal of information management*, vol. 20, no. 3, pp. 197–208, 2000.

[295] K. A. Pituch and Y.-k. Lee, “The influence of system characteristics on e-learning use,” *Computers & Education*, vol. 47, no. 2, pp. 222–244, 2006.

[296] Y. Lee and K. A. Kozar, “An empirical investigation of anti-spyware software adoption: A multitheoretical perspective,” *Information & Management*, vol. 45, no. 2, pp. 109–119, 2008.

[297] W.-S. Lin, “Perceived fit and satisfaction on web learning performance: Is continuance intention and task-technology fit perspectives,” *International Journal of Human-Computer Studies*, vol. 70, no. 7, pp. 498–507, 2012.

[298] D. J. Xu, S. S. Liao, and Q. Li, “Combining empirical experimentation and modeling techniques: A design research approach for personalized mobile advertising applications,” *Decision support systems*, vol. 44, no. 3, pp. 710–724, 2008.

[299] J. F. Hair, C. M. Ringle, and M. Sarstedt, “Pls-sem: Indeed a silver bullet,” *Journal of Marketing theory and Practice*, vol. 19, no. 2, pp. 139–152, 2011.

[300] C. M. Ringle, S. Wende, and J.-M. Becker, “Smartpls 3,” *Boenningstedt: SmartPLS GmbH, http://www. smartpls. com*, 2015.

[301] J. Henseler, G. Hubona, and P. A. Ray, “Using pls path modeling in new technology research: updated guidelines,” *Industrial management & data systems*, vol. 116, no. 1, pp. 2–20, 2016.

[302] J. F. Hair Jr, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications, 2016.

[303] N. Urbach and F. Ahlemann, “Structural equation modeling in information systems research using partial least squares,” *JITTA: Journal of Information Technology Theory and Application*, vol. 11, no. 2, p. 5, 2010.

[304] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 7th ed. Upper Saddle River, NJ, USA: Prentice-Hall, Inc, 2010.

[305] D. Garson, "Partial least squares: Regression and path modeling," *Asheboro, NC: Statistical Publishing Associates*, 2012.

[306] M. Tenenhaus, V. E. Vinzi, Y.-M. Chatelin, and C. Lauro, "Pls path modeling," *Computational statistics & data analysis*, vol. 48, no. 1, pp. 159–205, 2005.

[307] M. Sarstedt, J. Henseler, and C. M. Ringle, *Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results*. Emerald Group Publishing Limited, 2011, pp. 195–218.

[308] S. Nadkarni and P. P. Shenoy, "A causal mapping approach to constructing bayesian networks," *Decision support systems*, vol. 38, no. 2, pp. 259–281, 2004.

[309] G. Sakellaropoulos and G. Nikiforidis, "Prognostic performance of two expert systems based on bayesian belief networks," *Decision Support Systems*, vol. 27, no. 4, pp. 431–442, 2000.

[310] J.-H. Ahn and K. J. Ezawa, "Decision support for real-time telemarketing operations through bayesian network learning," *Decision Support Systems*, vol. 21, no. 1, pp. 17–27, 1997.

[311] T. D. Nielsen and F. V. Jensen, *Bayesian networks and decision graphs*. Springer Science & Business Media, 2009.

[312] D. Koller, N. Friedman, L. Getoor, and B. Taskar, "Graphical models in a nutshell," *URL http://www. seas. upenn. edu/taskar/pubs/gms-srl07. pdf*, 2007.

[313] D. Heckerman, D. Geiger, and D. M. Chickering, "Learning bayesian networks: The combination of knowledge and statistical data," *Machine learning*, vol. 20, no. 3, pp. 197–243, 1995.

[314] A. Gelman, J. B. Carlin, H. S. Stern, and D. B. Dunson, *Bayesian data analysis*. Chapman and Hall/CRC, 2014, vol. 2.

[315] A. L. Madsen, F. Jensen, U. B. Kjaerulff, and M. Lang, "The hugin tool for probabilistic graphical models," *International Journal on Artificial Intelligence Tools*, vol. 14, no. 03, pp. 507–543, 2005.

[316] C. S. Yiu, K. Grant, and D. Edgar, "Factors affecting the adoption of internet banking in hong kong?implications for the banking sector," *International journal of information management*, vol. 27, no. 5, pp. 336–351, 2007.

[317] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and tam in online shopping: An integrated model," *MIS quarterly*, vol. 27, no. 1, pp. 51–90, 2003.

[318] J. A. Castaneda, D. M. Frías, and M. A. Rodríguez, "Antecedents of internet acceptance and use as an information source by tourists," *Online Information Review*, vol. 33, no. 3, pp. 548–567, 2009.

[319] D. Gefen and D. W. Straub, "The relative importance of perceived ease of use in is adoption: A study of e-commerce adoption," *Journal of the association for Information Systems*, vol. 1, no. 1, p. 8, 2000.

[320] Y. Y. Mun and Y. Hwang, "Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model," *International journal of human-computer studies*, vol. 59, no. 4, pp. 431–449, 2003.

[321] N. Notario, A. Crespo, Y.-S. Martín, J. M. Del Alamo, D. Le Métayer, T. Antignac, A. Kung, I. Kroener, and D. Wright, "PRIPARE: Integrating privacy best practices into a privacy engineering methodology," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 151–158.

[322] D. Huth, "A pattern catalog forGDPR compliant data protection." in *PoEM Doctoral Consortium*, 2017, pp. 34–40.

[323] N. Notario, A. Crespo, A. Kung, I. Kroener, D. Le Métayer, C. Troncoso, J. M. del Álamo, and Y. S. Martín, "PRIPARE: a new vision on engineering privacy and security by design," in *Cyber Security and Privacy Forum*. Springer, 2014, pp. 65–76.

[324] T. Garsiel and P. Irish, "How browsers work: Behind the scenes of modern web browsers," *Google Project, August*, 2011. [Online]. Available: https://www.html5rocks.com/en/tutorials/internals/howbrowserswork/

[325] D. Turner, M. Fossi, E. Johnson, T. Mack, J. Blackbird, S. Entwisle, M. K. Low, D. McKinney, and C. Wueest, "Symantec global internet security threat report–trends for july-december 07," *Symantec Enterprise Security*, vol. 13, pp. 1–36, 2008.

[326] M. Garnaeva, J. van der Wiel, D. Makrushin, A. Ivanov, and Y. Namestnikov, "Kaspersky security bulletin 2015," *Overall statistics for*, 2015.

[327] N. Virvilis, A. Mylonas, N. Tsalis, and D. Gritzalis, "Security busters: Web browser security vs. rogue sites," *Computers & Security*, vol. 52, pp. 90–105, 2015.

[328] R. Unuchek, M. Garnaeva, D. Makrushin, F. Sinitsyn, and A. Liskin, "IT threat evolution Q1 2017. Statistics," *Securelist.com*, vol. 12, 2017. [Online]. Available: https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

[329] R. Wash and E. J. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users." in *SOUPS*, 2015, pp. 309–325.

[330] J. Sauer, K. Seibel, and B. Rüttinger, "The influence of user expertise and prototype fidelity in usability tests," *Applied ergonomics*, vol. 41, no. 1, pp. 130–140, 2010.

[331] M. Walker, L. Takayama, and J. A. Landay, "High-fidelity or low-fidelity, paper or computer? choosing attributes when testing web prototypes," in *Proceedings of the human factors and ergonomics society annual meeting*, vol. 46, no. 5. SAGE Publications Sage CA: Los Angeles, CA, 2002, pp. 661–665.

[332] H. M. Khalid, "Embracing diversity in user needs for affective design," *Applied ergonomics*, vol. 37, no. 4, pp. 409–418, 2006.

[333] R. Sefelin, M. Tscheligi, and V. Giller, "Paper prototyping-what is it good for?: a comparison of paper-and computer-based low-fidelity prototyping," in *CHI'03 extended abstracts on Human factors in computing systems*. ACM, 2003, pp. 778–779.

[334] I. Corp, "Ibm spss statistics for windows, version 25.0," *Armonk, NY: IBM Corp*, 2017.

[335] D. Manzey, M. Luz, S. Mueller, A. Dietz, J. Meixensberger, and G. Strauss, "Automation in surgery: the impact of navigated-control assistance on performance, workload, situation awareness, and acquisition of surgical skills," *Human factors*, vol. 53, no. 6, pp. 584–599, 2011.

[336] K. R. Heere and R. E. Zelenka, "A comparison of Center/TRACON automation system and airline time of arrival predictions," National Aeronautics and Space Administration (NASA), Tech. Rep., 2000.

[337] A. J. Sharkey, "Should we welcome robot teachers?" *Ethics and Information Technology*, vol. 18, no. 4, pp. 283–297, 2016.

[338] M. P. Groover, *Automation, production systems, and computer-integrated manufacturing*. Prentice Hall Press, 2007.

[339] J. Frketic, T. Dickens, and S. Ramakrishnan, "Automated manufacturing and processing of fiber-reinforced polymer (frp) composites: An additive review of contemporary and modern techniques for advanced materials manufacturing," *Additive Manufacturing*, vol. 14, pp. 69–86, 2017.

[340] V. Cheval, H. Comon-Lundh, and S. Delaune, "Automating security analysis: symbolic equivalence of constraint systems," in *International Joint Conference on Automated Reasoning*. Springer, 2010, pp. 412–426.

[341] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, pp. 12–27, 2017.

[342] R. Montesino and S. Fenz, "Automation possibilities in information security management," in *Intelligence and Security Informatics Conference (EISIC), 2011 European*. IEEE, 2011, pp. 259–262.

[343] L. F. Cranor, "A framework for reasoning about the human in the loop," *Advanced Computing Systems Professional and Technical Association*, 2008.

[344] B. Shneiderman and C. Plaisant, "Sharpening analytic focus to cope with big data volume and variety," *IEEE computer graphics and applications*, vol. 35, no. 3, pp. 10–14, 2015.

[345] J. Nielsen, "Progressive disclosure," *Jakob Nielsen's Alertbox*, 2006.

[346] G. A. Fink, C. L. North, A. Endert, and S. Rose, "Visualizing cyber security: Usable workspaces," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*. IEEE, 2009, pp. 45–56.

[347] J. R. Goodall, "Introduction to visualization for computer security," in *VizSEC 2007*. Springer, 2008, pp. 1–17.

[348] F. Abel, V. Dimitrova, E. Herder, and G.-J. Houben, "Augmenting user models with real world experiences to enhance personalization and adaptation," in *International Conference on User Modeling, Adaptation, and Personalization*. Springer, 2011, pp. 31–34.

[349] P. d. Meo, E. Ferrara, F. Abel, L. Aroyo, and G.-J. Houben, "Analyzing user behavior across social sharing environments," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 5, no. 1, p. 14, 2013.

[350] F. Abel, E. Herder, and D. Krause, "Extraction of professional interests from social web profiles," *Proc. UMAP*, vol. 34, 2011.

[351] A. Ammari, V. Dimitrova, and D. Despotakis, "Semantically enriched machine learning approach to filter youtube comments for socially augmented user models," *UMAP*, pp. 71–85, 2011.

[352] D. Despotakis, L. Lau, and V. Dimitrova, "A semantic approach to extract individual viewpoints from user comments on an activity," *Proc. UMAP*, 2011.

[353] D. Laney, "3d data management: Controlling data volume, velocity and variety," *META Group Research Note*, vol. 6, p. 70, 2001.

[354] A. A. Cárdenas, P. K. Manadhata, and S. Rajan, "Big data analytics for security intelligence," *University of Texas at Dallas@ Cloud Security Alliance*, 2013.

[355] T.-F. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, and E. Kirda, "Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks," in *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, 2013, pp. 199–208.

[356] R. Juárez-Ramírez, R. Navarro-Almanza, Y. Gomez-Tagle, G. Licea, C. Huertas, and G. Quinto, "Orchestrating an adaptive intelligent tutoring system: towards integrating the user profile for learning improvement," *Procedia-Social and Behavioral Sciences*, vol. 106, pp. 1986–1999, 2013.

[357] P. V.-C. Chang, "The validity of an extended technology acceptance model (TAM) for predicting intranet/portal usage," *School of Information and Library Science*, 2004.

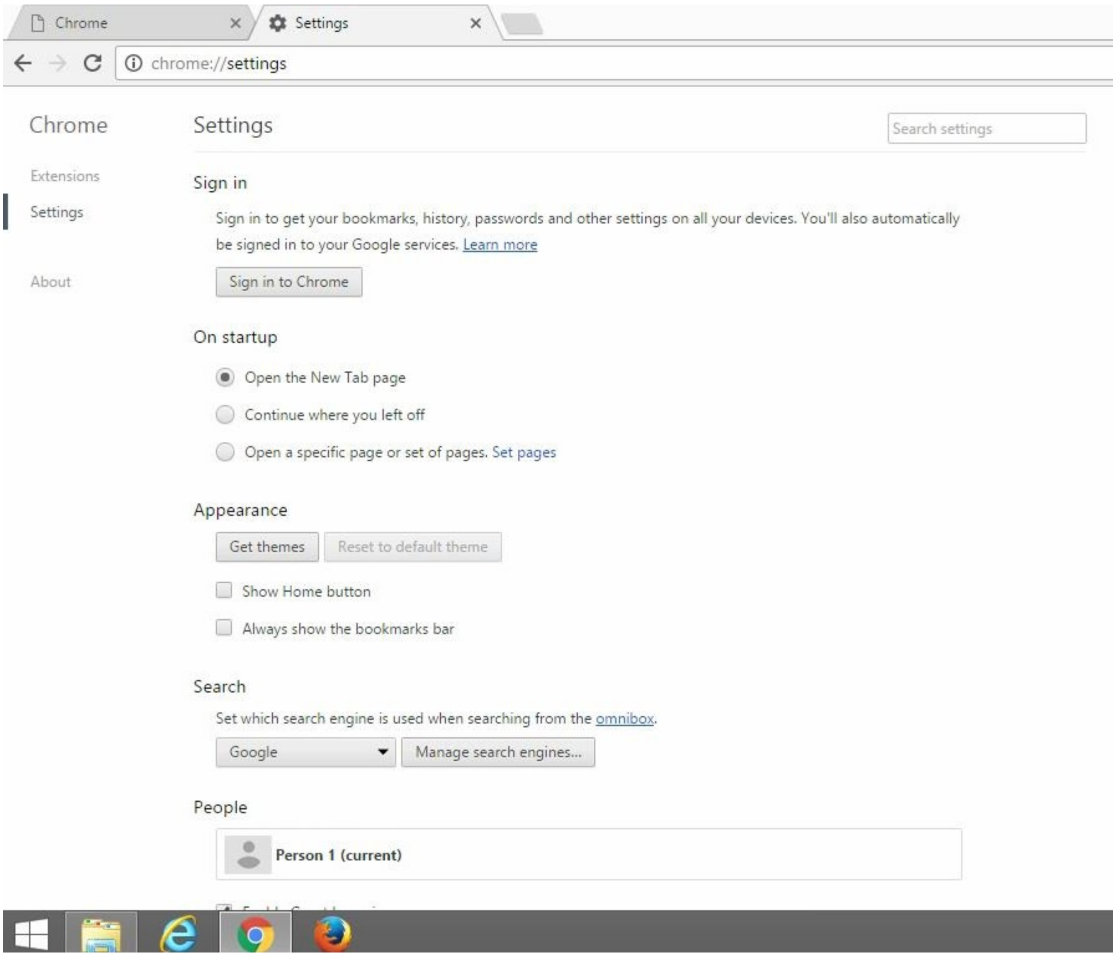
[358] J. Lu, C. Lu, C.-S. Yu, and J. E. Yao, "Exploring factors associated with wireless internet via mobile technology acceptance in mainland china," *Communications of the IIMA*, vol. 3, no. 1, p. 9, 2014.

[359] R. K. Chellappa and R. G. Sin, "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information technology and management*, vol. 6, no. 2, pp. 181–202, 2005.

[360] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish, "Anonymity, privacy, and security online," *Pew Research Center*, 2013.

Appendix A

Screenshots of the security interfaces tested in Chapter 4



Chrome

Extensions

Settings

About

Settings

Search settings

Sign in

Sign in to get your bookmarks, history, passwords and other settings on all your devices. You'll also automatically be signed in to your Google services. Learn more

Sign in to Chrome

On startup

● Open the New Tab page

○ Continue where you left off

○ Open a specific page or set of pages. Set pages

Appearance

Get themes | Reset to default theme

□ Show Home button

□ Always show the bookmarks bar

Search

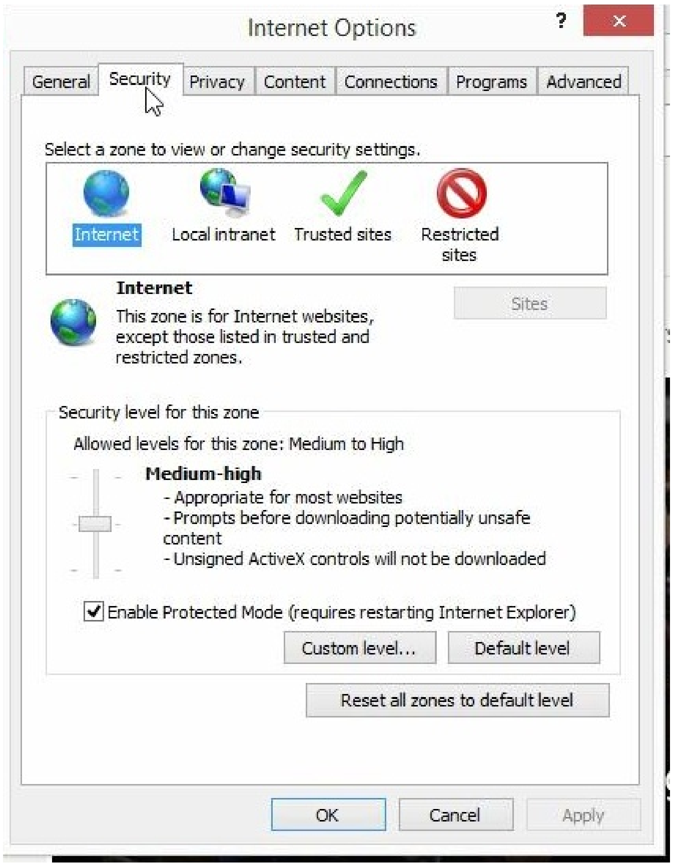
Set which search engine is used when searching from the omnibox.

Google ▾ | Manage search engines...

People

Person 1 (current)

FIGURE A.1: Main settings page for security in Google



Internet Options

Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

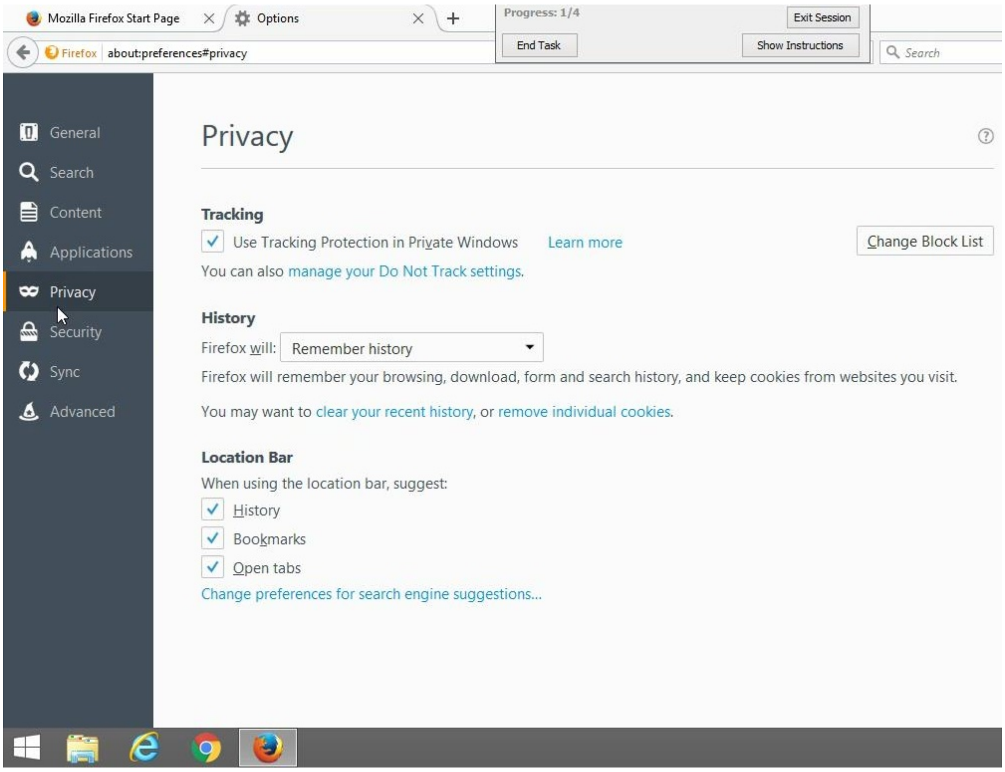
Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

FIGURE A.2: Main settings page for security in IE



Privacy

Tracking

☑ Use Tracking Protection in Private Windows Learn more

You can also manage your Do Not Track settings.

History

Firefox will: Remember history

Firefox will remember your browsing, download, form and search history, and keep cookies from websites you visit.

You may want to clear your recent history, or remove individual cookies.

Location Bar

When using the location bar, suggest:

☑ History

☑ Bookmarks

☑ Open tabs

Change preferences for search engine suggestions...

FIGURE A.3: Security UI for the Firefox version evaluated in Chapter 4

Appendix B

Observers' Task Sheet for Testing User Experience with Cybersecurity

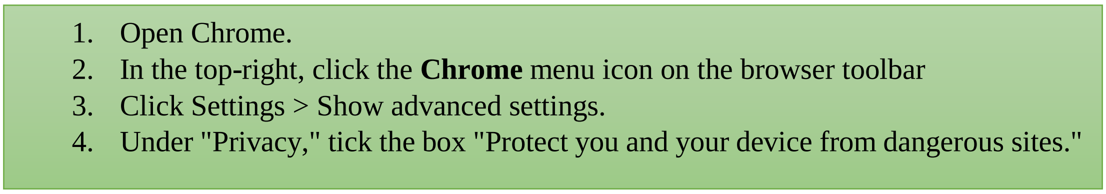
Please consider the following scenarios where you will be required to perform specific task to optimise the security settings of the following web browsers:

1. Google Chrome
2. Firefox and
3. Internet Explorer

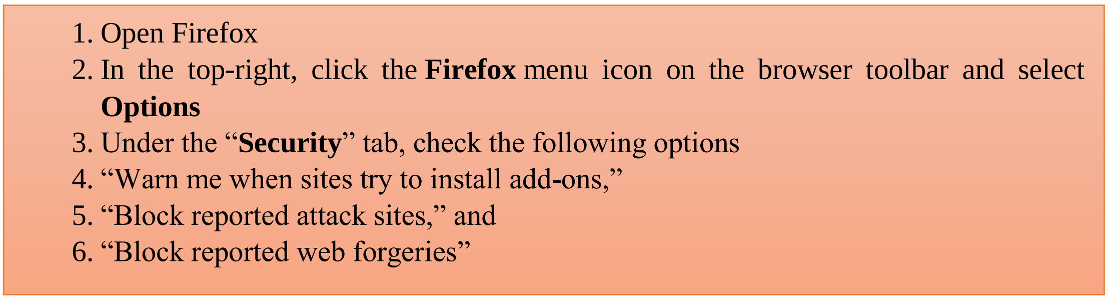
Please talk aloud and explain your thought processes while you are performing these tasks.

Scenario 1 – Security settings: You have recently purchased a new laptop and you have made a resolution to start using the internet securely to protect your data you therefore want to optimise the security settings of your default web browser before you start browsing on the internet.

Task 1: Navigate to where you can set your browser to protect you and your device from dangerous sites that can lead to phishing or malware invasion on your new laptop.



1. Open Chrome.
2. In the top-right, click the **Chrome** menu icon on the browser toolbar
3. Click Settings > Show advanced settings.
4. Under "Privacy," tick the box "Protect you and your device from dangerous sites."



1. Open Firefox
2. In the top-right, click the **Firefox** menu icon on the browser toolbar and select **Options**
3. Under the "**Security**" tab, check the following options
4. "Warn me when sites try to install add-ons,"
5. "Block reported attack sites," and
6. "Block reported web forgeries"

1. Open Internet Explorer, select the Tools button, and then select **Internet options**.
2. Select the **Security** tab and customize your security zone settings in these ways:
3. To change settings for any security zone, select the zone icon, and then move the slider to the security level that you want.
4. To create your own security settings for a zone, select the zone icon, and then select **Custom level** and choose the settings that you want.
5. If you chose Local intranet in the previous step, select Advanced, and then do one of the following:
6. Add a site. Enter a URL into the Add this website to the zone box, and then select Add.
7. Remove a site. Under Websites, select the URL you want to remove, and then select Remove.
8. On the Advanced tab, under Security, select the **Enable Enhanced Protected Mode** check box, and then select OK. You'll need to restart your PC before this setting takes effect.

Scenario 2 – Privacy Settings: You normally use your computer just to browse for information related to your studies and news item so you have never seen the need to optimise the security of your web browser. You recently started working on a project which you rather want to keep private hence have become very uncomfortable with the knowledge that anything you type into your address bar is instantly sent to google or other search engines. Although this feature of your browser makes searching for information more convenient, it also means that information about sites that you visit are also collected.

Task 2: Configure your content settings paying attention to what your personal policies are with regards to Cookies, JavaScript, Pop-ups, and other privacy related settings to optimise security and improve your privacy status.

1. Open Chrome.
2. In the top-right, click the **Chrome** menu icon on the browser toolbar
3. Click Settings > Show advanced settings.
4. Under "Privacy," click on “Content Settings…”
5. Under Cookies, select “Keep local data only until you quit your browser”
6. Under JavaScript, select “Do not allow any site to run JavaScript.”
7. Under Pop-ups, select “Do not allow any site to show pop-ups.”

Disable the instant search feature of your browser to minimise the kind of information being collected about your browsing activities.

8. 8. Go to Google home page (google.co.uk)
9. 9. At the bottom, right of the screen, click on **Settings** and then select '**Search Settings**' from the pop up menu.
10. 10. Find the section marked “Google Instant predictions” and select “Never show Instant results”

1. Open Firefox
2. In the top-right, click the **Firefox** menu icon on the browser toolbar and select **Options**
3. Under the “**Content**” tab,
   - Deselect “Enable JavaScript”
   - Select “Block pop-up windows”
4. Under the “**Privacy**” tab,
   - Deselect “Accept third-party cookies”,
   - Select “**I close Firefox**” from the “**Keep until**” dropdown list and
   - Select “Clear history when Firefox closes.”

1. Open Internet Explorer, select the Tools button, and then select Internet options.
2. On the Privacy tab, under Pop-up Blocker, select Settings.
   - In the Pop-up Blocker settings dialog box, under Blocking level, set the blocking level to High: Block all pop-ups (Ctrl + Alt to override).
   - Select Close, and then select OK.
3. In Internet Explorer, select the Safety button, and then select Delete Browsing History.
   - Select the check box next to Cookies.
   - Select the Preserve Favourites website data check box if you don't want to delete the cookies associated with websites in your Favourites list.
   - Select Delete.

Scenario 3 – Encryption and Backup: You normally signed into your favourite web browser with you're the browser's user profile account and have all your preferences synced across all your other devices (desktops, laptops, tablets and smartphones) for convenience. You recently became aware of the fact that because you have enabled sync on your web browser, all your personal information such as passwords, autofill data, preferences, and more is stored on external servers.

Task 3: Create a unique passphrase for encryption of these personal information so that only someone with your passphrase can read your data or can sync your encrypted data to a new device. Also, where possible create a back-up for your browser data that you choose to sync.

1. Open Chrome.
2. In the top-right, click the **Chrome** menu icon on the browser toolbar
3. Click Settings > Advanced Sync Settings
4. Under "Encryption Options" select the "Encrypt all synced data" option and create a unique passphrase for encryption.

Mozilla Firefox stores all your personal settings, such as bookmarks, passwords and extensions, in a profile folder on your computer, in a location separate from the Firefox program. You will need to back-up your profile, as you won't be able to recover your browser data if you lose it.

1. Open Firefox
2. In the top-right, click the **Firefox** menu icon on the browser toolbar and select **Options**
3. Select the "**Sync**" tab and use the options here to select what you want to sync
4. Select the "**Security**" tab:
   - Deselect "Remember logins for sites" or
   - Select "Use a master password" and follow the instruction to set a strong master password
5. Click the **Firefox** menu icon, click **Help** icon and select "Troubleshooting Information". The Troubleshooting Information tab will open.
6. Under the "Application Basics" section, click on "Show Folder". A window with your profile files will open.
7. Go to one level above your profile's folder, i.e. to %APPDATA%\Mozilla\Firefox\Profiles\
8. Right-click on your profile folder (e.g. xxxxxxxx.default), and select Copy.
9. Right-click the backup location (e.g. a USB-stick or a blank CD-RW disc), and select Paste.

To backup saved passwords in IE:

Step 1: Download NirSoft's IE PassView from here, a free software to view and backup passwords saved in Internet Explorer browser.

Step 2: Extract the downloaded zip file to get IE PassView executable and then double-click on the same to run it.

Step 3: Upon running IE PassView, it will scan the browser for saved passwords and displays URLs, usernames and their passwords.

Step 4: To backup all passwords, select all entries, right-click on them and then click Save selected passwords to save all usernames and passwords in a text file.

Scenario 4 – Password Manager: You have had to create several user accounts for the various sites related to your work or personal online transactions. All these accounts have different usernames and passwords hence you use the password manager feature of your browser to facilitate logins for these sites. You were recently travelling on vacation and did not have access to your personal laptop. However, an urgent matter at your office requires you to access some of these user accounts including emails that you were unable to do with your smartphone. While doing this on a computer in a public library, you accidentally accepted the web browser's offer to help remember your password.

Task 4: Verify that you can remove a username and password for a given site and it will no longer autofill on that sight nor will it be listed in password manager

Steps/Description

1. Enable password manager function of the web browser
2. Go to a site that you that you will need to sign in, e.g. http://moodle.nottingham.ac.uk or http://www2.hm.com/en_cn/index.html
3. Enter your username and password
4. When a dialog appears asking if you would like to save this information, click yes
5. Go to settings and view the saved passwords
6. Highlight this site and username in the list and click remove but cancel/ choose No if the option is available
7. If step 6 is successful, go back to view the saved passwords again else go to step 9
8. Highlight the website and username in the list and click remove and Click ok
9. Logout and login back to the site
10. Logout and close the web browser

Repeat all the 4 tasks above until you have used all the 3 web browsers (Chrome, Firefox and IE)

Appendix C

Survey Instrument, Descriptions And References For Measured Items

Part 1 – Demographic Profile/ External Variables

Essential for defining personal aspects of users in specific contexts [112, 356].

Individual Differences – Demographics	**Options**
Gender What is your gender?	A. Male B. Female C. Prefer not to say
Age In which category is your age?	A. 18-24 years B. 25-34 years C. 35-44 years D. 45-64 years E. 65-74 years F. 75 years or older
Education What is the highest degree or level of education you have completed? If currently enrolled, mark the previous grade or highest degree received.	A. 12th grade or less (no diploma) B. High school diploma C. Some college, no degree D. Associate or technical degree E. Bachelor's degree F. Graduate degree/professional
Employment Status	A. Employed for wages B. Self-employed C. Out of work and looking for work D. Out of work but not currently looking for work E. A homemaker F. A student G. Retired H. Unable to work
Income What category best describes your annual household income?	A. Less than $10,999 B. $11,000 to $49,999 C. $50,000 to 99,999 D. $100,000 or more

Ethnicity How would you classify yourself?	A. Arab B. Asian/Pacific Islander C. African/Black D. Caucasian/White E. Hispanic F. Latino G. Multiracial H. Other:......................
Physical Environment/Location Please indicate how often you use a notebook computer in the following locations.	A. Home: B. Apartment Lounge: C. Friend's house: D. Coffee Shop: E. Students Residence Halls: F. Classrooms/ Lecture Halls G. Other:......................
Experience and/or Frequency of use The set of questions here will be used to determineusers level of experience with web browser security settings as well as actualusage [113, 357]. How many times do you use web browsers during a week?	A. not at all B. once/week C. several times/week D. less than once/day E. once/day F. 2-3/day G. bseveral times/day
Which of the following web browsers are you most familiar with?	A. Internet Explorer B. Google Chrome C. Firefox D. Other:......................
Which of the following web browser design do you prefer and/or find enjoyable to use?	A. Internet Explorer B. Google Chrome C. Firefox D. Other:......................
How often do you change security settings on your web browser?	A. not at all B. once/week C. several times/week D. less than once/day E. once/day F. 2-3/day G. several times/day

Domain Knowledge(DK) Adapted from Milne et al. [116]. DK_1: I have hadsignificant experience with configuring my browser security settings in thepast. DK_2: I am knowledgeable about cybersecurity and privacy related technologies. DK_3: I am skilled at avoiding dangers while browsing the internet	5-point Likert scale type strongly agree — strongly disagree

Individual Differences – Descriptive Charateristics
SE and SBCL are PMT constructs used to examine the mediating effects of participant's protection motivation on cybersecurity behaviours. The set of questions here are used to examine users level of experience with their preferred web browser as well as exposure to web browser security issues and protection motivation levels [113, 357]. SE items are adapted from the instrument developed and empirically validated by [293] while SBCL items are adapted from [291].

Self-Efficacy (SE)
I could optimise my web browser security settings . . .
SE_1: . . . if I had only the web browser manuals for reference.
SE_2: . . . if I had seen someone else doing it before trying it myself (Reverse Coded)
SE_3: . . . if there was no one around to tell me what to do as I go

Security Breach Concern Level (SBCL)
SBCL_1: Cybersecurity issues affects me directly
SBCL_2: Cybersecurity threats are exaggerated (Reverse Coded)
SBCL_3: I think cybersecurity issues should be taken seriously
SBCL_4: Security breaches are only targeted at organizations (Reverse Coded)

System Characteristics (SC) — SC assesses participants view on the user friendliness of their preferred web browser and are measured using items from [130, 136]. The construct is used to elicit individual preferences in terms of the Design, Terminology/ Language and Navigation of the browser security interface/ user interactions(IC) with the following items:
IC_1: I understand the terms used on my preferred browser security interfaces
IC_2: Layout of the browser security interface is clear and consistent

IC_3: The sequence of screens for security settings are difficult to navigate (Reverse Coded)

IC_4: Security functions are well depicted by buttons and symbols

---

Part 2 (A) – User Perceptions (TAM & PMT)

Perceived Ease of Use (PEOU) – is "the degree to which an individual believes that using a particular system would be free of physical and mental effort [96]." Likert type statements were adapted from previously validated measurement inventory of TAM variables and rephrased for web browser security settings [117, 136, 248, 358].

PEOU_1: Learning to configure a browser security settings is easy for me

PEOU_2: Interacting with the interface for web browser security settings does not require a lot of my mental effort

PEOU_3: My interaction with web browser security settings is clear and understandable

PEOU_4: I find it easy to optimise my web browser security to the level of protection I want for my computer and privacy

Perceived Usefulness (PU) – which is also adapted from TAM's scale items is the degree to which a person believes web browser security settings would improve their protection against cyber-attacks [96].

PU_1: Web browser security functionalities gives me greater control over my safety and privacy online

PU_2: Overall, I find browser security settings useful in protecting my computer from cyber attacks

PU_3: Optimising my browser security settings gives me peace of mind when I am working with the internet

PU_4: The sensitive nature of information I search for and/or store on my personal computer requires me to optimise my web browser security settings

Perceived Risk (PR) – Questionnaire items for perceived risk was adapted from [112]. Their research findings indicate that perceived risk indirectly impacts intentions to use an online application under security threats.

PR_1: Security functionalities embedded in web browsers are not adequate for preventing cyber attacks

PR_2: It is important to optimise browser security when visiting sites that requires data input

PR_3: I can make mistake whiles configuring my browser settings which can cause damage to my computer

Value for Personalization (VFP) – in this study VFP refers to the level of appreciation that a user has for all types of personalization possibilities within cyberspace. Items were adapted from the value of online personalisation scale developed and validated by Chellappa and Sin [359].

VFP_1: I value online applications that are personalized based on information that is collected automatically (such as IP address, pages viewed, access time) but cannot identify me as an individual.

VFP_2: I value products and services that are personalized on information that I have voluntarily given out (such as age range, salary range, Zip Code) but cannot identify me as an individual.

VFP_3: I value application interfaces that are personalized for the device (e.g. desktop, mobile phone, tablet, etc.), browser (e.g. Internet explorer, Chrome, Firefox, etc.) and operating system (e.g. Windows, Unix) that I use.

Part 2 (B) — Attitude to Personal Data (APD)

To minimize survey fatigue, the APD scale adopted from [279] is simplified based overall cluster membership predictor importance of the APD factors as well as reliability score of the measured items.

Protection

PDP_1: I regularly look out for new policies on personal data protection

PDP_2: I consider the privacy policy of institutions where I give out such personal details

PDP_3: I don't always optimize my privacy settings when I create an online profile (Reverse Coded)

Awareness

PDA_1: Such details about me are of value to external organizations

PDA_2: Researchers don't need my consent to access my personal details (Reverse Coded)

PDA_3: Data collection organizations need to disclose the way the data are collected processed and used.

Privacy Concern

PRI_1: I am sensitive about giving out information regarding my preferences

PRI_2: I am concerned about anonymous information (information collected automatically but cannot be used to identify me, such as my computer, network information, operating system, etc.) that is collected about me.

Part 3 — Cybersecurity Behavioural Intentions

Personalized Cybersecurity Adoption Intention (BI) — Items used to examine participants' general attitude to personalized adaptive web browser security are adapted from [113, 358].

BI_1: I am likely to accept personalized browser security update notification
BI_2: It is possible that I will allow adjustments to my web browser security settings to improve my safety online
BI_3: I am certain that I will pay attention to cybersecurity alerts tailored to my personal preference

Actual Cybersecurity Behaviour (ACB) – Items determining user interaction with web browser security settings were selected and adapted from the list of strategies people adopt to protect themselves online identified by [360].

ACB_1: I have used service that allows me to browse the web anonymously
ACB_2: I don't set my browser to disable or turn off cookies (Reverse Coded)
ACB_3: I regularly clear cookies and browser history while I use the internet
ACB_4: I sometimes encrypt my communications while using the internet

---

Part 4 - Components of personalization

Items were adapted from [298] to acquire participants' ratings of the personalization dimensions identified for the purposes of building a BN-based model for adaptive cybersecurity.

User preference

1. Please indicate the importance of the following user interface characteristics to be considered in personalizing your web browser security and privacy settings:

a Language
b Presentation style (popup, icon change etc.)
c Navigation style (buttons, drop down etc.)
d Level of Information (Detailed vs. simplified)
e Others (please specify)

Adaptive Cybersecurity

2. Please indicate the importance of the following characteristics of an adaptive cybersecurity to be considered in personalizing your web browser security and privacy settings.

a User Effort Required
b Benefit of the security configuration
c Cost of the automated configuration
d Others (please specify)

Context

3. Please indicate the importance of the following contextual factors , which should be taken into consideration in personalizing your web browser security and privacy settings.

a Browser Type

b Enabled Browser Extensions
c Location
d Time
e Others (please specify)

User Goals/Needs

3. Please indicate the importance of the following user actions, which should be taken into consideration in personalizing your web browser security and privacy settings.

a Active Browsing session
b Browser History
c Explicit security/privacy queries
d Previous acceptance of personalized cybersecurity
e Others (please specify)

Appendix D

Participant's Task Sheet for Prototype Evaluation

There are three newly installed web browsers on your desktop:

1. Firefox Version 63.0.3 (Latest version as at 2018-11-16)
2. SecAdapt StdV1
3. SecAdapt V2

Please consider the following scenarios that require you to perform a specific task to optimise the security and privacy controls of these three web browsers. Please talk aloud and explain your thought processes while you are performing these tasks.

1. Security Scenario

You have recently purchased a new laptop and you have made a resolution to start using the internet in a more secure manner so as to prevent cyber attacks. You, therefore, want to improve the security settings of your default web browser before you start browsing on the internet. Your new laptop comes with a new web browser called SecAdapt with an agent that will assist you in meeting your security and privacy needs while browsing the internet. To activate the agent you will need to fill a registration form once and SecAdapt can then use the details you provide along with your interactions and other available metrics to adapt the security and privacy configurations according to your personal preferences.

Task 1

Set your browser to protect you and your device from dangerous sites that can lead to phishing or malware invasion on your new laptop manually, and/ or by activating the automated assistance in version 2 of SecAdapt browser.

Please express your opinions about the prototype and how you feel about the design while interacting with the interface

2. Privacy Scenario

You normally use your computer just to browse for information related to your studies and news item so you have never seen the need to elevate the privacy settings of your web browser. You recently started working on a project which you rather want to keep private hence have become very uncomfortable with the knowledge that your browsing activities are being monitored for personalized content and services. Although these features of your browser make searching for information more convenient, it also means that information about sites that you visit are also collected.

Task 2

Configure your privacy settings to meet your personal preference and improve your privacy status online. In SecAdapt V2, you can enable the automated assistance for privacy settings.

Please keep expressing or talking about your personal privacy preferences while performing task 2 as well as how you feel about the interface design.

3. Data Back-up, Protection, and Restore Scenario

You normally sign into your favourite web browser with your user profile account and have all your preferences synced across all your other devices (desktops, laptops, tablets, and smartphones) for convenience. You recently became aware of the fact that because you have enabled sync on your web browser, all your personal information such as passwords, autofill data, preferences, and more are stored on external servers. Additionally, SecAdapt and Firefox store all your personal settings, such as bookmarks, passwords, and extensions, in a profile folder on your computer, in a location separate from the web browser itself. You will need to create a back-up for your synced and stored browsing data, so you can recover them easily in case of loss from system damage or data corruption.

Take note that the back-up and restore feature may work differently in each of the 3 web browsers.

Task 3

Create a back-up for your browsing data that you choose to sync. Also, create a unique passphrase for encryption of your personal data stored by the browser so that only someone with your passphrase can read your data or can sync your encrypted data to a new device.

4. Password Management Scenario

You have had to create several accounts for the various sites related to your work or personal online transactions. All these accounts have different usernames and passwords hence you use the password manager feature of your browser to facilitate logins for these sites. You were recently traveling on vacation and did not have access to your personal laptop. However, an urgent matter at your office requires you to access some of these user accounts including emails that you were unable to do with your smartphone. While doing this on a computer in a public library, you accidentally accepted the web browser's offer to help remember your password.

Task 4

Navigate to where you can manage your password and verify that you can view as well as remove or change saved Login details that may have been compromised.

Please keep expressing your opinion about the prototype and how you feel about the design while interacting with the interface

Repeat all the 4 tasks above until you have used all the 3 web browsers!

Dummy Login Details

Google:	us275072@gmail.com	Password: dummy@2750
Google:	research.idic@gmail.com	Password: china317
Firefox Sync:	evaluation.login@outlook.com	Password: T3stp5wd1
Outlook:	evaluation.login@outlook.com	Password: T3stp5wd1

Appendix E

Initial Iterated Sketches and Mock-ups

The following diagrams depict some examples of early sketches and iterated designs for the prototypes. The medium fidelity prototype was designed following feedback gathered using these early sketches and mock-ups.

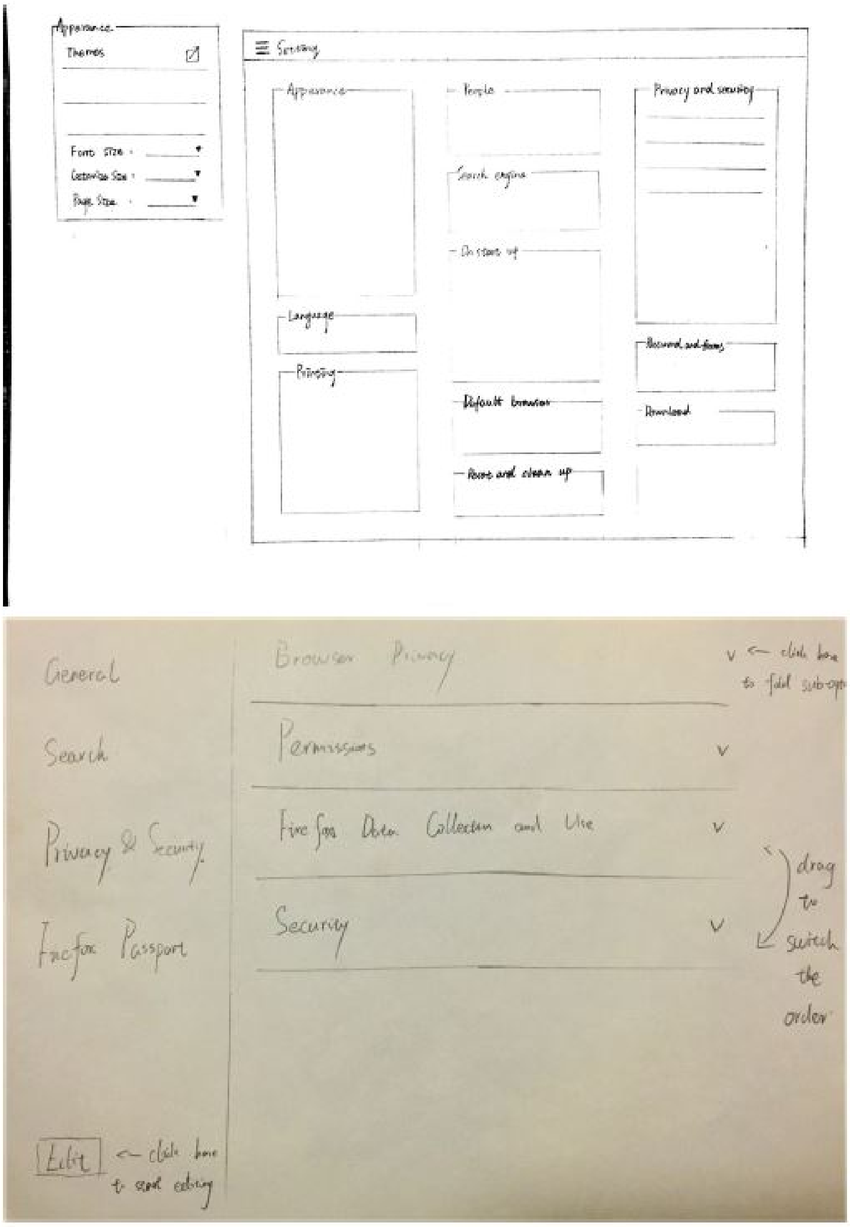


FIGURE E.1: Examples of early sketches

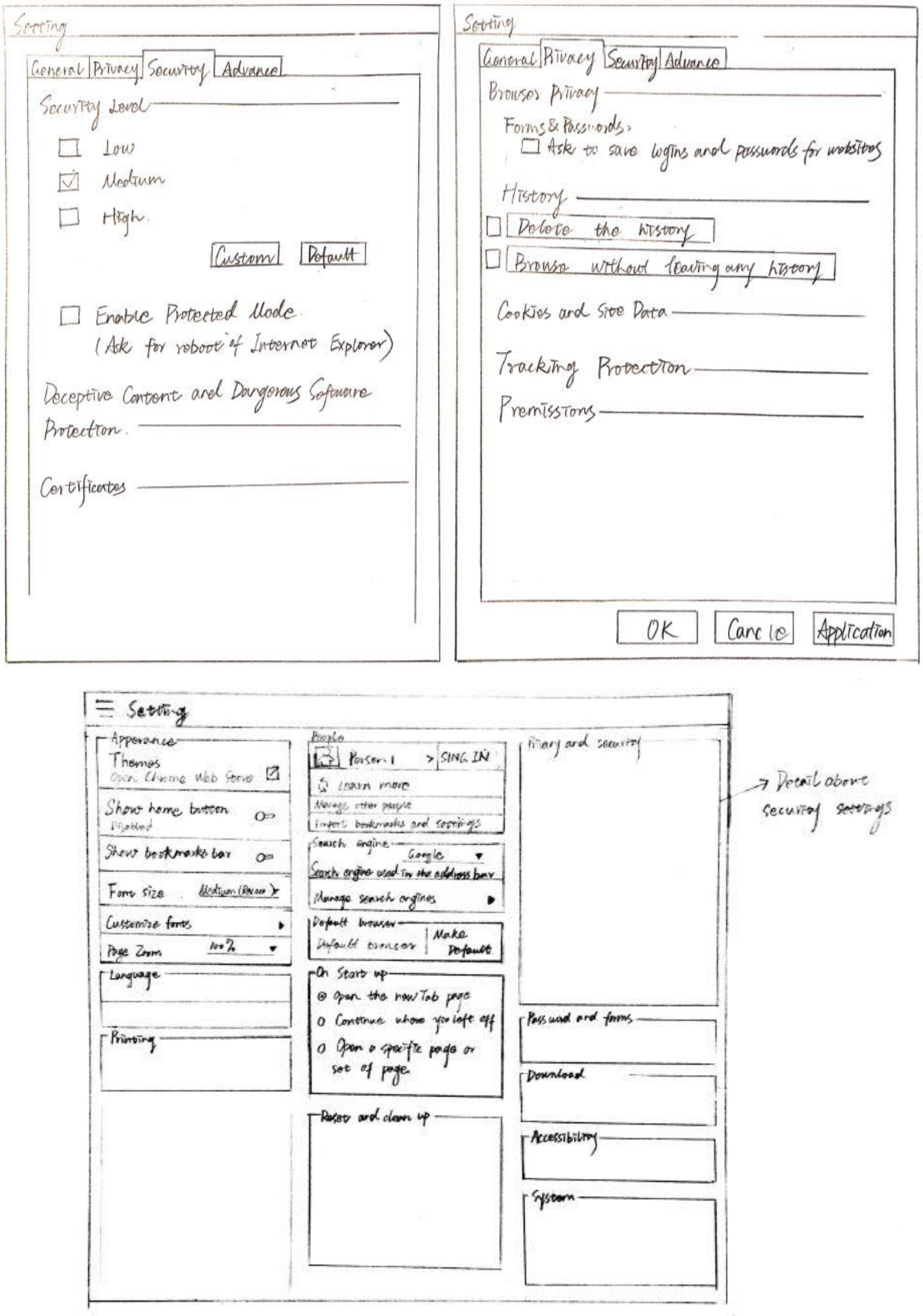


FIGURE E.2: Examples of early sketches

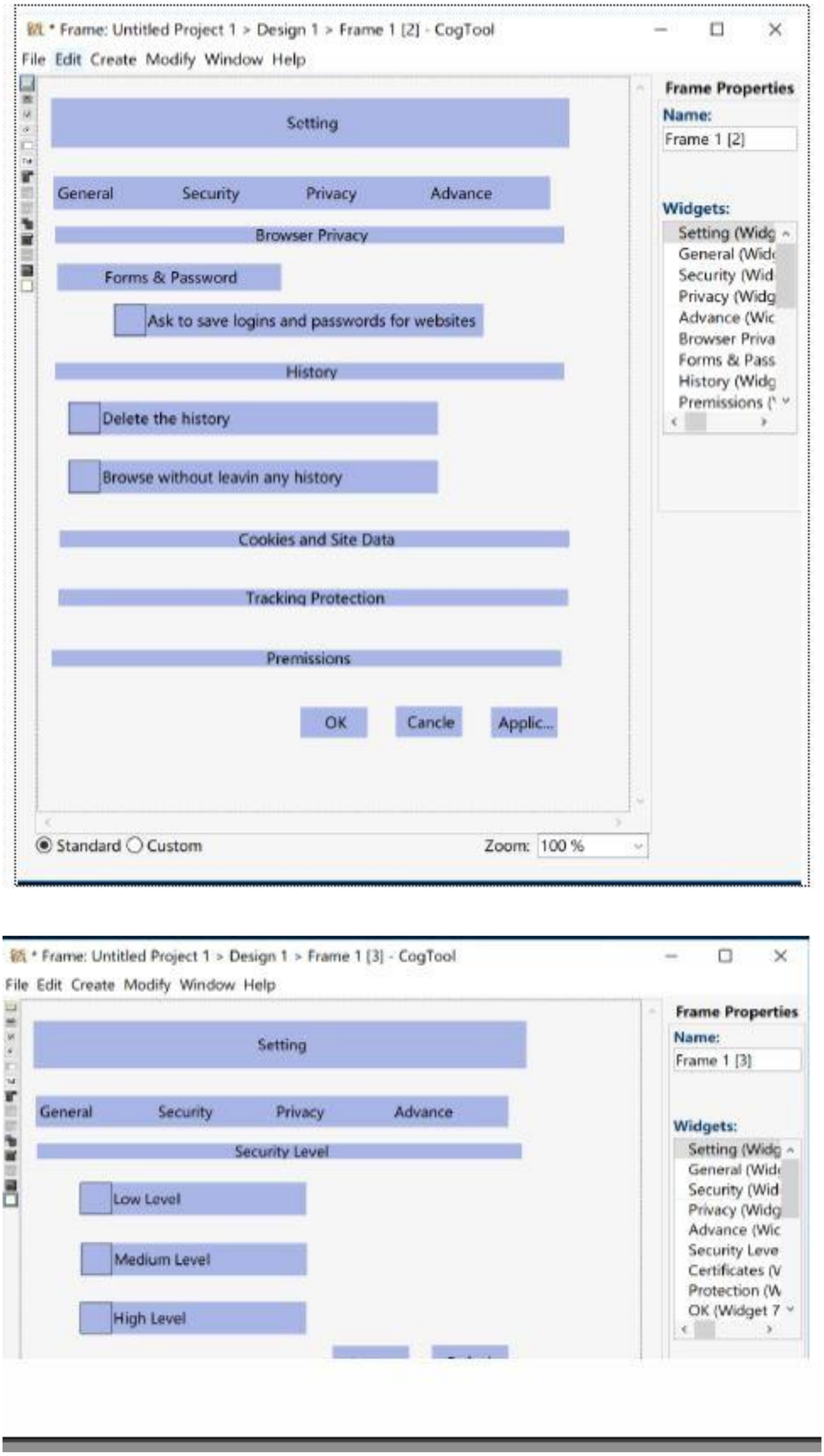
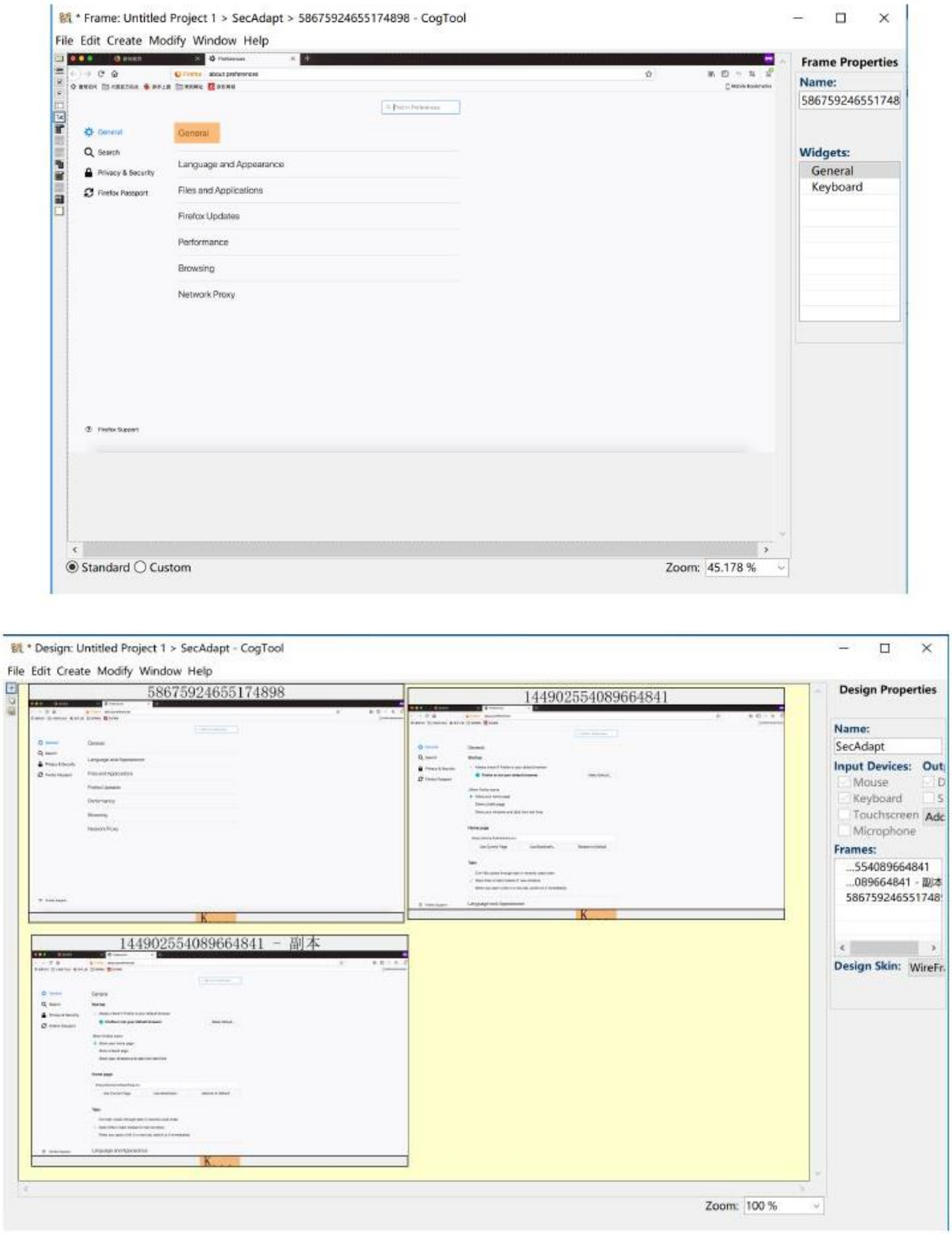


FIGURE E.3: Examples of mock-ups using CogTool



* Frame: Untitled Project 1 > SecAdapt > 58675924655174898 - CogTool

Frame Properties

Name: 586759246551748

Widgets:
General
Keyboard

● Standard ○ Custom

Zoom: 45.178 %

* Design: Untitled Project 1 > SecAdapt - CogTool

File Edit Create Modify Window Help
58675924655174898
144902554089664841
144902554089664841 - 副本
K

Design Properties

Name: SecAdapt

Input Devices:
□ Mouse
☑ Keyboard
□ Touchscreen
□ Microphone

Frames:
...554089664841
...089664841 - 副本
586759246551748

Design Skin: WireFr

Zoom: 100 %

FIGURE E.4: Screenshots of efficiency testing conducted with some of the early mockups in CogTool

Appendix F

Medium Fidelity Prototype SecAdapt: Screenshots

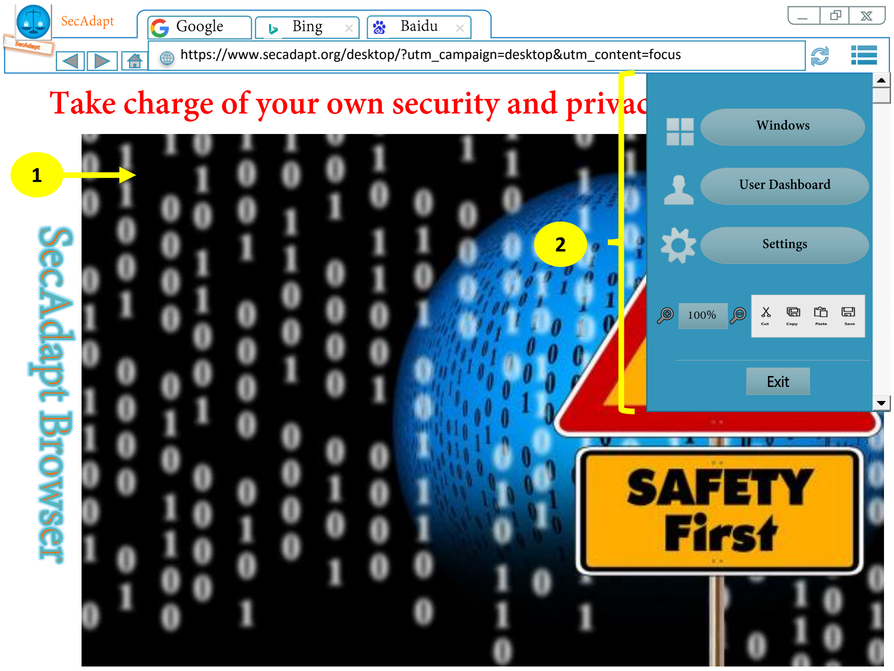
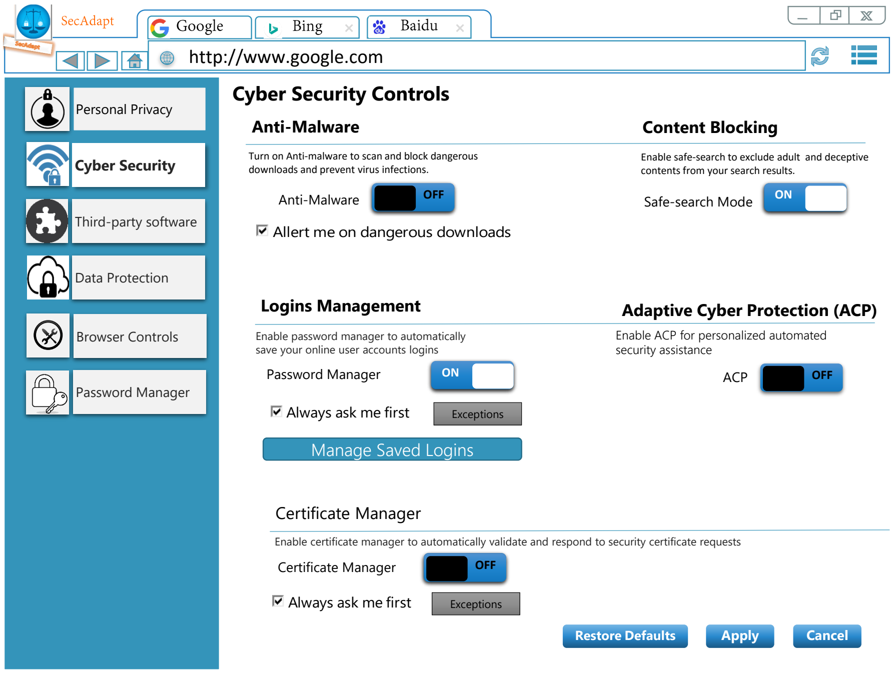

SecAdapt
Google
Bing
Baidu
https://www.secadapt.org/desktop/?utm_campaign=desktop&utm_content=focus
Take charge of your own security and privac
1
2
SecAdapt Browser
Windows
User Dashboard
Settings
100%
Exit
SAFETY
First

FIGURE F.1: SecAdapt home page designed for security awareness among users



Cyber Security Controls

Anti-Malware

Turn on Anti-malware to scan and block dangerous downloads and prevent virus infections.

Anti-Malware OFF

☑ Allert me on dangerous downloads

Content Blocking

Enable safe-search to exclude adult and deceptive contents from your search results.

Safe-search Mode ON

Logins Management

Enable password manager to automatically save your online user accounts logins

Password Manager ON

☑ Always ask me first Exceptions

Manage Saved Logins

Adaptive Cyber Protection (ACP)

Enable ACP for personalized automated security assistance

ACP OFF

Certificate Manager

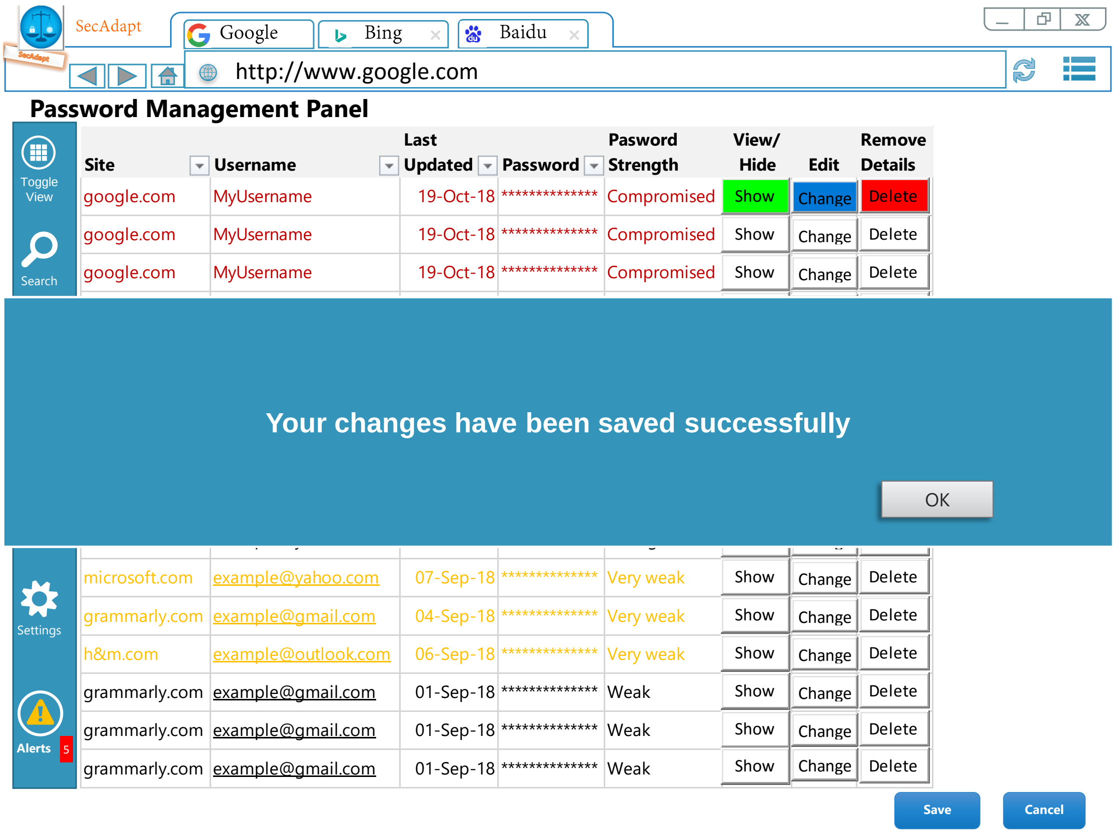
Enable certificate manager to automatically validate and respond to security certificate requests

Certificate Manager OFF

☑ Always ask me first Exceptions

Restore Defaults Apply Cancel

FIGURE F.2: Screenshot of the security settings page in SecAdapt V1



Password Management Panel

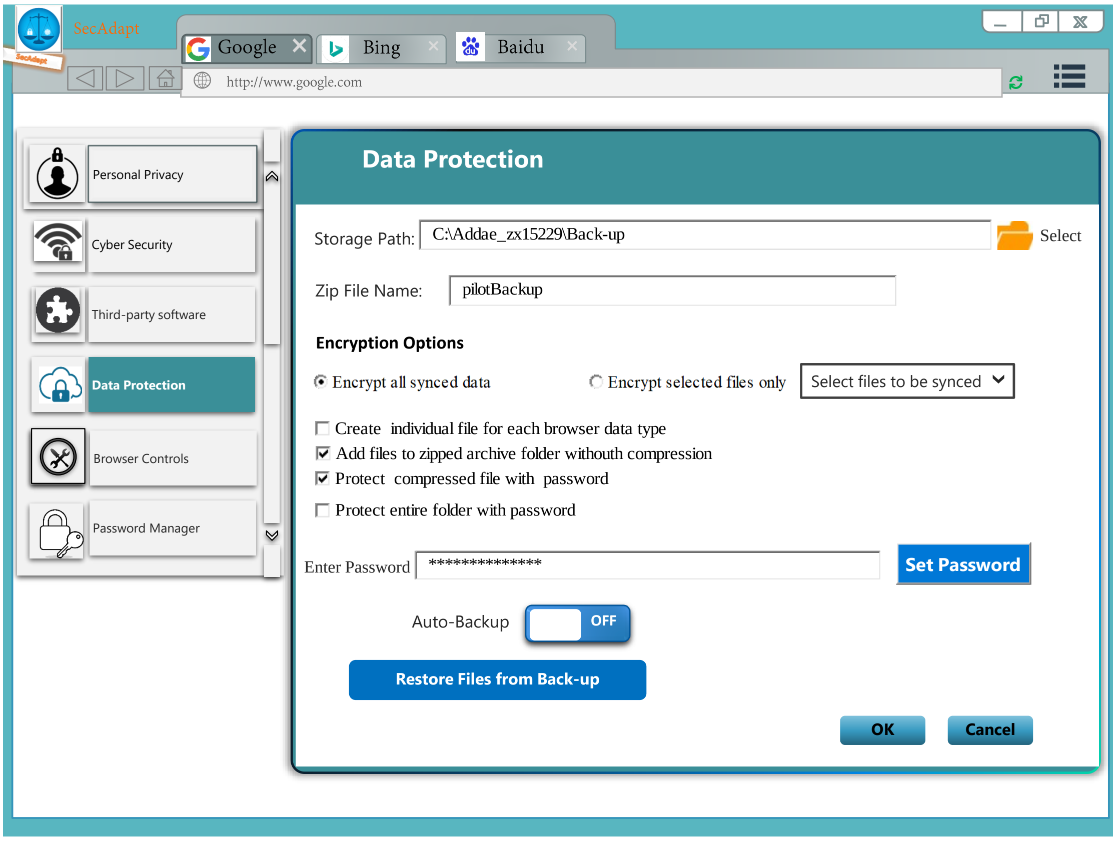
Site	Username	Last Updated	Password	Pasword Strength	View/ Hide	Edit	Remove Details
google.com	MyUsername	19-Oct-18	**************	Compromised	Show	Change	Delete
google.com	MyUsername	19-Oct-18	**************	Compromised	Show	Change	Delete
google.com	MyUsername	19-Oct-18	**************	Compromised	Show	Change	Delete
microsoft.com	example@yahoo.com	07-Sep-18	**************	Very weak	Show	Change	Delete
grammarly.com	example@gmail.com	04-Sep-18	**************	Very weak	Show	Change	Delete
h&m.com	example@outlook.com	06-Sep-18	**************	Very weak	Show	Change	Delete
grammarly.com	example@gmail.com	01-Sep-18	**************	Weak	Show	Change	Delete
grammarly.com	example@gmail.com	01-Sep-18	**************	Weak	Show	Change	Delete
grammarly.com	example@gmail.com	01-Sep-18	**************	Weak	Show	Change	Delete

Your changes have been saved successfully

OK

Save Cancel

FIGURE F.3: Screenshot of feedback on a password management task in SecAdapt V1



Data Protection

Storage Path: C:\Addae_zx15229\Back-up Select

Zip File Name: pilotBackup

Encryption Options

● Encrypt all synced data ○ Encrypt selected files only Select files to be synced

□ Create individual file for each browser data type

☑ Add files to zipped archive folder withouth compression

☑ Protect compressed file with password

□ Protect entire folder with password

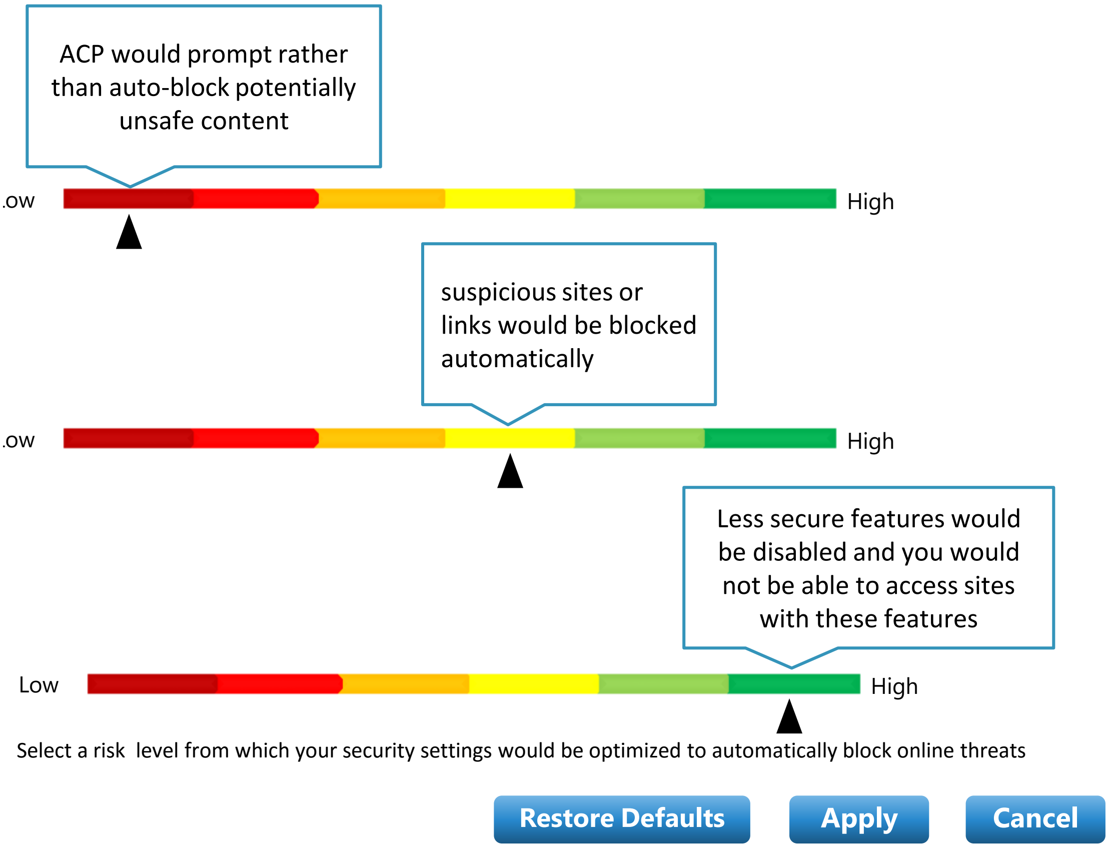
Enter Password *************** Set Password

Auto-Backup OFF

Restore Files from Back-up

OK Cancel

FIGURE F.4: Screenshot of the data protection interface in SecAdapt V2



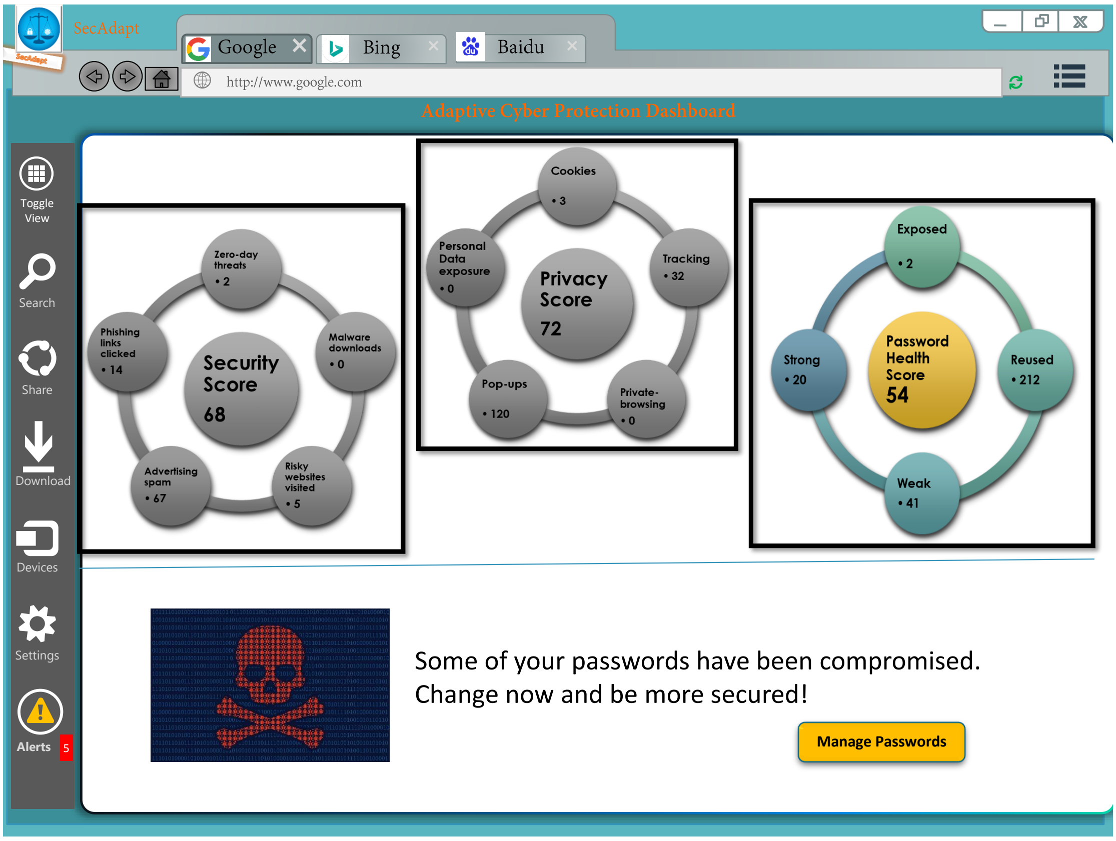
ACP would prompt rather than auto-block potentially unsafe content

suspicious sites or links would be blocked automatically

Less secure features would be disabled and you would not be able to access sites with these features

Select a risk level from which your security settings would be optimized to automatically block online threats

FIGURE F.5: Some levels of adaptive automation provided in SecAdapt V2



Some of your passwords have been compromised. Change now and be more secured!

FIGURE F.6: Example adaptive automated assistance for password safety management

Appendix G

Initial Implementation of SecAdapt V2

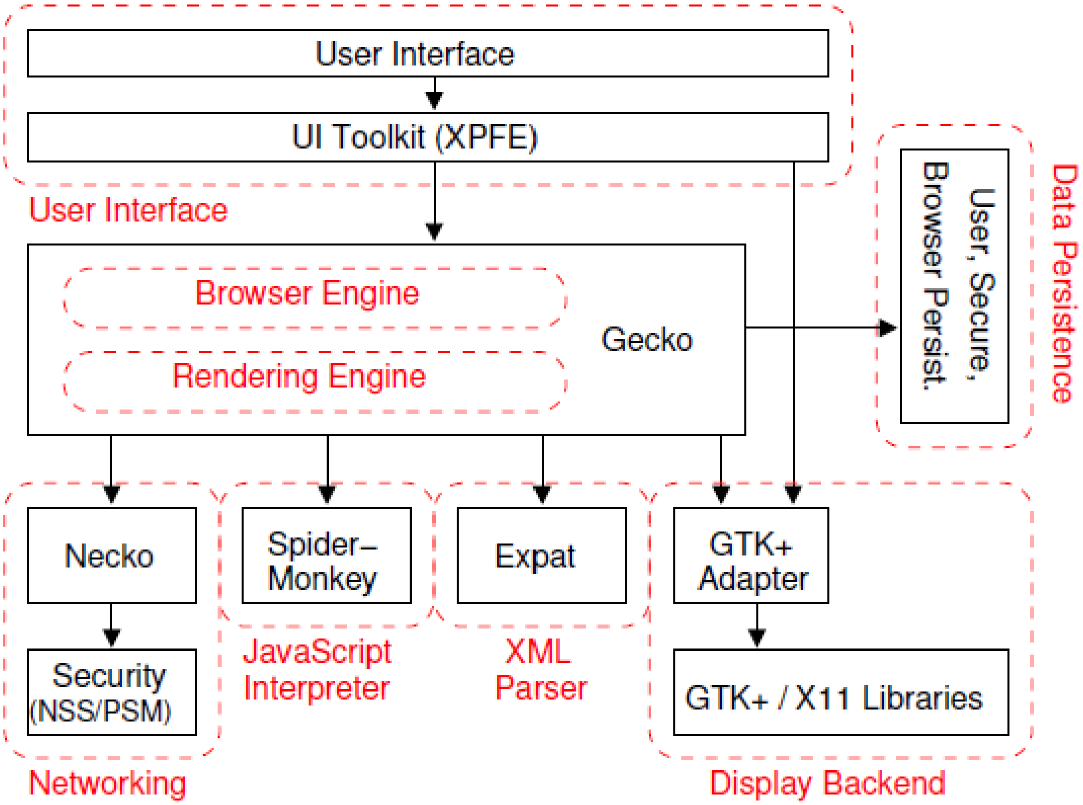
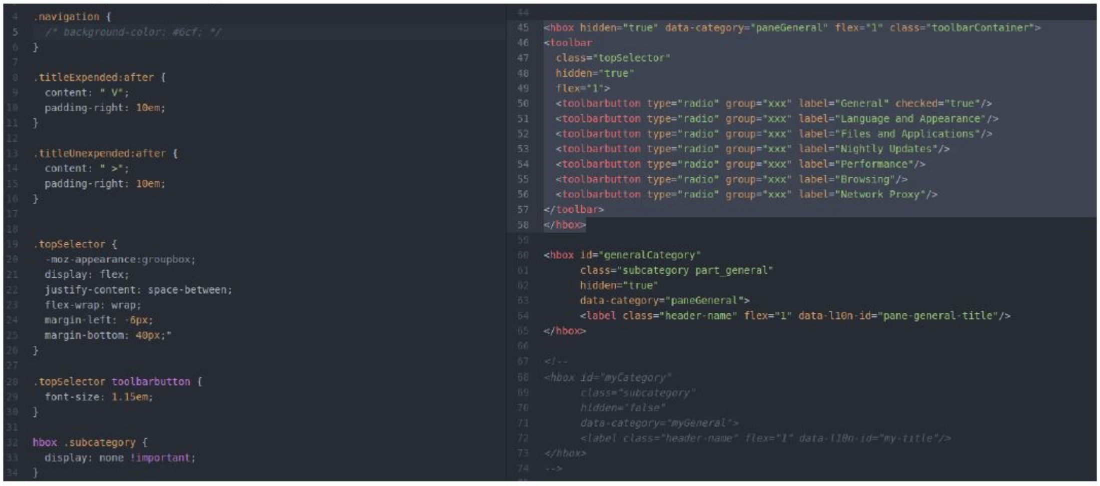


FIGURE G.1: Firefox Browser Architecture [6]



```
.navigation {
  /* background-color: #6cf; */
}

.titleExpended:after {
  content: " V";
  padding-right: 10em;
}

.titleUnexpended:after {
  content: " >";
  padding-right: 10em;
}


.topSelector {
  -moz-appearance:groupbox;
  display: flex;
  justify-content: space-between;
  flex-wrap: wrap;
  margin-left: -6px;
  margin-bottom: 40px;"
}

.topSelector toolbarbutton {
  font-size: 1.15em;
}

hbox .subcategory {
  display: none !important;
}
```

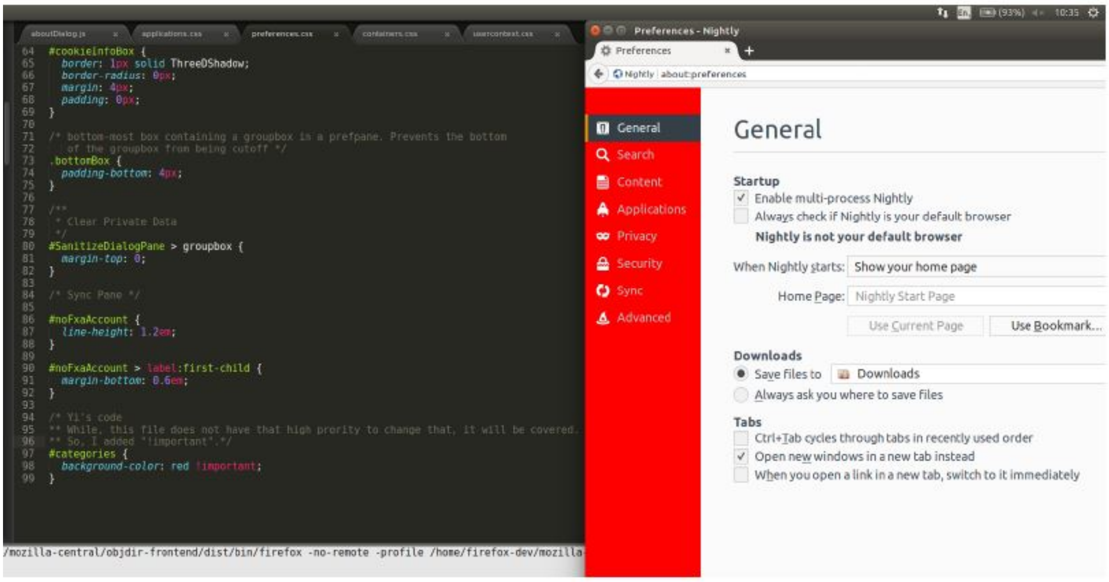
```

<hbox hidden="true" data-category="paneGeneral" flex="1" class="toolbarContainer">
<toolbar
  class="topSelector"
  hidden="true"
  flex="1">
  <toolbarbutton type="radio" group="xxx" label="General" checked="true"/>
  <toolbarbutton type="radio" group="xxx" label="Language and Appearance"/>
  <toolbarbutton type="radio" group="xxx" label="Files and Applications"/>
  <toolbarbutton type="radio" group="xxx" label="Nightly Updates"/>
  <toolbarbutton type="radio" group="xxx" label="Performance"/>
  <toolbarbutton type="radio" group="xxx" label="Browsing"/>
  <toolbarbutton type="radio" group="xxx" label="Network Proxy"/>
</toolbar>
</hbox>

<hbox id="generalCategory"
      class="subcategory part_general"
      hidden="true"
      data-category="paneGeneral">
      <label class="header-name" flex="1" data-l10n-id="pane-general-title"/>
</hbox>

<!--
<hbox id="myCategory"
      class="subcategory"
      hidden="false"
      data-category="myGeneral">
      <label class="header-name" flex="1" data-l10n-id="my-title"/>
</hbox>
-->
```

FIGURE G.2: Code snippets explored in the Mozilla build system VM



```css
#cookieInfoBox {
  border: 1px solid ThreeDShadow;
  border-radius: 0px;
  margin: 4px;
  padding: 0px;
}

/* bottom-most box containing a groupbox in a prefpane. Prevents the bottom
   of the groupbox from being cutoff */
.bottomBox {
  padding-bottom: 4px;
}

/**
 * Clear Private Data
 */
#SanitizeDialogPane > groupbox {
  margin-top: 0;
}

/* Sync Pane */

#noFxaAccount {
  line-height: 1.2em;
}

#noFxaAccount > label:first-child {
  margin-bottom: 0.6em;
}

/* Yi's code
** While, this file does not have that high prority to change that, it will be covered.
** So, I added "!important".*/
#categories {
  background-color: red !important;
}
```

```
/mozilla-central/objdir-frontend/dist/bin/firefox -no-remote -profile /home/firefox-dev/mozilla
```

General

Startup

☑ Enable multi-process Nightly

□ Always check if Nightly is your default browser

Nightly is not your default browser

When Nightly starts: Show your home page

Home Page: Nightly Start Page

Use Current Page | Use Bookmark...

Downloads

● Save files to Downloads

○ Always ask you where to save files

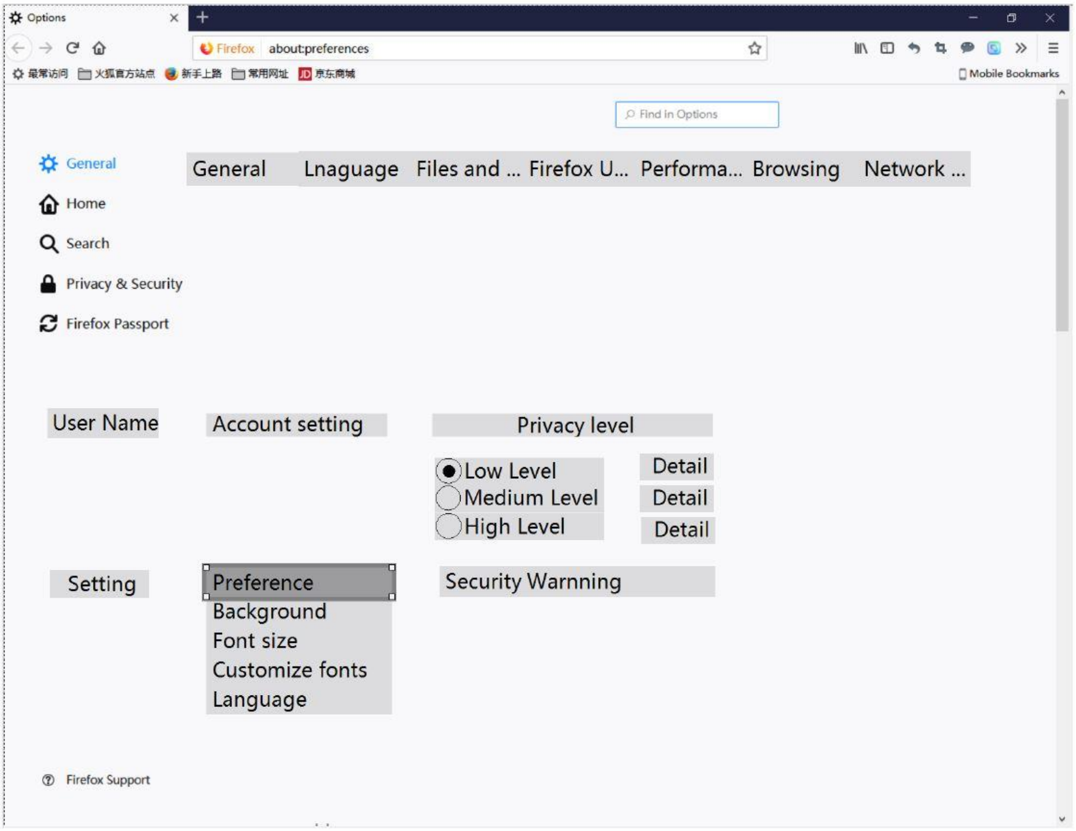
Tabs

□ Ctrl+Tab cycles through tabs in recently used order

☑ Open new windows in a new tab instead

□ When you open a link in a new tab, switch to it immediately

FIGURE G.3: Exploring the Firefox source code for high-fidelity prototype implementation



General | Lnaguage | Files and ... | Firefox U... | Performa... | Browsing | Network ...

User Name

Account setting

Privacy level

● Low Level — Detail

○ Medium Level — Detail

○ High Level — Detail

Setting

Preference

Background

Font size

Customize fonts

Language

Security Warnning

FIGURE G.4: An example implementation of initial designs using a pre-configured Mozilla build system VM

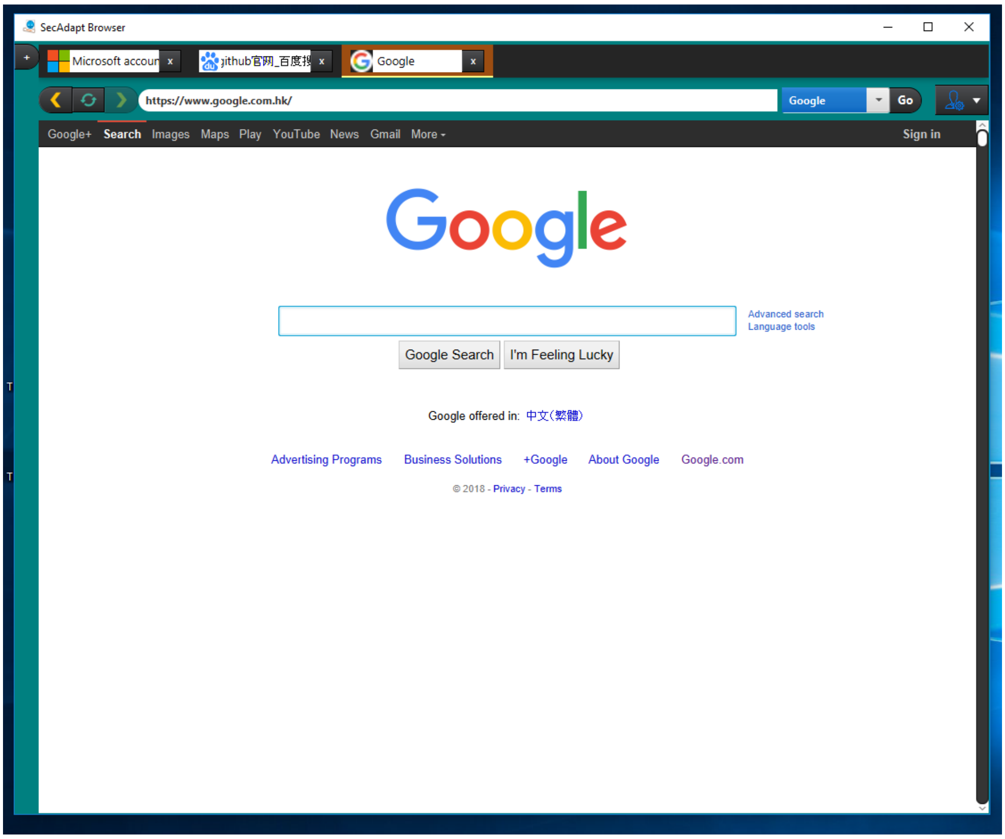
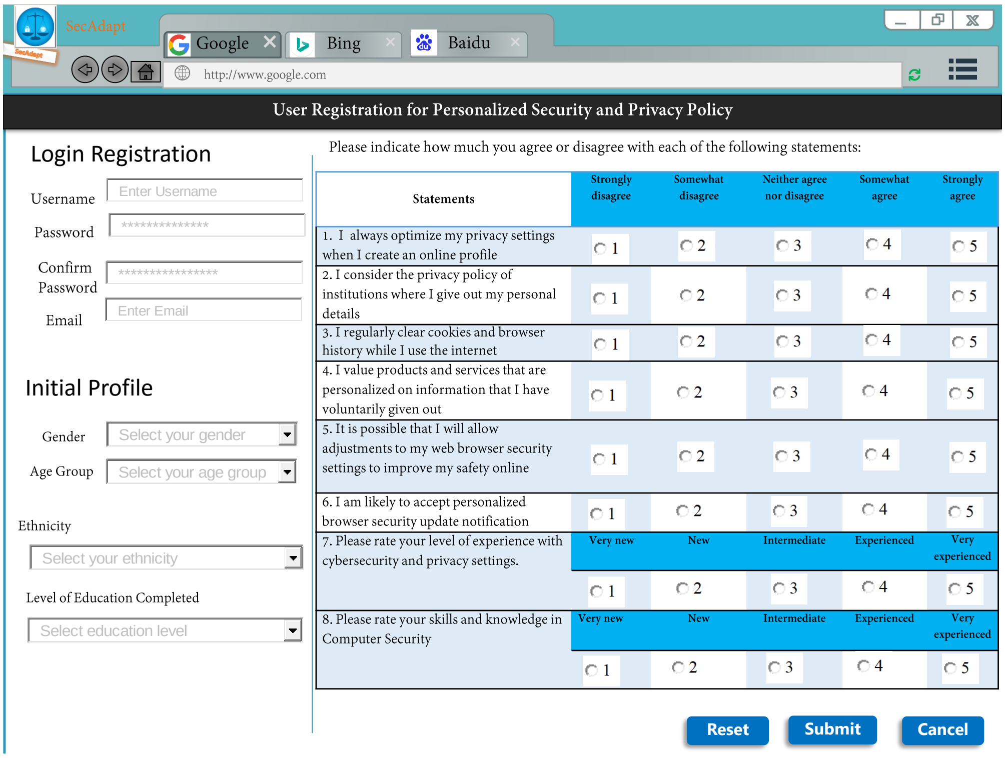

SecAdapt Browser
Microsoft accour
jithub官网_百度搜
Google
https://www.google.com.hk/
Google
Go
Google+ Search Images Maps Play YouTube News Gmail More
Sign in
Google
Advanced search
Language tools
Google Search
I'm Feeling Lucky
Google offered in: 中文(繁體)
Advertising Programs Business Solutions +Google About Google Google.com
© 2018 - Privacy - Terms

FIGURE G.5: browser implementation with JavaFX Scene Builder in NetBeans IDE to log participants browsing data for adaptation in SecAdapt V2



User Registration for Personalized Security and Privacy Policy

Login Registration

Username Enter Username

Password **************

Confirm Password ****************

Email Enter Email

Initial Profile

Gender Select your gender

Age Group Select your age group

Ethnicity Select your ethnicity

Level of Education Completed Select education level

Please indicate how much you agree or disagree with each of the following statements:

Statements	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
1. I always optimize my privacy settings when I create an online profile	○ 1	○ 2	○ 3	○ 4	○ 5
2. I consider the privacy policy of institutions where I give out my personal details	○ 1	○ 2	○ 3	○ 4	○ 5
3. I regularly clear cookies and browser history while I use the internet	○ 1	○ 2	○ 3	○ 4	○ 5
4. I value products and services that are personalized on information that I have voluntarily given out	○ 1	○ 2	○ 3	○ 4	○ 5
5. It is possible that I will allow adjustments to my web browser security settings to improve my safety online	○ 1	○ 2	○ 3	○ 4	○ 5
6. I am likely to accept personalized browser security update notification	○ 1	○ 2	○ 3	○ 4	○ 5
7. Please rate your level of experience with cybersecurity and privacy settings.	Very new	New	Intermediate	Experienced	Very experienced
	○ 1	○ 2	○ 3	○ 4	○ 5
8. Please rate your skills and knowledge in Computer Security	Very new	New	Intermediate	Experienced	Very experienced
	○ 1	○ 2	○ 3	○ 4	○ 5

FIGURE G.6: Registration interface in SecAdapt V2 Coded with VBA