FACTORS AFFECTING SECURE COMPUTER BEHAVIOUR

by
Matthew Hull

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF ARTS

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2015

Abstract

Understanding users' individual differences may provide clues to help identify computer users who are prone to act insecurely. We examine factors that impact users' reported security behaviour with respect to some common computer security issues. We conducted two online surveys with a total of 650 participants to investigate the relationship between self-reported security behaviour and users' knowledge, motivation, confidence, risk propensity, and sex-typed characteristics. We found that all of these factors had an impact on security behaviour; however, knowledge was the most important. We provide recommendations relating to understanding participants' individual differences as a way to identify users at risk of behaving in an insecure manner. Further, we suggest that deeper understanding of the relationships between personality characteristics and security behaviour can provide researchers with tools to more comprehensively interpret their data.

Acknowledgements

Foremost, I would like to express my gratitude to my supervisor, Dr. Sonia Chiasson. I count myself lucky to have had a supervisor that was always able to offer help, encouragement, and expertise at every stage of of the research process. Her ability to provide expert advice on my writing, précis my rambling sentences, and proofread what seemed like never-ending drafts, was second to none. For all of this—thank you.

I would like to thank the members of my committee: Dr. Robert Biddle, Dr. Alejandro Ramirez and Dr. Anil Somayaji for their time and constructive feedback.

Finally, I recognise that my studies would not have been possible without the financial assistance of Carleton University via teaching assistantships, research assistantships, and scholarships.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

The rapid growth of the internet has facilitated the development of many online businesses and services. For example, people use services to obtain information, communicate with others, shop online, and pay their bills. This growth, however, has provided a fertile environment for persons with malicious intent to take advantage of users that act in an insecure manner.

A recent white paper [22] noted phishing attacks alone were estimated as resulting in losses of $5.9 billion (USD) in one year, and were increasing. Further, malware inadvertently downloaded by users can often be used by malicious actors as a means to create Botnets used in Distributed Denial of Service (DDOS) attacks. DDOS attacks have been estimated to cost businesses an average of $40,000 per *hour* [48]. Understanding users' behaviour as it pertains to computer security is paramount in protecting against threats and enabling users to perform secure actions.

There is a growing body of literature that shows success in improving user security behaviours through improved design of systems [42] and education of users [55]. However, there is less research on examining the antecedents of security behaviour. Research has shown that users' security behaviour intention can be accounted for in part by their perceptions. For example, their perception of their ability to carry out a task adequately or their perception of the efficacy of using a protective measure [59]; both may impact their decision to act securely. However, these perceptions may change depending on other variables (e.g., the availability of resources [46]; user's assessment of risk). Sometimes these variables are tangible (e.g., money enabling someone to purchase security software) but sometimes they are not. For example, investigation into personal characteristics that are typically sex-typed, and their potential impact on users' perceptions and behaviour, may expose certain characteristics

as leading to adverse security behaviour.

1.2 Research question

There is a body of work implementing behavioural frameworks as a basis for predicting and modelling user security behaviour (e.g., Theory of Planned Behaviour [2], the Technology Acceptance Model [23], and Protection Motivation Theory [73]); however, whilst these models individually show relationships between behavioural antecedents and security outcomes, they often focus on different factors, or are conflicting in their findings [71]. As such, our current research focuses on amalgamating some of the main findings from the literature in order to understand which factors are relevant and show good predictive ability. Therefore, our research addresses the following question: *what personality characteristics and factors affect participants' security behaviour?*

1.3 Contribution

This thesis contributes the following results to the literature:

1. Our research shows the relative importance of factors that influence security behaviour. We investigate the impact of users' *knowledge*, *motivation*, *confidence*, *propensity to take risk*, and *sex-typed characteristics* (masculine and feminine), on their security behaviour.

2. Our research highlights the importance of understanding participants' individual differences when conducting security research. We argue that an assessment of these factors when conducting research enables a more comprehensive interpretation of data.

We accomplish this using a survey-based methodology. Our instrument was developed iteratively using existing literature and input from domain experts. It was administered to 650 participants across two studies. Results from statistical analyses show consistency between the two studies and align with previous findings, while clarifying the relationship between security behaviour and specific user characteristics.

1.4 Thesis outline

The rest of this thesis is laid out in the following way. Chapter 2 details the background research with respect to usable security and the main security issues that users face on a regular basis. We also examine some of the research into factors that may affect security behaviour. Finally we look at research into predictive models of security behaviour and discuss our preliminary study that was the catalyst for this work. Chapter 3 details the construction process for the instrument used in the two research studies within this thesis. Chapter 4 outlines the research methodology, results and summary of the first online study. Chapter 5 outlines the second study's methodology, results and summary. Chapter 6 provides a discussion and conclusion to this thesis.

Chapter 2

Background

2.1 Introduction

Computer security research has traditionally focused on the more technical aspects of securing systems, for example, improving intrusion detection, or providing enhanced encryption for data; however, more recently focus has been applied to the human aspect of computer security and, specifically, making security more usable for the end-user. There is a tension between security and usability of systems such that an increase in one of these factors tends to instigate a measured decrease in the other. Often, ensuring good usability of security protocols is neglected in favour of enhanced technical security. As a result of these security increases there tends to be a provision of complex procedures that users need to follow to ensure that the system is being properly implemented. Usable security research moves toward understanding how user-centred design practice and efficient communication can positively impact computer security systems [1].

2.2 Overview of usable security issues

User interfaces are a potential battleground for security research—good interfaces may promote security, whilst bad ones inhibit it. Whitten and Tygar [91] describe in their, now seminal, paper, *Why Johnny Can't Encrypt*, five main properties of designing user interfaces for security systems:

The unmotivated user property: This property describes how users do not make security their primary goal, they are more interested, for example, in downloading music or watching shows online. Security is a secondary motivation that users expect, most of the time, to already be in place.

The abstraction property: Rules governing security behaviour and compliance are often too abstract for users to fully comprehend. Designers should account for these abstractions and ensure that communication of intentions/outcomes are logical and intuitive.

The lack of feedback property: Providing feedback to users so that they understand the state of a system is imperative; however, it is fundamentally difficult to provide meaningful feedback with security systems as they are often extremely complex. Furthermore, systems must not reveal information that could help attackers.

The barn door property: This property describes how, if there is a possibility that information is accidentally left unprotected, there is often no way to tell for sure if it has been viewed by an unauthorised person. The recommendation is that security systems should adequately detail the state of a system so that mistakes, such as security lapses, can be prevented.

The weakest link property: Any security measure is only as strong as the weakest link. Often even if a security protocol is secure, it still may rely on some user participation, such that, if a user does not know how to adequately secure a system, they may leave themselves open for attack.

Whitten and Tygar's [91] properties of designing interfaces highlight that security design needs to be adaptable to the human element. Without prior thought into how users will communicate with, and understand a system, system designers fail users by their inability to take into account users' needs. Part of designing for the human element in a system is being cognisant that no matter how secure a system is, they often require human input to be able to function correctly (e.g., updating anti-virus software).

Schneier [13] notes that, "...security is only as good as its weakest link, and people are the weakest link in the chain." Users are susceptible to attacks because they are required to make security related decisions based on a series of complex evaluations and judgements. Quite often this security calculus is based on limited knowledge and understanding of the potential threats. Users often also think of security as a

secondary task; something to complete only if they have the time or inclination whilst completing their primary task [91]. For example, when a user logs into a website and is required to authenticate, the user is thinking about what they will do once they have been logged in, not the process of logging in.

Techniques that support the user are proposed by Adams and Sasse [1]. The authors posit that service providers should stop thinking of users as the enemy and instead start understanding why users are prone to act in an insecure manner. They highlight the following points that are detrimental to users' ability to act in a secure way: users often lack the knowledge to be able to make secure decisions; security interface design needs to be more user-centred; and users need to be sufficiently motivated to want to carry out secure behavioural practices. The authors' recommendations are in line with Whitten and Tygar's [91], such that, they promote designing security systems holistically and understanding that, although users may often be the *weakest link*, there are ways to support the user so that this is not always the case. In the following subsections we discuss some of the main causes of insecure behaviour among end-users.

2.3 Compliance

Even when properly conceived interfaces are designed, there is often no guarantee that users will be compliant. Generally speaking, most people subconsciously abide by the *principle of least effort* [95], that is they try to strike a balance between the costs of completing an action and the benefits of completing an action. This cost-benefit analysis means that people try to accrue the largest gains with the smallest amount of effort. With regard to computer security compliance, security often only becomes a viable option for the user if the effort required to enable security functions is below the limiting threshold. This subconscious evaluation can often lead to users making inadequate security decisions or circumventing security altogether. For example, when password composition policies are implemented that are overly complex, users tend to adopt strategies that reduce the efficacy of the security protocol [75]. These strategies include re-using passwords across different systems and websites [31, 50], or writing down their passwords [1].

That is not to say that password policies are completely ineffective, for example, when password policies are more relaxed, users often make insecure password choices such as making obvious, easy to remember passwords. Although a major security concern at the time, corporate password security breaches do provide researchers with an invaluable insight into the mind of the user and, specifically, their password creation strategies. A 2013 data breach of Adobe Systems (in conjunction with poor encryption) lead to the release of the 'Top 100 Adobe Passwords with Count' by the Stricture Group [43]. They note that 1,911,938 accounts used the password '123456' and 345,834 accounts used the password 'password'. The users that created these passwords are a good example of expending the *least effort* when the opportunity arises. Thus, it seems like a balance needs to be found between overly excessive and overly lax measures; users need to be supported in a fashion that makes them more willing to comply. Von Solms and Von Solms [88] further argue the case for supporting the user. The authors note that having defined company policies does not necessarily mean that employees will obey them, instead companies have to create a culture that surrounds these policies making the social norm within the company to behave in a secure manner.

Understanding why users act in the way that they do is important for researchers and organisations; however, the reasons are often complex. Herath and Rao [46] conducted a study investigating employee security policy compliance behaviour. They surveyed 312 employees from 78 different organisations in the United States. Their results highlight three main themes that affect users' security behaviour outcomes:

Perceptions: Users' perceptions regarding the potential severity of a threat was found to be significantly related to users' concerns, which were in turn related to security policy attitude. They also found that the perceived cost of responding to a security issue motivated users to behave more securely. Further, resource availability was positively associated with feelings of self-efficacy: the more resources that were available to enable users to comply with security policies, the more users felt equipped to execute these policies. Conversely, if security policies were perceived to be interfering with the efficacy of their work, then users would be more likely to try and circumvent security protocols.

Intent to comply: Results indicated that both response-efficacy and self-efficacy (moderated by resource availability) had a significant effect on the intentions of users to comply with security policies. Further, the authors found that social factors also moderated social compliance, such that, users were influenced both by the expectation of others to comply to security policies, as well as by the behaviour of others complying to security policies.

Organisational commitment: The authors found that organisational commitment affected response-efficacy and compliance intention. That is, the more a user felt committed to their organisation, the more that they felt that their actions would be effective. Further, those more committed individuals were more likely to comply with security policies.

Herath and Rao's [46] research highlights the complexity of user behaviour. Understanding these behaviours is necessary in combating user non-compliance. The downstream effect of these insecure user behaviours can often have consequences more far-reaching than the user initially understands. For example, research by the Ponemon Institute [49] [1] estimates that around 30% of root causes of data breaches can be attributed to negligent human causes and estimates the cost of these human related errors at $117 per capita, per annum.

2.4 Cost-benefit ratio

Users' attitudes toward security behaviour often involve users making judgements as to the cost and benefits of employing security measures. Research investigating user incentives to take more risk online was conducted by Christin *et al.* [19]. In their research, the authors found that by paying participants, they were able to make them ignore security advice. Their results show that 59.4% of participants would run an unknown program on their machine for 60 minutes for the payment of $0.01 (USD). When this amount was raised to $1.00 (USD), 82.3% of participants ran the code for one hour, even though 70% of the participants knew that this was contrary to

[1] This is the ninth annual survey by the Ponemon Institute and it aggregates responses from over 250 organisations in 11 countries.

recommended security advice. These results indicate that users are willing to make what seem like irrational security decisions for very little benefit. One of the reasons that the users in this study may have made these decisions was because they saw the initial costs (e.g., cost of action rather than the potential cost if something went wrong) to be minimal (all the users had to do was run a program in the background on the computer).

Beautement *et al.* [10] looked the cost/benefit ratio in more depth. The authors investigated how users balance perceived costs and benefits to making security compliant decisions, in what they term a *compliance budget*. They find that participants weigh potential costs of compliant behaviour (e.g., increased physical load; missed opportunities) against the potential benefits of the behaviour (e.g., avoiding security breaches, being protected from company sanctions) when making security decisions. The authors recommend that by targeting users' compliance budget directly, it is possible to increase overall compliant behaviour. For example, ensuring that users know that their compliance is being monitored can increase the potential threat of sanctions, thus increasing compliance. This balancing act can also be seen in Albrechtsen [3], such that, when users are required to increase the amount of effort they expend on information security, this can often come at the price of efficiency and usability in other areas of their working roles. These results echo those of Adams and Sasse [1] insomuch as: knowledge, a balance between usability and security, and adequate motivation, are areas in which changes can have the most impact on users' decisions to act securely or not.

Herley [47] emphasises the role of cost/benefit analysis, arguing that users make an economic judgement call when assessing security advice and often this lands on the side of rejecting the advice in favour of reduced overhead. The author notes that users understand their own assets and are in a better position to make judgement calls about risk than security professionals and, further, much of the time asset value is assigned by the user. Obviously this is not always the case, there are times where there will be an actual tangible value associated with something (e.g., bank funds), but in the case where value is not tangible (e.g., photo sharing websites), users may be much more willing to forgo robust security in order to achieve a lowered overhead.

2.5 Willingness to take risks

In a reflection of the non-digital world, users are required to make risk-assessments when they are navigating online spaces. Research by Lacohee *et al.* [56] investigated the ways in which users made such risk assessments. The authors found that trust had less of a role to play in mediating users' behaviour online than the perceived risks involved in carrying out certain objectives. Specifically, users relied on their own past experience, intuition, and the experiences of others to guide their decision-making process. Further, users were more likely to take risks when they had more of an assurance that, if something did go awry, they would not be impacted too severely (e.g., purchasing from a potential dubious website knowing that, by using a credit card, they would be protected should something happen).

A study by Garg and Camp [39] found that the severity of the consequences of online risk taking behaviour was the most important factor in users' decisions. The authors investigated which risk characteristics were the most important within five different mental models of risk communication (medical, criminal, physical, warfare, economic, miscellaneous) used by the security industry. They found that, across all of the mental models, *dread* characteristics (rare and catastrophic events) of a threat were the biggest driver of risk perception, such that, the more that dread characteristics were highlighted, the greater the perceived risk. The authors also found characteristics that were drivers of risk perception specific to certain mental models. For example, aspects of control, within the medical model, were also related to risk perception. As a result, the authors recommend that when communicating risk, it may be possible to combine related aspects to increase overall impact. Ng *et al.* [67] find similar results in their work—the authors' research into the Health Belief Model of security behaviour also found that perceived severity is the biggest influence on security behaviour.

To complicate matters, Van der Pligt [85] argues that people often struggle with their inability to fully assess the magnitude, as well as the likelihood, of potential risks. For example, sensationalised risks may be thought of as much more likely to happen even though, in reality, such a risk only poses a threat to the minority. Such inability to fully assess the risks associated with certain behaviours (or lack of), poses a real

threat to users' computer security. Not only is there the potential to inadequately assess the threat, there is also the potential that users' may not have the required knowledge of the threat, or feel sufficiently empowered, to be able to employ relevant preventative measures. Work by Byrne *et al.* [14] indicates that by increasing users' knowledge of potential risks, users are able to better assess the extent of the potential risk, severity and cost.

2.5.1 Risk mitigation software

To combat the prevalence of insecure user behaviour, an industry has grown to develop software solutions to problems faced by users. For example, password managers such as Lastpass[2] help reduce the cognitive burden placed on users when required to remember many complex passwords. Further, users employ other software, such as: anti-virus software, software to scan computers for malware, browser extensions to warn against phishing websites. These solutions are offered to the user as a means to go about their business in a secure manner without expending too much effort. However, usability issues with many of these systems mean that the expected security benefits do not occur [18, 91]. Having so many automated security measures may be reducing users' ability to assess security risks themselves (i.e., they think that they are immune to threats as they have appropriate protective software installed, when in reality, they are still compromising their own, and others' security). Furnell [35] argues that often, users may be proactive in their use of security measures (e.g., downloading and using free security software) but fail to understand to what extent, or against what threats, the software will protect them. Further, with security measures such as firewalls, users may be vaguely aware of their need but do not understand what the measures do or what they protect against.

In addition to users incorrectly understanding what their software is protecting them against, there is also the possibility that even when they are alerted to danger they do not react appropriately. Users often ignore alerts and signs from their computer if they receive them on a continuous basis, in essence they get fatigued and

[2]https://lastpass.com/

learn to screen them out [41]. In other instances, users do not fully understand warning signs. For example, cues within their browser [24] that would alert them to the illegitimacy of the website that they are visiting, thus opening them up to potential danger.

2.6 Mental models

When users interact with technology, they form mental models of the systems they are using. These models evolve so as to help users explain and predict system behaviour. Sometimes these mental models are correct and improve a user's ability to comprehend and use a system; however, sometimes they are incorrect and may lead to improper use of a system.

In a study by Camp *et al.* [15], the authors investigated how security experts and non-experts assigned terms associated with computer security behaviour (e.g., 'worm', 'lock', 'firewall') to different mental models (e.g., medical infections, criminal behaviour). The authors found that there were certain terms that participants struggled to classify, that is, they could not place the term within an existing mental model. Further, they also found fundamental differences in the categorisation of terms between the experts and the non-experts. These results highlight that, in order to properly convey security communication, it is first necessary to understand what mental models system users have so that communications can be correctly targeted in order to have the greatest impact.

To understand how users come to acquire their mental models of security, Wash [89] looked at home users' perceptions of threats through the lens of 'folk models'. In his research, Wash conducted interviews with participants and asked them about their knowledge of security threats and the types of protective measures available to them. Following this, he asked participants how they would act when presented with certain security related scenarios. Wash found four 'folk models' in play with regard to malicious software: *bad*—these participants did not have a thorough understanding of malicious software and, as a consequence, could only view such software as having bad outcomes; *buggy software*—these participants were under the impression that the malicious software was regular software that had a number of bugs; *mischief*—the

participants understood that the malicious software was purposefully created by a malicious actor and that the consequences would be more in line with the annoyance of the buggy software rather than the criminal intent of the following crime model; *crime*—the participants understood that malicious software mostly had a criminal element to it (i.e., it was intended to harvest personal information with the intent to be used for criminal purposes). The results, Wash argues, show that there are wide ranging beliefs with regard to: the effects of malicious software, the conduit for transmission of this software onto the end users' system, and the reasons and intent for the implementation of the malicious software. In short, many users have incorrect or poorly implemented mental models of security systems and threat vectors, further, these poor models can be attributed in part to poor (or a lack of) education.

2.7 User characteristics

Every person is unique and, by extension, every user has a unique set of personality characteristics and traits that have the potential to affect their security behaviour. Analysis of the role of *self-efficacy* is investigated by Milne *et al.* [65]. The authors find that users' feelings of self-efficacy (their perceived confidence in their own abilities), in regard to safe and secure navigation of the web, had a strong relationship to their actual exhibition of behaviours of a protective nature. Further, they find that the perceived likelihood of a threat had a strong relationship with users' undertaking of protective behaviours, whilst perception of the threat by itself (without a clear perception of the likelihood that it would arise) resulted in users exhibiting insecure behaviours. These results indicate that to properly motivate users to undertake protective behaviours, one must first educate them so that they feel confident in their abilities to combat the threat, as well as providing information so that they can accurately assess their own susceptibility to the threat. It seems that perception of the existence of the threat alone is not enough to motivate the user into seeking out, or undertaking, protective behavioural measures.

Even educated, well intentioned users may not follow through and behave securely in a real world setting. Shropshire *et al.* [77] investigated personality constructs that

may moderate the relationship between users' initial intentions and their actual computer security behaviours. Participants' personality traits, *conscientiousness* and *agreeableness*, were found to moderate the relationship between users' intention to act securely, and their actual behaviour. Users displaying greater level of conscientiousness were more likely to follow through with their intention to act securely and users displaying greater levels of agreeableness also were found to be more likely to follow through on their initial intent to act securely. This study highlights two important points. First, personality traits are an important consideration when thinking about technology use and, specifically, the adoption and use of security technology. Second, behavioural intention may not be a good predictor of actual behaviour by itself, it needs to be viewed within a network of dynamic related factors.

Further work investigating the impact of personality traits on security behaviour was conducted by Gabriel *et al.* [38]. They investigated correlations between personality traits and security behaviour. Their research found that *imagination*, along with *emotionality*, *anxiety*, and *altruism*, had the highest positive correlations with security behaviour. Further, *immoderation* (defined by the authors as acting in the interest of short-term gains rather than long-term consequences) and *excitement seeking* had the strongest negative correlation with security behaviour.

If personality traits have an impact on secure behaviour, it is important for researchers to understand this so that they can take these factors into account; however, there may not much that can be done to change certain traits in a way that is beneficial in improving users' security behaviour. For example, one may be able to facilitate a change in a user's mental model through education, but not be able to change a user's propensity to take risk. It is important to gain insight into the immutable characteristics, as well as the changeable, so that they can be taken into account. As an example, research suggests that females may be more susceptible to certain computer security threats, such as phishing [51, 76], than males; however these findings are in the minority. Most security research finds that there are no significant differences in between sexes with regard to security behaviour [57, 65]. Understanding how factors such as these *may* impact users' security behaviour enables researchers to account for them in the design of experiments (e.g., by asking relevant information about the

characteristics being measured), as well as enabling the correct interpretation of data post-collection.

2.7.1 Population segments

We have reviewed research looking at users' individual differences (the micro level); however, work has also been carried out to understand how different sections of the population differ in their security behaviours (the macro level). Friedman *et al.* [33] investigated how risk perceptions can differ between communities. They set out to compare users' understanding of the risks and harms associated with web use with respect to three different types of communities: rural, suburban, and high-tech. They noted that the communities differed in their concerns about web risks. The suburban and high-tech communities had definite concerns, whereas 21% of the rural community had no concerns at all. The participants' levels of concern from the three communities were the same in regard to information security and information privacy. However, whilst all three communities were, in general, most concerned about risk and harm in regard to information, the issues with the highest percentage of concerned participants differed across groups. Although in reality these types of communities may not be mutually exclusive (e.g., a web designer may work from home and live in rural community), the study does highlight that different communities may have different concerns regarding security, and thus different thoughts regarding costs, benefits, and associated risks.

In a qualitative study, Furnell *et al.* [37] interviewed twenty novice IT users and found that many users were not interested or motivated to protect themselves against potential threats, even though they were aware of the threat. The authors argue that there are two potential ways to combat this apathy, empowering users to take responsibility for their own (and others') security would help improve behaviour; however, research by Lalonde Levesque *et al.* [57] indicates that even when users have the knowledge to be secure (and are arguably empowered), they do not always follow good security practices. The authors found that the users that they classified as 'expert' were twice as likely to be in the high risk category.

2.7.2 User motivation

Protection Motivation Theory was originally proposed by Rogers [73]. This theory posits that a person will assess a threat based on their own perception of how susceptible they are to a threat, how severe the threat is, and the likelihood that the threat will occur. Rogers argues that once the threat has been assessed, a mental calculus comes into play to evaluate both the perceived efficacy of the threat response, as well as the person's self-efficacy in completing the required response. Protection Motivation Theory is widely regarded as good framework for predicting protective behaviours [32].

With regard to users' personal motivation for enacting secure behaviours, it seems that most understand their role in the protection process, and possess the basic information to assess threats. A study by Furnell [34] found that 90% of home computer users felt responsible for the security of their personal computer systems; a follow-up study found similar results [79]. In Furnell's study, over 98% of participants understood basic security terminology (e.g., computer virus, hacker). This understanding (or at least claimed understanding) is a core premise for users to adequately assess the type of threat using the Protection Motivation Theory. One caveat to the successful outcome of users' threat evaluations is that much of the user's evaluation is made using their own knowledge of the threat (e.g., perceived severity, perceived susceptibility) and, as previously discussed, there are many ways for this knowledge to be inadequate (e.g., incorrect mental models). For example, there could be a disparity in users' perceptions of severity, such that, they make risk evaluations based on the less severe premise of 'buggy software' rather than, the potential risk that the malware may be keylogging software. Other personal motivations may be simply related to users' perceptions; Shropshire *et al.* [77] found that user perceptions with regard to the ease of use of a security system, as well as the usefulness of the system as a whole, were positively related to users' intention to act in a secure way—these factors would directly relate to the *efficacy of threat response* outlined in Rogers' [73] Protection Motivation Theory.

Although there is an obvious personal motivation component to security behaviour, there may also be a prosocial motivation. Altruism has been associated

with secure computer behaviours [38]. Protection Motivation Theory can also be used as a framework to account for social aspects of behaviour [80], such that, pressure to be socially responsible can impact users' cost/benefit analysis even though the benefit, in these cases, may not be directly to the users themselves. Anderson and Argawal [5] argue that this is the indeed the case. They use the example of a user not wanting to spread a virus via email to friends. Even though this may seem altruistic, it may be motivated more by self-interested reasons, such as what others think of them or and a potential loss of social standing.

Although understanding the reasons that users act insecurely seems complicated—the many interlinking factors often being highly related and non-static—they do provide a basis for understanding how to improve users' security behaviour. Some factors, (e.g., conscientiousness) may not be easily changed; however, other factors may be manipulated so that users become more compliant. Often, fear and threat of sanctions is used as a means of user compliance control [17].

Motivation by fear, however, is not always the best approach. LaRose *et al.* [59], look at how users are empowered to take responsibility for their own security actions. They argue that one tool normally employed to enforce compliance is that of threat. Threat appraisal on the individual level is an assessment by the user about the severity and susceptibility of a particular threat. Using fear as a motivator can have unintended effects—sometimes moderate levels of fear can produce the highest levels of secure behaviour whilst low and high levels of fear can inhibit protective behaviour. However, they also found that for some users, moderate levels of fear produced the least action toward secure behaviour while high and low levels of fear produced more secure behaviour. The authors argue that without knowing how the individual perceives the threat level, it is not possible to say whether the fear will induce or inhibit secure behaviour.

Of the factors mediating users' security behaviour, LaRose *et al.* [59] find that a sense of *personal responsibility*, *self-efficacy* and *response-efficacy* (belief in the technology/safety measures' ability to combat the perceived threat) have the most noticeable impact on a person's online security behaviour. They argue that fear messages should include details of how to combat the issues, thus raising levels of

self-efficacy and, in situations where users have high levels of self-efficacy, it will be the perceived response-efficacy that mediates their course of action.

2.8 Improving end-user security behaviour

One way to improve the security behaviour of users is to improve their confidence in themselves to be able to ensure their own protection. Rhee *et al.* [72] investigated factors affecting users' self-efficacy with regard to information security (a factor we have already discussed as being closely related to behaviour in section 2.3 [46, 59]). Their results highlight three aspects that impact a users' feelings of self efficacy: computer experience, security breach incidents, and general controllability. Further, the authors found that users with greater feelings of self-efficacy were more likely to engage in secure behaviours (e.g., checking to see if websites they visit are encrypted; using strong passwords). Their research mirrors previous findings on self-efficacy and security behaviours, but it adds new information in regard to the factors affecting self-efficacy itself. In section 2.3 we discussed the effect of resource availability on users' self-efficacy [46]; however, this research indicates that multiple factors affect self-efficacy, which in turn may have an impact on security behaviours.

2.8.1 Reward

Using reward to change behaviour is not something novel. In section 2.4, we discussed the possibility of changing user behaviour for the worse [19]; Chen *et al.* [17] instead investigated reward as a way to entice users to act securely. The authors investigated how punishment, reward, and certainty of control (in this case certainty of control means how certain the user was that the reward or punishment would actually happen) affect compliance. They found significant effects of all three of factors on compliance intention. Further, they found that reward only made a significant difference in compliance when there was a low punishment environment; reward did not moderate compliance when there was a threat of severe punishment for non-compliance. Their results lend support to the view that in many situations, non-compliance is controlled with punishment; however, they show that this does not necessarily need to be the case. It may be more beneficial to use reward as a mechanism to increase security

compliance intention.

2.8.2 Design

Whitten and Tygar [91] highlighted that interface design was an important property in computer security systems than involve user participation. Their reasoning was that good design can communicate information to a user in a way that enables the user to make informed and correct decisions about the state of the system, how the system is structured, and their own security. Grimes *et al.* [42] investigate design from a different angle. Using the Theory of Planned Behaviour [2] framework (section 2.9 provides an overview), the authors argue that the appeal of a website and users' trust in a website moderate users' subjective norms regarding security behaviour. These subjective norms will affect their intention and thus their overall security behaviour. The authors found that, when interacting with a website that had a high appeal, users were more likely to create higher entropy passwords than when they interacted with a low appeal website. Their work highlights the possibility that influencing security behaviour passively, and in a way that does not place an extra burden on the user (e.g., requiring the training sessions), may be an option in conjunction with other compliance controls.

2.8.3 Collaboration

Albrechtsen and Hovden [4] explored employee engagement through small information security workshops. The workshops involved: discussion, reflection, a short cartoon that introduced participants to the basic concepts of information security, group work, and a final discussion. Quantitative and qualitative data was collected longitudinally by the researchers and found that the workshop interventions had a significant impact on users' awareness and behaviour in regard to information security. When asked about the reasons for their changes in behaviour, over 80% of the participants named the workshop as the cause of the behavioural change. The results indicate that the participatory nature of the workshops improved dialogue, understanding of procedures, and understanding of motivations. This positive participation in the information security dialogue may enable more secure behaviour

compliance in corporate environments where policy, although dictated, may be rationalised through collective reflection and discussion by employees. It is not difficult to imagine their results being applicable outside of the organisational setting; for example, security software for the home user often has associated help and chat forums as a means for users to connect with each other and discuss potential issues regarding the specific software. Increasing user participation in these forums (as long as they are moderated appropriately so that correct information is being disseminated) could potentially result in changed user behaviour.

2.8.4 Education

Educating users so that they are aware of when they are behaving insecurely is imperative to improving security behaviour outcomes. Further, ensuring that users harbour the correct mental model of a system is an important factor in ensuring compliant behaviour. Zhang-Kennedy *et al.* [94] found that by educating users through infographic posters and an interactive web-comic, they were able to foster a deeper comprehension of security threats—in this case password attacks. Further, the participants reported real life behavioural changes in the days following the session. Similar success in training users was found by Kumaraguru *et al.* [55]. Their research investigated the efficacy of online training materials relating to phishing threats. The authors found that users who were provided with the material were better at identifying phishing websites than the control group.

If educating users is to be effective in the long run then it is important for users to obtain correct and useful information. Furnell *et al.* [34] found that respondents were most likely to obtain their security advice from informal sources, such as friends or family—increasing the chance of propagating misinformation. However, 43% of participants also indicated that they had visited websites dedicated to promoting internet safety and computer security measures in an attempt to educate themselves. Problematically though, in a follow up question, participants indicated that the information provided by these types of websites were of no use to them. The authors argue that providing security information to users at the time of purchase would greatly influence a user's perceptions about security; however, they note that this is

not common practice. We see similar results in Aytes and Connolloy [7], such that, the authors note that 93% of participants self-reported that they were *knowledgeable* or *expert* in their understanding of email and 69% of participants stated that they were *knowledgeable* or *expert* in their understanding of protecting their computer. Yet similar to Furnell *et al.* [34], a considerable percentage of these users are getting their information from friends or colleagues (52%), and only a few respondents received any security training (19%).

2.9 Modelling security behaviour

With an understanding of the types factors that potentially drive users' decisions with regard to security behaviour, there has been active research into creating predictive models of security behaviour; these models are generally based on theories regarding how users' accept technology. The two dominant theoretical frameworks regarding technology acceptance are the Theory of Planned Behaviour [2] and the Technology Acceptance Model [23].

2.9.1 Foundational models

The *Theory of Planned Behaviour*, in its simplest form, argues that a person's behaviour is mediated by their prior intention to perform the behaviour. Their intention is determined by three factors: *attitude*—this is the evaluation by the user as to whether the behaviour is of benefit to them; *subjective norm*—this consists of how normal or abnormal the behaviour is according to the users' perceptions within their social frame of reference; *perceived behavioural control*—this constitutes both the perception of how easy it is to perform the behaviour as well as the perceived sense of control over the behaviour. Research findings have been mixed in their validation of the Theory of Planned Behaviour—while some researchers have indicated that these relationships exist [87], others have not found the same relationships [71]. To further complicate the model, researchers have argued that the sense of how easy a behaviour is, and the control that a user believes they have over the behaviour (together evaluated as *perceived behavioural control*), should in fact be separate factors as they are themselves moderated by intrinsic and extrinsic factors respectively [71].

The *Technology Acceptance Model* builds on the Theory of Planned Behaviour by positing that technology acceptance is mediated by perceptions of a technology's *ease of use* as well as its *usefulness*. The Technology Acceptance model was developed, in part, due to variations in the successful validation of the Theory of Planned Behaviour model; that is, the *subjective norm* did not seem to be a consistent determining factor of behavioural intention [71]. Further, validation of *attitude* as a determinant of behavioural intention was also mixed [86], thus leaving a streamlined model that proposes perceived ease of use and perceived usefulness as antecedents of perceived behavioural control and of the relationship between perceived behavioural control and behavioural intention [87].

2.9.2 Technology awareness

Dinev and Hu [25] construct a model that investigates the antecedents of factors within the Theory of Planned Behaviour. They find that *Technology Awareness* is directly related to behavioural intention, subjective norms, and attitude and thus, is a key determinant in establishing whether an end-user will accept a technology. The authors find differences in the adoption of, *protective* technologies (e.g., anti-spyware, anti-virus software) when compared to other *positive*[3] technologies, for example, video editing software. They argue that the threat of exposure to malicious behaviour is a greater driving force in adoption rates of protective technologies, than either perceived ease of use, or perceived usefulness. It is the concept of *threat awareness* that they argue is the main determinant of behavioural intention when looking specifically at protective technologies.

2.9.3 Perceptions and norms

We discussed how behavioural intention may be moderated by aspects such as self-efficacy and subjective norms [46]. Ng *et al.* [67] explore the problem of modelling user acceptance and use of protective technologies further. They argue that technology acceptance models such as Theory of Planned Behaviour and Technology Acceptance

[3]The authors use the term positive technology so as to make a distinction from, so called, *negative* technologies, such as malware.

Model, although robust to a certain degree, fail to accurately take into account the nuances of behavioural determinants *specific* to security behaviour.

Ng *et al.* [67] look to *Protection Motivation Theory* [73] and, in particular, an adaptation of the *Health Belief Model* [74] as a basis for modelling user behaviour within this specific problem space. Briefly, Protection Motivation Theory suggests that users will assess threats depending on their perceived susceptibility, perceived severity, and likelihood of occurrence; the Health Belief Model suggests that ones' understanding of health problems, the perceived benefits, the perceived costs and barriers, and feelings of self-efficacy all impact decisions to take measure to improve health outcomes. They find three major determinants of a user's computer security behaviour: perceived susceptibility, perceived benefits, and self-efficacy.

Ng & Mohammad [68] attempt to model end-user security behaviour from a socio-behavioural perspective. They use a modified version of the Theory of Planned Behaviour, in this case the *Decomposed Theory of Planned Behaviour*[4] [81]. Their results indicate that attitude and subjective norms have a significant positive relationship with behavioural intention; however, perceived behavioural control was not consistent. Further, perceived usefulness of security behaviour was found to have a positive relationship with security attitudes. The researchers also found that family, peer and media influence had a strong influence on a user's subjective norms regarding security behaviour.

2.9.4 Risk modelling

Aytes and Conolly [8] explore risk and computer security compliance behaviour. They construct a model of users' behaviour to understand why users engage in risky computer security practices. Their model combines extrinsic and intrinsic factors as antecedents of behaviour and specifically takes into account users' perceptions of risk—Figure 2.1 details this model. They argue that although these perceptions may be flawed in their assessment of the *actual* risks involved, they play an important part in the decision-making process. Aytes and Conolly break down their model into four

[4]this model proposes the full decomposition of attitude, subjective norm, and perceived behavioural control to account for their respective antecedents.

main components:

Information Sources: These are information conduits that users tap to educate themselves (actively or passively) in regard to security measures (e.g., media, friends and family, past personal experiences).

User's Knowledge: Fed into by *information sources*, this part of the model constitutes what users actually know about the threat(s) and the countermeasures (e.g., the time/cost taken to deploy the countermeasure, how the threat could affect other people).

User's Perception: Fed by the user's knowledge, this is the part of the model where users are making an assessment of the threat, their ability to protect themselves and others from it and the cost/benefit analysis of protecting against the threat (e.g., assessing the probability and magnitude of negative consequences).

Behavioural Choice & Outcome: Users' perceptions and general disposition to engage in risk taking behaviour are, according to Aytes and Conolly's model, the two main precedents of a user's choice to either engage in preventative measures or risky behaviours. The final part of their model is the feedback loop from the behavioural choice into the user's *information sources*.

2.9.5 Coping with threat

Liang & Xue [60] investigate how users cope with IT threats and create a model using the *Technology Threat Avoidance Model* (TTAT). In its simplest form, the TTAT states that when a user encounters a threat, they will undertake a safeguarding measure if they think the measure can ameliorate the threat. They also posit that users may 'avoid' the threat by using emotion-focused coping. Their results indicate that if users are clearly made aware of a threat and are able to make a threat appraisal and a coping appraisal, they will be more motivated to exhibit secure computer behaviour. If a user fails to see a threat, or sees it but believes it to be unavoidable, they will not be motivated to take precautionary measures. To make a threat appraisal, users need to be aware of the severity and susceptibility of the threat. To perform a coping

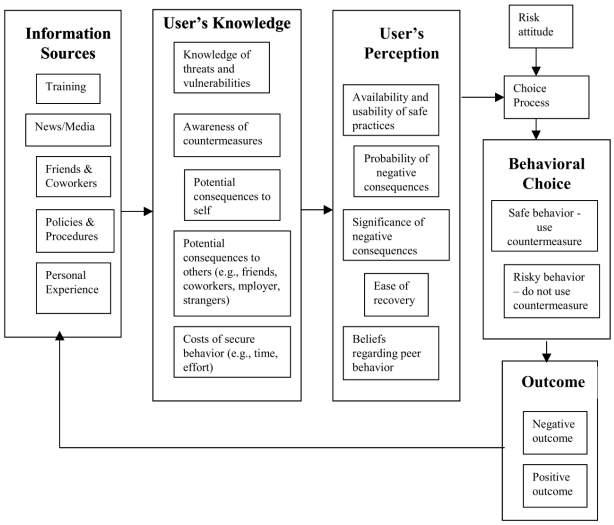


Figure 2.1: Aytes and Conolly's security behaviour model [8]

appraisal, users require information on the effectiveness of protective behaviour, the cost of implementation, and their confidence in correctly implementing the measure. Interestingly, the authors found a negative relationship between the perceived threat and the effectiveness of the safeguard. They argue that users may feel less fear of a potential threat if they feel that the measures that they have in place are particularly effective.

2.10 Assessing end-user security behaviour

Assessing end-user security behaviour is complex. Observational studies, although rich in terms of the quality of the data they produce, are often cost prohibitive [57]. To assess aspects of human behaviour that cannot be measured directly, researchers often rely on scales to measure underlying traits and constructs. These psychometric measures, though common in the field of Psychology, are less commonly used in Human-Computer Interaction research and, specifically, security research.

Haque *et al.* [45] applied psychometric principles to create a scale to assess users' comfort level when asked to create strong passwords. The scale measures participants' perception of the ease of use, hinderances, and user satisfaction with password creation. Results indicate that the scale was successful in comparing the influence of

different interfaces on participants' comfort levels, and the authors were able to use these findings to enable better design of interfaces for mobile password input. Further, the scale provided insight into how different subsets of users experience security measures.

Egelman *et al.* [27] expand the use of scales as an assessment tool in security research. The authors create a psychometric measure that evaluates users on four security topic areas: passwords, securement, awareness, and updating. They relate their scale to existing psychological constructs to understand if those constructs are related to security behaviour. Their results indicate that many of the constructs (e.g., Domain Specific Risk-taking Scale) were indeed related to the security behaviours measured. The scale has potential practical implementations. For example, it could be used in organisations as a way to quickly assess employees' security behaviours and highlight employees that would benefit from targeted education.

The use of security measurement scales within organisations has been researched by Parsons *et al.* [70]. The authors developed the Human Aspects of Information Security Questionnaire (HAIS-Q) to investigate the relationship between users' knowledge of policy, knowledge of procedure, attitude towards policy, attitude towards procedure, and behaviours when using company computers. The scale enabled researchers to understand how these these relationships were interlinked. Further, they were able to iteratively refine their scale so that it was more robust and fine grained for use in the future.

As well as measuring specific characteristics or constructs, surveys methodologies are also useful in measuring security behaviours in general. For example, Stanton *et al.* [78] use a survey to investigate password behaviours. Further, we previously discussed Heath and Rao's [46] survey investigating employee security policy compliance behaviour; as well as Furnell's [34] study of home computer users' security knowledge and behaviours.

2.11 Preliminary study

It is understood that people employ different models for assessing and reacting to threats depending on their experience, context, economic judgements and other attributes. As yet, research in usable security has not attempted to understand the way socially constructed attributes of personality such as masculinity and femininity, as opposed to sex alone, can moderate the way that value judgements are made and their potential effect on users' secure computer behaviour.

Increases in the usability of security systems are generally promulgated through acts such as teaching a user how to correctly use a system or ensuring the users' mental model of the system is correct. It is clear, however, that the efficacy of these acts have varying degrees of success and are strongly mediated by exosystemic factors [1, 91]. For example, a user's previous experience with similar systems or the value of the assets that they wish to protect may affect their experience of using, and value of, a security system. Designing a system to account for a broad spectrum of users' individual differences and experiences can be challenging, as such researchers often endeavour to improve a security system's usability by focusing on areas that tend to see maximum usability improvements across a wide range of users. While these methods can be effective in improving the objective usability of the system, they still do not account for the idiosyncrasies in relation to users' individual differences.

Individual differences that can affect a user's judgement of a security system can be mediated by constructs that are innate in all of us—for example, we may be more willing to disregard a security protocol if we have a propensity for taking risk; or a trusting person may be more likely to share their computer password with a work colleague. These aspects of human personality can account for many of the choices people make, either consciously or unconsciously; however, these differences are yet to be rigorously studied as they relate to usable security. Researchers in the fields of psychology and economics understand that peoples' individual differences play a significant part in how they make decisions; however, when the research focuses on the differences between sexes, participants are split according to their sex and, as a consequence, the underlying factors that may cause those 'sex' differences are often ignored.

Research results such as these can be problematic in that they hypothesise that sex alone is a predictor of behaviour and, as a consequence, disallow that a trait may be a good predictor of behaviour even if the person displaying this trait is of the opposite sex to which the trait is normally associated. If the possibility to exhibit both masculine and feminine traits is provided, regardless of sex, it is then possible to evaluate the relationship between a person's propensity to perform these traits and their behaviour — independent of the view that these traits only exist when they are situated in a specific and appropriate (to cultural norms) body.

We conducted a questionnaire study looking at this interplay between participants' propensity to take risks, their exhibition of culturally specific masculine and feminine traits, as well as their self-reported secure computer behaviour. The study was conducted online and evaluated 155 participants' exhibition of these constructs in an attempt to identify if there was any relationship between them.

The survey was broken down as follows:

1. Demographic questions. These questions included standard demographics such as age and sex.

2. Computer expertise questions. These included participants' education in an IT related field and extent of computer use.

3. Risk-taking inventory questions. This inventory was taken from the work of Meertens & Lion [63] and consisted of a set of seven questions designed to provide a non-domain specific measure of risk-taking behaviour. These questions were 7-point Likert items ranging from 1 = 'Strongly disagree' through to 7 = 'Strongly agree'. Items were summative to form a measure of risk.

4. Bem Sex-role Inventory - Short-Form [11]. This inventory measured participants' masculinity and femininity on a culturally-defined scale (i.e., it had items that are deemed, for example, masculine within a western cultural context), regardless of their sex. It consisted of 30 Likert items with a 7-point scale (10 masculine, 10 feminine and 10 neutral) that summated into two scales—one for masculinity and one for femininity (as per Bem [11], neutral answers were disregarded).

5. Security behaviour questions. Participants were asked to respond *agree*, *disagree*, or *N/A*. These questions followed five separate themes, each containing five questions unless otherwise specified.

   (a) *Protective behaviour*: measures participants undertake to ensure their computer is protected from harmful actions (e.g., do participants take measures to ensure that their anti-virus is always up-to-date).

   (b) *Passwords*: mechanisms users employ to deal with passwords (e.g., do they write down their passwords).

   (c) *Connecting with unknown entities*: how participants connect with unknown entities or let unknown entities connect with them (e.g., do they use peer-to-peer networks or connect to open Wi-Fi sources).

   (d) *Privacy*: measures participants take to protect their privacy (e.g., do they try to limit data collection when visiting websites).

   (e) *Perceptions*: participants' general perceptions of their security compliance behaviour (three questions).

We found a higher propensity to take risk was associated with less secure behaviour, but only to some items within the behaviour measure. Further, we found risk to be significantly related to the masculine sex-typed characteristics; however, we found no such relationship between participants' risk scores and their feminine scale scores. We found that participants' general perceptions of their own security behaviour were related to their reported security behaviours, indicating that participants were somewhat aware of their own security behaviour (i.e., they did not think that they were acting securely whilst at the same time not reporting secure behaviour.

The results from this study were not able to conclusively relate masculine or feminine characteristics to security behaviour. We believe that this is an artefact of the behaviour measure that we used and that construction of a more refined measure would have enabled further investigation of these relationships.

2.12 Statistical analysis

We use multiple statistical tests to analyse the data we collected during our research. Table 2.1 provides and overview of the common tests used in this thesis. Other tests used are described at the point they are used within the text. We assume the standard significance level of .05 for most tests unless otherwise stated (e.g., application of a correction to control for type 1 error).

Table 2.1: Statistical tests

Name	Description	Output
ANOVA	A parametric test comparing three or more sample means to ascertain if they are from the same population distribution.	$F\ (df_{\mathrm{M}},\ df_{\mathrm{R}}) = \mathrm{n},\ p = \mathrm{v}$
Kruskall-Wallis	A non-parametric test using ranks to compare two or more independent samples to ascertain if they are from the same population distribution.	$H\ (df) = \mathrm{n},\ p = \mathrm{v}$
Mann-Whitney	A non-parametric test using ranks to compare two independent samples to ascertain if they are from the same population distribution.	$U = \mathrm{n},\ p = \mathrm{v},\ r = \mathrm{e}$
Where:	n = value of test statistic v = significance level of test r = effect size df = degrees of freedom df_{M} = degrees of freedom for the effect of the model df_{R} = degrees of freedom for the model residuals	

We use the following terminology in relation to regression analyses (used in sections 4.5.5 and 5.6.4):

Multicollinearity: this exists when predictor variables are correlated and can make it difficult to assess the importance of the individual predictors.

VIF(*Variance Inflation Factor*): a measure of multicollinearity; lower is better.

Tolerance levels: a measure of multicollinearity; lower is better.

Standardised residuals: residuals (difference between data points and value of outcome predicted by the model) divided by an estimate of their standard deviation; used to identify outlying data points.

R^2: variance in outcome accounted for by predictor variables in the regression model.

$R^2_{ADJUSTED}$: this is the R^2 value adjusted for *shrinkage* (i.e., the variance in outcome accounted for if the model had been obtained from the *sample population*).

Cook's distance: a measure of the influence that an individual case has on the model.

Chapter 3

Instrument design

3.1 Introduction

This chapter details the construction process for our survey instrument; this process is broken down into four parts:

1. Identification of underlying factors that, after researching existing predictive behavioural models within the security literature, we deemed most relevant to understanding users' interactions and behaviour regarding computer security.

2. Determining what core computer security competencies we wished the instrument to evaluate. We conducted an online poll asking security researchers about the security competencies that they felt were essential for non-expert computer users to understand, and to be able to enact on a regular basis.

3. We followed up our poll with a focus group that asked security researchers to talk about computer security core competencies in more depth and expand on the ideas resulting from our poll.

4. Following the focus group, we developed questions that would evaluate our chosen core competencies. We refined these questions through two card sorting tasks to ensure appropriate face and content validity. Face validity refers to a subjective interpretation of a set of items' ability to actually measure what it appears to measure; content validity refers to a set of items' ability to comprehensively measure an underlying construct.

3.2 Identification of factors

Background research into predictive models of security behaviour enabled us to choose which factors relating to users' security behaviours would be the most meaningful for

an instrument to investigate users' core security competencies.

We created a hierarchy of factors by reviewing five existing models within the literature that we felt contributed the strongest models for predictive security behaviours [8, 25, 36, 60, 67]. Three of the five models used regression or structural equation modelling techniques to return data on which factors had more (or less) of an effect on behavioural outcomes; the remaining two models were proposed research models with their construction details based firmly in the extant literature [8, 36].

We carefully looked at the individual models and took into consideration the main effects, as understood by the authors' analyses of their data. In situations where no main effect for a factor was found across any of the models, the factor was removed from the list of potential factors for the current hierarchy (if an effect was found only in one model it was kept). Some models were more specific in their identification of factors; therefore, some judgement was needed to place categories of one model as sub-categories of another model. For example, Aytes and Connolloy [8] have a factor labelled 'knowledge of countermeasures', so it seems reasonable to place 'effectiveness of safeguard', from Ng *et al.*'s model [67], as a sub-factor. This process was repeated until the factors were either: eliminated (due to the original authors' analyses finding them non-significant factors); combined—if two factors seemed to convey the same meaning but the authors had used slightly different phrasing (an example of this is Aytes and Connolloy's [8], 'costs of secure behaviour', and Liang and Xue's [60], 'safeguard cost'); made into sub-factors (as per the example above); or else identified as high-level factors.

The result of collapsing these models into one hierarchical tree of factors is available in Figure 3.1. We are left with three main factors that are predictive of users' security behaviours: technology awareness, self-efficacy and perceived benefits. We initially used terminology from the literature but subsequently renamed some factors to more accurately reflect our intentions.

Technology Awareness: in broad scope, technology awareness relates to users' understanding of the threats to which they may be susceptible when using technology or navigating online spaces; however, it also relates the users' understanding of possible preventative measures or actions that may be taken

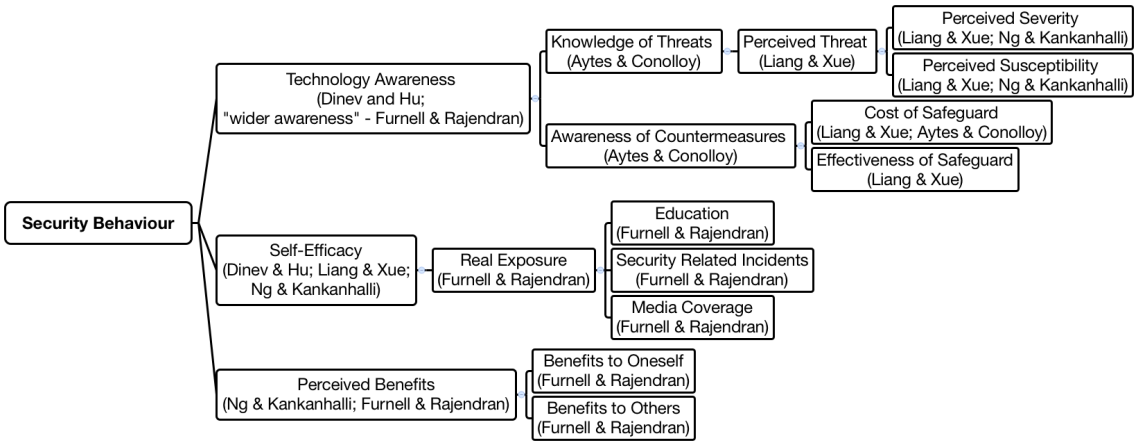


Figure 3.1: Hierarchy of security factors

to protect against such threats. Moving forward, we term this construct as participants' *knowledge*.

Self-efficacy: relates to "...an individual's belief in his or her capacity to execute behaviours necessary to produce specific performance attainments..." [9]. In more simple terms, it is an individual's confidence in their ability to complete a task—in the case at hand, this refers to users' ability to perform protective security measures. Referring to Figure 3.1, we see that the level of confidence in ability can be affected by factors such as previous experience and education. It is reasonable to assume that educating users about specific security threats and potential preventative measures can have an effect on a participants' confidence in executing those preventative measures [16] whether they decide to undertake those measures or not. Previous experiences in dealing with computer security related problems, as well as highly publicised security breaches also shape the way individuals feel about their own ability to defend from potential attacks. This is not to say that education and previous exposure can always have a positive influence; work by LaRose *et al.* [59] finds that educating users can be difficult and, if done with an element of inducing fear (as is often the case), may increase users' insecure behaviours.

Perceived Benefits: these refer to participants' motivational factors for carrying out secure behavioural practices. These may include benefits to oneself, benefits

to others, or even benefits to society as a whole. This is the arena in which users start to perform cost/benefit analyses in an attempt to decide if it is worth making time and money investments to protect against security threats [47]; however, these judgements can often be flawed, Van der Pligt [85] argues that people often struggle with their inability to fully assess the magnitude, as well as the likelihood, of potential risks. For clarity, we term this factor as participants' *motivation*

Behaviour: we used these three constructs as the basis for determining factors that would make up our instrument; however, as our instrument is designed to be an assessment of participants' competency with basic computer security functions, it is necessary for us to include behaviour as an additional factor to aid us in deciding if users put into practice these security behaviours. For example, it is entirely possible that users do not perform secure behavioural practices even when they have the required knowledge and self confidence in their ability—normally this behaviour would be a result of the user conducting some security cost/benefit assessment [47].

With the addition of behaviour as a factor, we were left with four focus areas that made up the basis for our instrument: *knowledge*, *behaviour*, *motivation* and *self-efficacy*. In the next stage of the development process, we decided which core competencies would make up the knowledge and behaviour portions of the instrument. This was not necessary with the self-efficacy and motivation sections as we are able to measure these in a general way with regard to security, rather than in relation to particular security practices.

3.3 Online poll of security researchers

In deciding what core competencies we reasonably expected users' to possess, and to be able to implement on a regular basis, we consulted a group of four usable security researchers from the CHORUS (Carleton's Human Oriented Usable Security) lab. We asked the researchers to complete an online form with their recommended list of users' core security competencies. We also asked for the reasoning behind their decisions.

The process was anonymous; they were not able to see others' recommendations and suggestions, so were not influenced by their peers.

Responses from the researchers were mixed; however, there were two frontrunners: password management best-practice and knowledge of security risks involving phishing. With regard to password management, examples from our researchers included, "...some idea of why certain best password practices are important is also essential to motive[ate] secure behaviour...', and, "Understanding the need to choose good hard to guess passwords...". When commenting on potential phishing attacks one researcher mentioned, "Understanding the risks of email (aka phishing) and know that an email from your bank to log-in may in fact be dangerous. (A lot of people have fallen for these scams)", while another noted, "Social engineering/phishing...because it's so common and affect[s] a lot of people everyday". Other competencies that our researchers highlighted were: understanding Wi-Fi connections (how to set up a secure Wi-Fi system, Wi-Fi encryption), understanding the difference between HTTP and HTTPS connections, social media security, protecting against malicious software, and anti-virus best practices.

3.4 Focus groups

We conducted a round-table focus group to expand on the suggested competencies and come to some agreement on which competencies were the most basic and important for end-users. We invited two different computer security doctoral researchers to speak openly about what competencies they felt were the most important to the everyday user. Our researchers reiterated sentiment from the previous poll that password management best practices and a basic knowledge of phishing attacks (and what users can do to protect themselves against such attacks) were the two most important aspects. Our researchers also agreed that knowledge surrounding malware and how it can be downloaded to one's computer unintentionally would also be a significant factor. Lastly, our researchers felt it would be important for everyday users to understand how to manage updates on their computer, whether it be their browser, operating system, or anti-virus. They felt that an adequate understanding of the risks involved when ignoring or delaying these security updates was imperative for users.

The results of this discussion led to four potential avenues for exploration: password best practice, phishing (understanding, detection and prevention), user understanding of how malware can be downloaded unintentionally and how to avoid such situations, and finally aspects of how users manage their updates. We use these four factors as the basis for the knowledge and behaviour parts of our instrument. We also included users' understanding of their computer and the security options that are available to them (e.g., use of anti-virus software or a computer firewall). We included this dimension as it aligns with two factors mentioned by our researchers: understanding of malware and computer updates. We see these three dimensions as parts of an overarching factor relating to *preventative security measures* (e.g., behaviours that reduce the likelihood that a user's personal computer will be infected/subject to attack).

3.5 Construction of questions

Operationalisation of the constructs was achieved by first looking to see if we were able to adapt questions from previous literature, something that Ng *et al.* [67] describe as drawing "...representational questions from a universal pool". We were able to do this for the part of our measure that evaluates participants' confidence with computer security practices. These questions were adapted from Compeau *et al.* [20] who constructed and validated a scale of computer self-efficacy. This scale has been widely adapted in the literature and has shown good construct validity [6, 60]. For the other parts of our instrument (knowledge, behaviour, and motivation) we opted to create these questions from scratch. For the knowledge and behaviour parts of the instrument, part of the reasoning to start from scratch was so that we could specifically target our core competencies as well as ensuring that both sections were fully aligned in terms of following up on questions regarding knowledge with companion questions regarding behaviour. In regard to the motivation section, we were not able to find a generic security motivation scale that spoke to both the personal and social reasons for enacting secure behaviour; as such, we opted to create one.

3.6 Card sorting

After the first round of item creation, we conducted a test with a group of four individuals (again, security researchers from the CHORUS lab) to further develop and refine the items. In this task, we tested content validity by asking researchers to complete card sorting tasks. All researchers had taken at least one graduate level course in usable security and all were actively researching in the usable security area.

3.6.1 Round one

In a variation on the technique proposed by Moore and Benbasat [66], we presented the items to the researchers in random order on slips of paper. Working individually, they placed items underneath the most fitting (in their opinion) construct headings; the items were presented on slips of paper that had been shuffled. The researchers had unlimited time to complete the exercise; however, on average, took around ten minutes to complete the task. Additionally we asked the researchers to write any notes onto the pieces of paper that they felt would be useful in our assessment afterward (e.g., if an item was ambiguously worded). We also asked the researchers to not force an item into a particular construct—if they were unsure of where is should reside then they could leave it out and make a note of why they thought it did not fit. Figure 3.2 shows the completed Round One card sort from one of the group.

As a measure of inter-rater reliability (i.e., the degree of consensus between participants) we use Fleiss' Kappa ($\varkappa$). Fleiss' Kappa is a measure of reliability of agreement between a fixed number of raters (for a thorough description of Fleiss' Kappa see [30]). The first round of card sorting yielded a kappa value of $\varkappa = 0.47$. According to Landis and Koch [58], this is a moderate agreement between raters. The exercise served to highlight items within the instrument that needed to be modified. For example, one of the questions that related to phishing behaviour was initially worded, "I would check the certificate of a website if I was unsure of its legitimacy", we found that the wording of this question was misinterpreted by some of the researchers as belonging to the motivation factor rather than the behaviour factor. We changed the wording of this item (along with other items that had similar issues) according to the feedback from researchers. From the first round of card sorting, we removed completely 1 item,

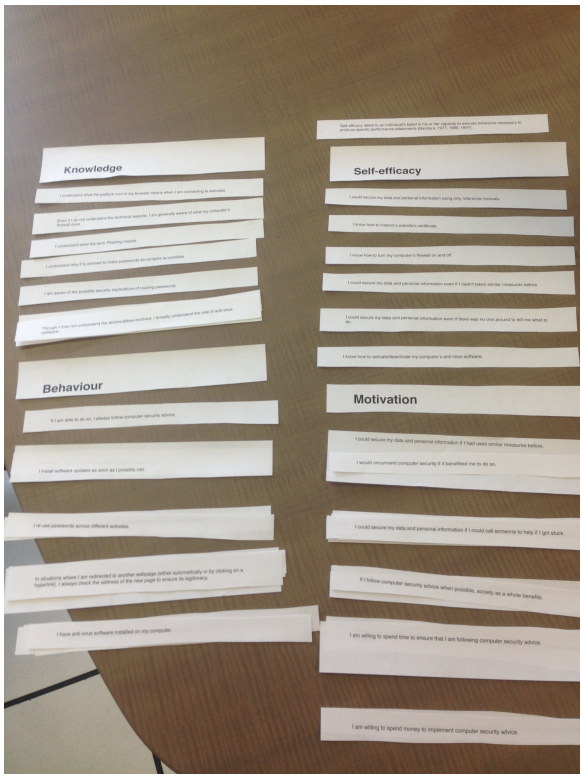


Figure 3.2: First round of card sorting

made 31 minor changes to existing items, and added 3 new items. We also changed the name of the factor *self-efficacy*. Though we had provided a description of what the term meant, feedback from the researchers indicated that the terminology was not clear. We decided to call this factor *confidence in ability* for the second round of sorting. For the rest of this work, we will use the term *confidence* to refer to this factor.

3.6.2 Round two

We performed a second round of card sorting that followed the same general format as the first. We used five different researchers and asked them to complete the sorting task; however, rather than being conducted in the lab setting with physical pieces of paper, this round of card sorting was conducted electronically. Specifically, we presented the items and the construct headings to the researchers in an Excel spreadsheet and asked them to move the items underneath the appropriate construct

heading. Figure 3.3 shows part of the spreadsheet used for the second round of card sorting. This round of card sorting yielded much higher agreement, $\varkappa = 0.83$. Again, using Landis and Koch's interpretation of $\varkappa$ values, this is "almost perfect agreement" (0.81 - 1.00) [58]. Following this second round of card sorting, the only alterations made to the instrument were that we removed two items from the motivation section. These items were not interpreted well by our researchers and they were essentially alternatively worded duplicates of other items in the instrument.

3.7 Final instrument

The final instrument consisted of 45 items split across our four factors: *knowledge*, *behaviour*, *motivation*, and *confidence*. The knowledge and behaviour sections of the instruments were broken down into 6 sections:

1. General questions that related to either knowledge or behaviour at a high level rather than to a specific security issue.
2. Questions relating to password practices.
3. Questions relating to phishing.
4. Questions that related to participants' understanding and use of computer security measures (e.g., firewall).
5. Questions relating to malware.
6. Questions relating to software updates.

All measures use a five-point Likert scale that ranges from 1 = *Strongly agree* to 5 =*Strongly disagree*. The set of questions are presented below:

Questions relating to participants' computer security knowledge

- General
    1. I am aware of at least some of the security threats to personal computer users.
    2. Of the security threats that I know about, I am aware of the actions that I need to take to protect my computer.

- Passwords
    3. I understand the possible security implications of reusing passwords.
    4. I understand why it is important to make passwords as complex as possible.
    5. I understand why one should avoid using personal information for the basis of passwords.
- Phishing
    6. I understand what the term Phishing means.
    7. I understand what the padlock icon in my web browser means when I am connecting to websites.
    8. I understand what a website's certificate indicates with regard to computer security.
- Computer Security Measures
    9. I understand, in a broad sense, the purpose of my computer's firewall.
    10. I understand, in a broad sense, the purpose of anti-virus software.
- Malware
    11. I understand the possible security implications of running programs downloaded from unofficial sources.
    12. I understand the ways in which malicious software can be unintentionally downloaded to my computer.
- Updating Software
    13. I understand why it is important to install software updates as soon as possible after they are available.
    14. I understand the possible security implications of ignoring software updates.

Questions relating to participants' computer security behaviour

- General
    1. No matter the situation, I always follow computer security advice.
    2. When I find out about a security threat, I research ways to protect myself against it
- Passwords
    3. I re-use passwords across different websites.

4. I always try to make my passwords as complex as I can.
5. I sometimes use personal information (e.g., my pet's name) as the basis for passwords.

- Phishing
  6. When I am asked to log in to a website, I make sure to check for the padlock icon in my web browser.
  7. I always look at the address of a web page to ensure its legitimacy.
  8. I always check the certificate of a website if I am unsure about its legitimacy.
- Computer Security Measures
  9. I made sure I had anti-virus software installed when first setting up my personal computer.
  10. I periodically check the status of my anti-virus software.
  11. I made sure the firewall was activated when first setting up my personal computer.
- Malware
  12. I would click on an unsolicited pop-up or banner advertisement if it seemed interesting.
  13. I only download from websites that I trust.
  14. I only click on links in emails if I am sure of the legitimacy of the sender.
- Updating Software
  15. I always install software updates as soon as I possibly can.
  16. If possible, I set my software to install updates automatically.

Questions relating to participants' motivation to perform computer security actions

1. I would ignore computer security advice if it benefitted me to do so.
2. I may ignore computer security advice if it doesn't benefit me personally.
3. By following computer security advice when possible, society as a whole benefits.
4. I have a responsibility to other people to ensure that I follow computer security advice whenever possible.
5. If I incur a financial cost by following computer security advice then I am less

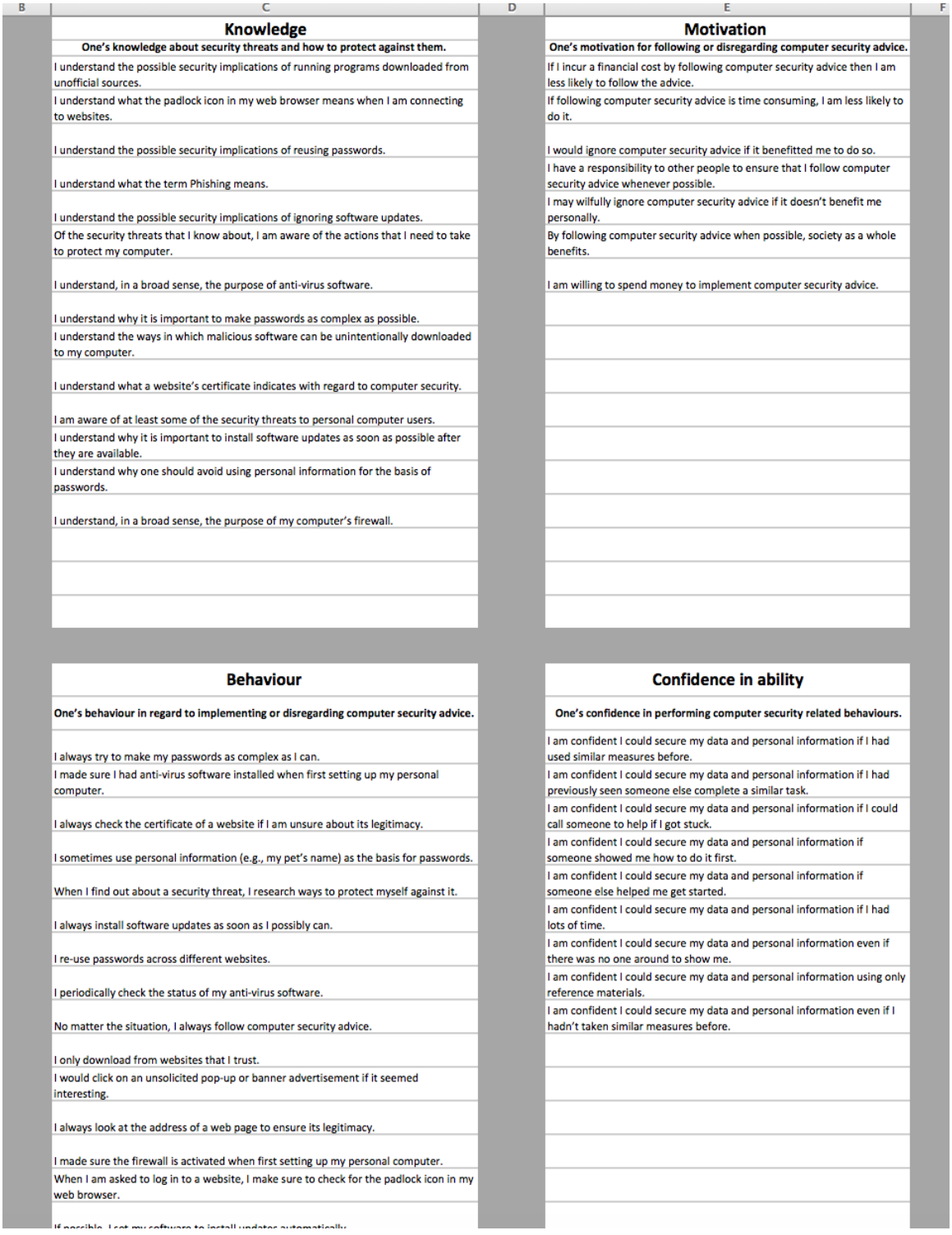
likely to follow the advice.

6. If following computer security advice is time consuming, I am less likely to do it.

Questions relating to participants' confidence in performing computer security actions

1. I am confident I could secure my data and personal information even if there was no one around to show me.
2. I am confident I could secure my data and personal information even if I hadn't taken similar measures before.
3. I am confident I could secure my data and personal information using only reference materials.
4. I am confident I could secure my data and personal information if I had previously seen someone else complete a similar task.
5. I am confident I could secure my data and personal information if I could call someone to help if I got stuck.
6. I am confident I could secure my data and personal information if someone else helped me get started.
7. I am confident I could secure my data and personal information if I had lots of time.
8. I am confident I could secure my data and personal information if someone showed me how to do it first.
9. I am confident I could secure my data and personal information if I had used similar measures before.

This questionnaire is the end result of a multi-step process that involved a literature review to identify candidate factors, an online poll with experts, a focus group with experts, and two rounds of card sorting with experts. We refined our survey instrument at each step, resulting in a 45 item survey covering users' behaviour, knowledge, motivation, and confidence with respect to security behaviours.



Knowledge
One's knowledge about security threats and how to protect against them.
I understand the possible security implications of running programs downloaded from unofficial sources.
I understand what the padlock icon in my web browser means when I am connecting to websites.
I understand the possible security implications of reusing passwords.
I understand what the term Phishing means.
I understand the possible security implications of ignoring software updates.
Of the security threats that I know about, I am aware of the actions that I need to take to protect my computer.
I understand, in a broad sense, the purpose of anti-virus software.
I understand why it is important to make passwords as complex as possible.
I understand the ways in which malicious software can be unintentionally downloaded to my computer.
I understand what a website's certificate indicates with regard to computer security.
I am aware of at least some of the security threats to personal computer users.
I understand why it is important to install software updates as soon as possible after they are available.
I understand why one should avoid using personal information for the basis of passwords.
I understand, in a broad sense, the purpose of my computer's firewall.

Motivation
One's motivation for following or disregarding computer security advice.
If I incur a financial cost by following computer security advice then I am less likely to follow the advice.
If following computer security advice is time consuming, I am less likely to do it.
I would ignore computer security advice if it benefitted me to do so.
I have a responsibility to other people to ensure that I follow computer security advice whenever possible.
I may wilfully ignore computer security advice if it doesn't benefit me personally.
By following computer security advice when possible, society as a whole benefits.
I am willing to spend money to implement computer security advice.

Behaviour
One's behaviour in regard to implementing or disregarding computer security advice.
I always try to make my passwords as complex as I can.
I made sure I had anti-virus software installed when first setting up my personal computer.
I always check the certificate of a website if I am unsure about its legitimacy.
I sometimes use personal information (e.g., my pet's name) as the basis for passwords.
When I find out about a security threat, I research ways to protect myself against it.
I always install software updates as soon as I possibly can.
I re-use passwords across different websites.
I periodically check the status of my anti-virus software.
No matter the situation, I always follow computer security advice.
I only download from websites that I trust.
I would click on an unsolicited pop-up or banner advertisement if it seemed interesting.
I always look at the address of a web page to ensure its legitimacy.
I made sure the firewall is activated when first setting up my personal computer.
When I am asked to log in to a website, I make sure to check for the padlock icon in my web browser.
If possible, I set my software to install updates automatically.

Confidence in ability
One's confidence in performing computer security related behaviours.
I am confident I could secure my data and personal information if I had used similar measures before.
I am confident I could secure my data and personal information if I had previously seen someone else complete a similar task.
I am confident I could secure my data and personal information if I could call someone to help if I got stuck.
I am confident I could secure my data and personal information if someone showed me how to do it first.
I am confident I could secure my data and personal information if someone else helped me get started.
I am confident I could secure my data and personal information if I had lots of time.
I am confident I could secure my data and personal information even if there was no one around to show me.
I am confident I could secure my data and personal information using only reference materials.
I am confident I could secure my data and personal information even if I hadn't taken similar measures before.

Figure 3.3: Second round of card sorting

Chapter 4

Survey study one

4.1 Methodology

We delivered our instrument to participants using the CrowdFlower online service[1]. CrowdFlower is a micro-task recruitment system for persons to post jobs and surveys similar to Amazon's Mechanical Turk[2]. Extensive research has been carried out examining the use of Amazon's Mechanical Turk (MTurk) workers for human-subjects research and it has shown to be a good source for quality data and population diversity (for a comprehensive review, see Mason & Suri [61]). MTurk workers have also been shown to be higher educated and more technologically aware than the general population [84]. Although we do not use MTurk workers directly because it is not possible to post jobs to Amazon's Mechanical Turk without a US billing address, we assume similar attributes are present in our sample; however, we are cognisant of the implications of this assumption (i.e., without research comparing the CrowdFlower workers to the MTurk workers we cannot be 100% sure).

We created the survey using the built-in tools of the CrowdFlower platform (as opposed to using the platform to redirect workers to another website hosting the survey). CrowdFlower customers are able to create jobs on the platform using either a graphical user interface tool or by using simple HTML and CML (CrowdFlower Markup Language) code. We decided to use the HTML and CML as it gave us more control over the layout and presentation of the survey.

Once we had completed the construction of the job, we used CrowdFlower's built-in quality controls to try and reduce the potential occurrences of participants 'gaming' the system. To that end, we ensured the following protocols were in place:

1. The only contributors that were able to complete the survey were CrowdFlower's

[1] https://www.crowdflower.com/
[2] https://www.mturk.com/

highest rated contributors. According to CrowdFlower's website at the time of the study, these contributors accounted for around 7% of monthly judgements made on the platform and maintained a high-level of accuracy across a variety of jobs posted to the platform [21].

2. We decided to choose participants in the United States, United Kingdom, Canada and Australia as our targeted countries because this would be most likely to result in participants' first language being English. CrowdFlower has the option for the selection of required languages but the language list does not include English—this is likely due to the service being hosted in the United States and as such, the assumed default is that participants are able to speak English competently. We chose this extra measure as the nature of the survey requires a full understanding and comprehension of the questions involved and we felt there was the potential for people to understand enough english to use the website but maybe misinterpret complex or nuanced questions.

3. We set the minimum time to complete the job at 300 seconds. Prior to posting the survey, we asked three volunteers to read through the online survey questions fully but did not require them to make a response to the items. We averaged the time of the three participants to be 270 seconds. We then added 0.5 seconds for each question as a minimum amount of time the participants would need to complete the survey. If participants on CrowdFlower take less time than this to complete the job then they are automatically removed from the job by CrowdFlower's system.

4. We allowed each participant to complete the survey one time only.

4.2 Survey presentation

A posting on the CrowdFlower platform announced the name of the job and provided the recruitment notice (see appendix A). After participants had elected to take part in our survey, they were provided with a consent form (see appendix B) that informed them of their rights as a participant, how much they were to be paid, how to withdraw from the study, and whom to contact should they need further information regarding

the study. Once they had read this information, participants then proceeded to complete the survey (as per appendix C). The study protocol was reviewed and cleared by the Carleton University research ethics board.

4.3 Participants

Participants were required to be over the age of 18, be fluent in English, and use a Microsoft Windows computer as their main computer. 436 participants took part in our initial study, they ranged in age from 18 years to 79 years ($M = 36.91$, $SD = 12.07$). 236 males and 199 females took part in the study; one participant preferred not to disclose their sex. As per the recruitment notice for the job, participants received $0.50 (USD). We created a subset from our data by removing the following individuals: 34 participants due to all Likert responses being the same value (our assumption here is that they were not reading the questions and were instead just marking the same number on the scale for each question); 28 participants who did not use Microsoft Windows as their operating system (this removal was because we specifically ask questions relating to anti-virus use and many users of OS X and Linux do not use anti-virus software). We were left with 374 participants, 189 males and 185 females—their ages ranged from 18 years to 79 years ($M = 37.87$, $SD = 12.22$); further demographic descriptives can be seen in Table 4.1. All further analysis is completed on this set of 374 participants.

Table 4.1: Distribution of sex and age across educational levels

Educational Level	Sex (n)		Age (years)	
	Male	Female	M	$S.D$
Some high school, no diploma	11	5	35.13	15.28
High school	33	37	38.73	13.42
Some college, no degree	31	41	35.29	12.46
Technical/trade/vocational training	14	15	40.00	10.40
Associates degree	9	10	36.37	9.97
Bachelor's degree	63	58	38.63	11.42
Master's degree	17	13	37.03	11.91
Professional degree	4	4	44.13	16.66
Doctorate degree	7	2	39.89	10.78

We recruited our participants from four English speaking countries: Canada ($n =$

77), the United States (n = 176), the United Kingdom (n = 117), and Australia (n = 4). All but 3 of our participants owned their own computer; however, we assume that these participants have reasonable, ongoing, access to a computer as they were able to participate in our study and create and use an account with CrowdFlower for the purposes of earning money. In regard to previous education with computers, 12% of participants (n = 45) had an IT related degree and 18% of participants (n = 68) stated that they had taken a computer security related course[3]. Roughly two thirds of the participants used a computer daily for work (n = 262).

4.4 Hypotheses

We made the following hypotheses regarding our study:

H1 We expect that, overall, participants that score higher on our Security Potential measure (combined *knowledge*, *motivation* and *confidence* scores), will self-report as exhibiting more secure computer behaviours with respect to our competencies.

H2 Following on from **H1**, we expect that there will be a positive relationship between participants' scores on the three individual parts of our Security Potential measure and participants' self-reported security behaviours, such that:

- **H2a** Participants that report as having more *knowledge* of our computer security competencies will self-report as exhibiting more secure behaviours with regard to those same competencies.
- **H2b** Participants that report as having increased *motivation* to perform security behaviours will self-report as exhibiting more secure computer behaviours with respect to our competencies.
- **H2c** Participants that have more *confidence* in their ability to perform computer security behaviours will self-report as exhibiting more secure behaviours with regard to our competencies.

[3]Although it is not clear what type of security course this might have been. For example, participants may have interpreted this as a formal university-level course or short training sessions through their employer.

H3 We expect that there will not be significant difference in self-reported computer security behaviour between males and females.

4.5 Results

4.5.1 Internal consistency of scales

We use Cronbach's alpha to measure internal consistency levels within our four factors: knowledge, behaviour, motivation, and confidence. Cronbach's alpha indicates how closely related a set of items are within a group and is frequently used as a measure of scale reliability. Nunnally [69] argues that Cronbach's alpha greater than .70 indicates good internal consistency of measures—we found good levels of consistency for knowledge $\alpha = .96$; behaviour $\alpha = .87$; and confidence $\alpha = .95$. Internal consistency values for motivation were slightly lower at $\alpha = .65$ for all of the motivation items together; however, when broken into personal and social motivation, we find scores of $\alpha = .74$ for personal motivation (questions 1, 2, 5, 6 of the motivation section of the instrument), and $\alpha = .78$ for social motivation (questions 3, 4 of the motivation section of the instrument).

4.5.2 Distribution of participant responses

In the presence of good internal consistency, we scaled our items so that participants had only one score each for our four factors. We completed this task by simply summing participants' responses to each factor, then averaging participants' scores (i.e., divided the total score for each factor by the number of questions pertaining to that factor) so that scores for each ranged from a minimum of 1 to a maximum of 5. For the sake of clarity, we recoded participants' scores so that a higher score on the factor indicates that participants were more knowledgeable; reported more secure behaviour; were more motivated; were more confident. Table 4.2 shows the descriptive statistics for our four factors. All of our factors are non-normally distributed, as indicated by significant Shapiro-Wilk tests. Therefore, we use the median as the measure of central tendency as it is more robust to the effects of outlying data points [29].

Table 4.2: Distribution statistics for four scaled factors

Factors	Descriptives						Shapiro-Wilk
	Min.	Max.	Median	*S.D.*	Skewness	Kurtosis	*W*
Knowledge	1.07	5.00	4.36	.89	-1.67	2.40	.81**
Behaviour	1.31	5.00	3.69	.68	-.58	.38	.98**
Motivation	1.00	5.00	3.17	.69	.36	.37	.98**
Confidence	1.00	5.00	3.89	.93	-.80	.08	.94**

**Significant at the $p < .01$ level.

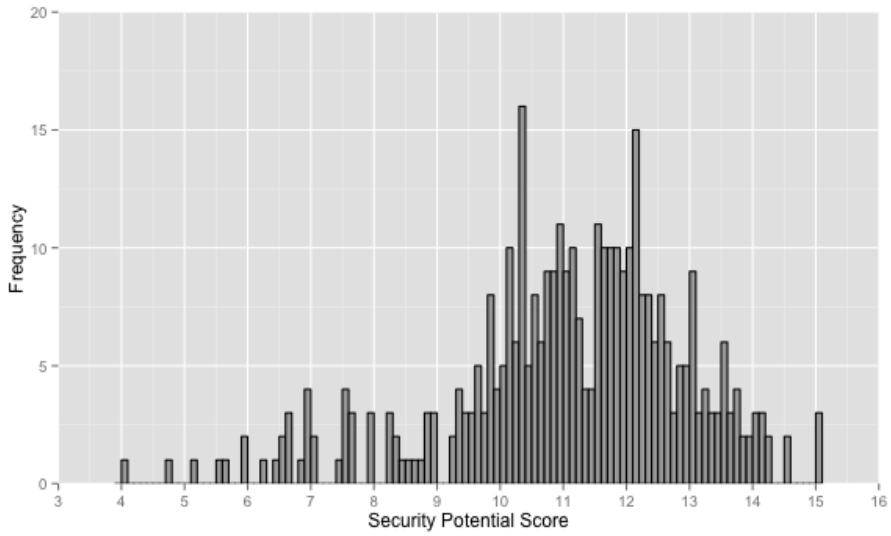


Figure 4.1: Distribution of participants' security potential scores

4.5.3 Security potential groupings

We calculated an overall score for participants by combining their scores on the knowledge measure, the motivation measure and the confidence measure, we term this overall score the participants' *Security Potential* score—participants with higher scores on this measure are classed as having more Security Potential (i.e., more likely to exhibit secure behaviours). We use this terminology do describe the potential that the participant has, at one moment in time (i.e., the time of the survey), to act securely. Scores are theoretically able to range from a minimum of 3 and a maximum of 15. Figure 4.1 shows the distribution of participant scores on the Security Potential measure. Participants ranged in their scores from 4.10 to 15.00 ($Mdn = 11.24$, $M = 11.08$, $SD = 1.90$).

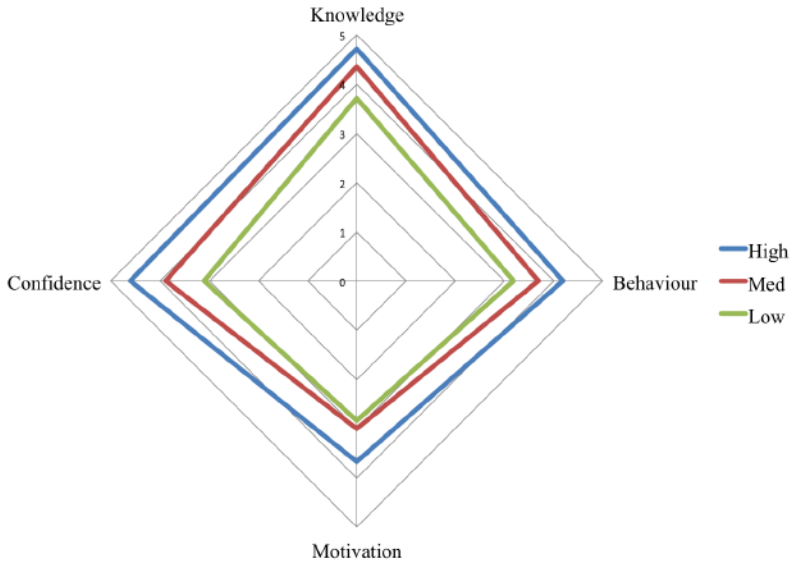


Figure 4.2: Three security potential groups

To investigate our first hypothesis (**H1**), we split the participants into three groups at the 33.4 percentile (10.52 on the Security Potential scale) and 66.6 percentile (12.00 on the Security Potential scale) percentiles. This enabled us to create *high* Security Potential, *medium* Security Potential, and *low* Security Potential groups—Figure 4.2 shows these groups. We make this split for two main reasons: first, it enables easier visualisation of the factors and their relationship to security behaviour; second, it serves as a way to understand the dispersion of Security Potential scores in more detail (e.g., the interquartile range for the low Security Potential groups is much more spread out than those in the medium or high groups)[4]. We hypothesised that our three groups will differ in the degree to which they self-report exhibition of secure behaviours. A Kruskall-Wallis test indicates that participants' levels of self-reported security behaviour is significantly different between the three groups, $H(2) = 171.87$, $p < .001$. A scatterplot of the relationship between Security Potential score and self-reported security behaviour can be seen in Figure 4.3.

Mann-Whitney tests were used to follow up this finding and a Bonferroni correction was applied so all effects are reported at the .025 level of significance. Participants

[4]The division of the groups into equal thirds, though useful, was arbitrary and not based on specific features apparent in the data.

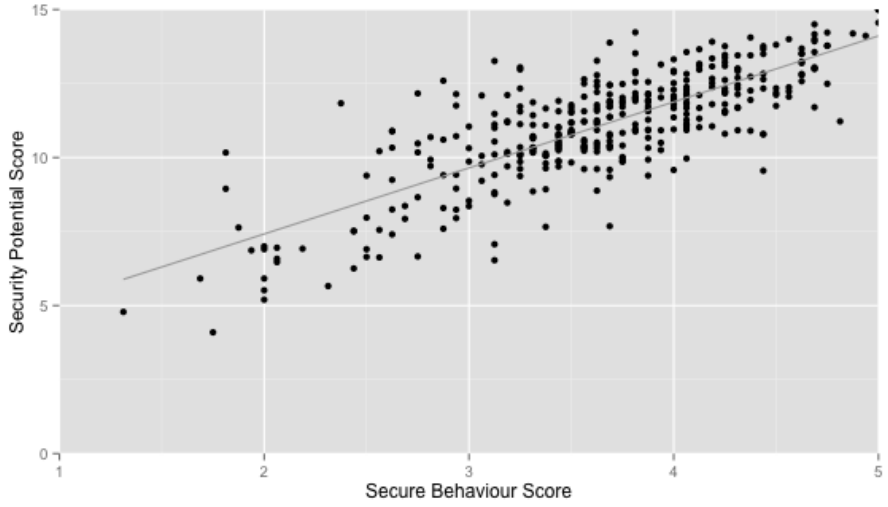


Figure 4.3: Scatterplot of security potential score and security behaviour

in the high Security Potential group were significantly more likely to report secure behaviour than participants in the medium Security Potential group, $U = 3484.50$, $p < .001$, $r = -.48$. Further, participants in the low security group were significantly more likely to report less secure behaviours than participants in the medium Security Potential group, $U = 3037.00$, $p < .001$, $r = -.53$. Effect sizes for these results indicate that both findings are substantive. Box plots in Figure 4.4 show the differences in dispersion between the three groups (notches indicate the 95% confidence interval around the median).

Overall, we find good support for our first hypothesis (**H1**) that participants with a higher Security Potential were more likely to report performing secure computer behaviours with respect to our competencies.

4.5.4 Specific security behaviours

To follow up on the differences in reported behaviour that we found when comparing the three Security Potential groups, we ran further Kruskall-Wallis tests to compare how the groups differed with respect to theme areas within the behaviour measure; for example, how the groups differed with respect to password questions. If differences were found, we followed up using Mann-Whitney tests with a Bonferroni correction to reduce the possibility of type 1 error due to multiple comparisons (significance was

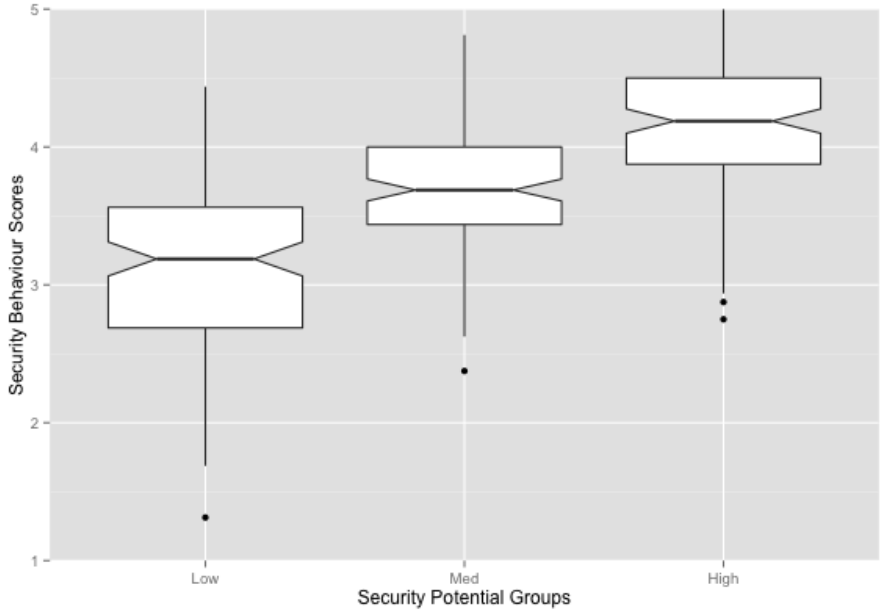


Figure 4.4: Dispersion of security behaviour scores for security potential groups

reduced to the .006 level). Table 4.3 details the results of these analyses.

Table 4.3: Comparison of specific security behaviours between three security potential groups

Behaviour	Kruskall-Wallis	Mann-Whitney			
		Low-Med		Med-High	
	$H^{\dagger}$	U	r	U	r
General	86.73**	4559.00**	-.36	5538.00**	-.25
Passwords	55.52**	6630.50*	-.13	4953.50**	-.31
Phishing	55.11**	5246.50**	-.26	5425.50**	-.26
Preventative	164.65**	3259.00**	-.50	3560.00**	-.47

Note: *$p < .05$ level. **$p < .001$ level. $^{\dagger}df$ for all values = 2.

Analysis of these results indicates that across all behavioural factors, participants in the high Security Potential group were significantly more likely to report exhibiting secure behaviours than participants in the medium group. Moreover, participants in the medium Security Potential group were significantly more likely to report secure behaviours than participants in the low Security Potential group across all factors except password behaviours—although the significance value is less that the standard .05, it does not meet our significance value of .006 or less.

4.5.5 Regression

To understand how the different aspects of our Security Potential measure impact participants' behaviour scores we performed a multiple regression analysis. Regression is a statistical tool that provides a way to predict an outcome variable using one or more predictor variables. In this study we are looking to see how well our predictor variables (the knowledge, motivation, and confidence parts of the Security Potential measure) can predict participants' responses on our outcome variable—self-reported security behaviour. We used a standard hierarchical regression inputting knowledge scores first, then motivation, and finally confidence. Table 4.4 outlines the final model.

Table 4.4: Regression model assessing impact of three factors on behaviour measure score

Step	Predictor	B	SE B	β
Step 1	Constant	1.38	.12	
	Knowledge	.55	.03	.72**
Step 2	Constant	.53	.13	
	Knowledge	.50	.03	.66**
	Motivation	.33	.03	.34**
Step 3	Constant	.36	.13	
	Knowledge	.38	.03	.40**
	Motivation	.35	.03	.34**
	Confidence	.16	.03	.22**

Note: $R^2 = .52$ for Step 1; $\Delta R^2 = .11$ for Step 2 ($p < .001$); $\Delta R^2 = .02$ for Step 3 ($p < .001$). **p $< .001$.

Analysis of case diagnostics show there is no VIF larger than 2.07, far less than the recommended maximum of 10 [12], with the average VIF being not substantially greater than 1 [12]. Tolerance levels are all above the recommended minimum of .2 [64]. These values indicate that there are not unacceptable levels of multicollinearity within our data.

We examined our data for standardised residuals less than -2 or greater than 2. We would normally expect 95% of our cases to fall between -2 and 2 and thus around 5% (approximately 18 cases with $n = 374$) of cases outside these bounds—we found 18 cases and can conclude that our model should be fairly representative of the population. All 18 values had Cook's distance well below 1 and covariance ratios

that indicated that none were unduly influencing the model.

The difference between the final model R^2 and the adjusted R^2 (a difference of .002) indicates that the model would would generalize well. Change statistics for the model indicate that at all steps in the regression, the entry of the variable made a significant impact on the model's predictive power. The impact of the variables are as follows:

- Knowledge (standardized β= .497): This value indicates that as knowledge score increases by one standard deviation (.884 units), participants' behaviour scores increased by .497 standard deviations. The standard deviation for behaviour scores is .676 and so this constitutes a change of 0.33 units on the behaviour measure (.497 x .676). Therefore, for every 1 full unit increase in knowledge score, we see an increase of .380 units on the behaviour measure. This is true only if the effects of confidence and motivation are held constant.

- Motivation (standardized β= .356): This value indicates that as motivation score increases by one standard deviation (.688 units), participants' behaviour scores increased by .356 standard deviations. The standard deviation for behaviour scores is .676 and so this constitutes a change of .241 units on the behaviour measure (.356 x .676). Therefore, for every 1 full unit increase on the motivation measure, we see an increase of .349 units on the behaviour measure. This is true only if the effects of knowledge and confidence are held constant.

- Confidence (standardized β= .219): This value indicates that as confidence score increases by one standard deviation (.931 units), participants' behaviour scores increased by .219 standard deviations. The standard deviation for behaviour scores is .676 and so this constitutes a change of .148 units on the behaviour measure (.219 x .676). Therefore, for every 1 full unit increase on the confidence measure, we see an increase of .159 units on the behaviour measure. This is true only if the effects of knowledge and motivation are held constant.

We can conclude that knowledge has the largest impact on participants' self-reported behaviour scores. That is, the more knowledgable participants are in regard

to our core competency security behaviours, the more likely they are to report that they exhibit these secure computer behaviours. Participants' motivation and confidence both significantly improve the model's fit with the overall model explaining 65.4% of the variance F (3, 370) = 233.47, $p < .001$, $R^2 = .654$, $R^2_{\text{ADJUSTED}} = .652$.

4.5.6 Correlations

To investigate our second hypothesis (**H2**), that our individual evaluation factors—knowledge, motivation, and confidence—would show significant positive relationships with behaviour scores, we looked at correlations between these factors—Table 4.5 details these correlations. We use Spearman's correlation coefficient (Spearman's *rho*, r_s) unless otherwise stated. Spearman's rho is a non-parametric test that is better suited for use with ordinal data than Pearson's product-moment correlation coefficient (Pearson's r) [29].

Table 4.5: Spearman's rho correlations between four factors

Factor	1	2	3	4
1. Knowledge Score	—			
2. Behaviour Score	**.67****	—		
3. Motivation Score	.22**	**.44****	—	
4. Confidence Score	.65**	**.56****	.08	—

Note: **Correlation is significant at the $p < .01$ level.

As indicated by Table 4.5, we find support for our second hypothesis that knowledge (**H2a**), motivation (**H2b**), and confidence in ability (**H2c**) are all significantly positively related to participants' self-reported security behaviours with respect to our competencies. In fact, all of our factors are significantly related except confidence and motivation which appear orthogonal.

4.5.7 Post-hoc correlations

We analysed the correlations between two of our variables, motivation scores and confidence scores, in relation to the *individual* themes within the behaviour measure: 1–general questions; 2–password behaviour questions; 3–phishing questions; and 4–preventative behaviour questions. Although we knew that both motivation

and confidence were significantly correlated with security behaviour as a whole, we were unsure as to how it would relate to the the specific aspects of the security measure individually. As such, we conservatively apply a Bonferroni correction to control for type 1 error—significance is therefore reduced to the .0025 level. Table 4.6 details these relationships.

We found significant positive relationships between participants' motivation scores and their self-reported behaviour for all four themes. We also found that participants' responses to the social aspect of our motivation question were better indicators of their reported security behaviour ($r_s = .55$, $p < .001$) than responses to the personal motivation aspect ($r_s = .24$, $p < .001$).

We found a similar series of significant positive relationships between participants' confidence scores and their self-reported behaviour across all four themes.

Table 4.6: Spearman's rho correlations between confidence, motivation, and aspects of behaviour

Factors	Behaviour Questions				
	Total Behav.	General	Password	Phishing	Preventative
Confidence	.55**	.33**	.29**	.36**	.54**
Motivation	.44**	.34**	.37**	.15**	.44**
Social Motivation	.55**	.45**	.23**	.29**	.56**
Personal Motivation	.24**	.19**	.30**	.05	.24**

**Significant at the p < .001 level.

Overall our data reiterates our findings from the earlier regression: all three factors have a positive relationship with participants' self-reported behaviour. When we investigate motivation and split our questions into *personal* (i.e., self-interest) and *social* (i.e., other-interest) motivation we see that social motivation shows a stronger relationship with secure behaviours than personal motivation. We aim to investigate this finding further in a follow up study.

4.5.8 Sex

We investigated the effect of participants' sex on the each of our four measures; descriptive statistics for the factors can be seen in Table 4.7. We hypothesised that there would be no significant difference between the scores of males and females

on these measures (**H3**). We conducted Mann-Whitney tests and found significant differences between scores by males and females with respect to both the motivation and behaviour. For motivation, we found that males were less motivated than females, $U = 14820.00$, $p < .01$, $r = -.13$. With regard to security behaviour we found that males reported less secure behaviour than females, $U = 15351.50$, $p < .05$, $r = -.10$.

Although the effect sizes we found were small, we completed a post-hoc analysis in an attempt to understand, with respect to the behaviour measure, which specific behaviour males and females differed. We compared male and female responses to the: general behaviour questions, password behaviour questions, phishing behaviour questions, and preventative behaviour questions. We find that the questions relating to preventative behaviour are the ones that show a significant difference between males and females. Specifically, we found that males reported less preventative security behaviour than females, $U = 13143.00$, $p < .001$, $r = -.22$.

Table 4.7: Descriptives for males and females across four factors

Factors	Descriptives				
	Sex	Min	Max	Median	*S.D.*
Knowledge	Male	1.07	5.00	4.36	.98
	Female	1.29	5.00	4.29	.77
Behaviour	Male	1.69	5.00	3.69	.68
	Female	1.31	5.00	3.69	.67
Motivation	Male	1.00	5.00	3.00	.66
	Female	1.50	5.00	3.33	.70
Confidence	Male	1.00	5.00	4.00	.99
	Female	1.11	5.00	3.89	.86

4.5.9 Preventative security behaviour and sex

To follow up on both our findings with respect to sex differences and preventative behaviour, as well as the difference in reported behaviours between our three Security Potential groups (high, medium, low), we performed an *Aligned Rank Transformation* for non-parametric factorial analysis [92]. Regular factorial ANOVA requires assumptions to be met which are often violated when using non-parametric Likert-scale data;

the Aligned Rank Transformation allows for use of non-parametric data and is capable of producing interaction effects in a similar vein to the tradition ANOVA. We expected to see main effects of grouping (section 4.5.3) and sex (section 4.5.8) in line with our previous analysis but are primarily investigating any potential interaction effects between the two.

We found a significant main effect of Security Potential grouping on participants' reported preventative behaviour scores, F (2, 368) = 162.08, $p < .01$. Tukey's HSD comparisons indicate that, in line with our previous findings, the high Security Potential group self-report as performing more preventative secure behaviours than the medium Security Potential group ($p < .01$). We also find that the medium Security Potential group report more preventative secure behaviours than the low Security Potential group ($p < .01$).

We found a significant main effect of participant sex on the reporting of preventative secure behaviours, F (1, 368) = 35.76, $p < .01$. Overall it appears that females are more likely to report performing secure behaviours than males.

We also found a significant interaction effect between Security Potential grouping and sex on reporting preventative security behaviours F (1, 368) = 35.76, $p < .01$. Figure 4.5 is an interaction graph detailing this interaction. We see that for the low and medium Security Potential groups, females report performing more preventative security behaviours than males; however, in the high Security Potential group both females and males reported around the same degree of preventative behaviours.

Our findings indicate that there is a consistent, though small, difference between males and females in their reporting of preventative security measures in the low and medium Security Potential groups; however, when looking at the high Security Potential group this difference is greatly reduced. Further investigation into this sex difference is needed to explain why the difference only exists for certain aspects of behaviour and what changes in the high Security Potential group render this difference negligible.

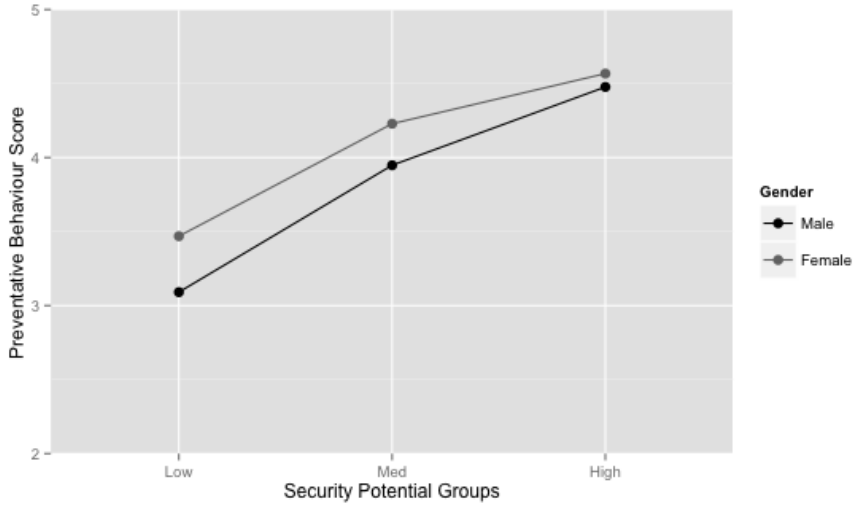


Figure 4.5: Interaction between grouping variable, sex and reported preventative security behaviour

4.6 Summary

We found support for both of our first (**H1**) and second (**H2**) hypotheses. We found significant relationships between individual aspects of the Security Potential measure (knowledge, motivation and confidence) and participants' self-reported security behaviours behaviours. Further, when our factors were grouped as a whole measure of Security Potential, participants that had a higher Security Potential score were more likely to report exhibition of secure competency behaviours.

We initially hypothesised that there would be no sex differences with respect to participants' scores on the factors of our evaluation measure (**H3**). Our data indicates that there are small differences between males and females in both their scores on the motivation scales (males being less motivated than females to perform secure competency behaviours) and with their self-reporting of behaviours that reflect preventative security measures (females report more security behaviours than males).

Further discussion of these results will be provided in Chapter 6 when we discuss both studies together.

Chapter 5

Survey study two

5.1 Introduction

For our second study, we made some modifications to our instrument. The purpose of these modifications was to expand on our findings from Study One (Chapter 4). Specifically, we wish to try and understand the reason for the sex differences that we saw, as well as expand on the motivational differences that we found. Further, we wish to explore if findings from Study One are replicable.

5.2 Additional measures

The modifications that we made to the instrument were all additions, that is, we did not remove any of the previous measures. We added three extra measures to the scale (detailed below). The first two were to further expand on results from Study One related to the sex difference and motivational differences. The third scale assessed participants' propensity to take risk. The addition of this scale has basis in the literature, such that research has found that participants that identify as engaging in riskier behaviour report as being less secure in their computer security [27, 76]. Our selected scale differs in that it presents a general propensity to take risk scale rather than a domain specific risk scale.

1. *Bem Sex Role Inventory* (short form) [11]:

   Following up on the small behaviour differences we found between males and females in Study One, we decided to investigate these differences in a way that looks at traditionally sex-typed characteristics to see if these characteristics have any influence on participants' security behaviours. We previously used this scale in our preliminary study (see appendix E and Section 2.11) and found that it was a better predictor of risk-taking behaviour than sex alone; however,

issues with our security scale prevented us from seeing whether it had a direct effect on security behaviour.

This inventory is predicated on the concept that a traditionally sex-typed person bases and models their behaviour on ideal standards of masculinity and femininity with respect to their culture; as such, this scale is based upon standards of masculinity and femininity as they pertain to a western culture (the initial work was based upon US ideals). The inventory is novel in its ability to generate both a score for masculinity and a score for femininity that are independent of each other (i.e., they do not negate each other and an increase on one scale does not automatically result in a decrease on the other). An advantage of this independence is that participants are able to score high on both scales or low on both scales in addition to the normal assessments of high masculinity/low femininity and high femininity/low masculinity.

The inventory used in the current study is the short form version that includes thirty questions in total: ten questions that relate to masculine ideals, ten that relate to feminine ideals and ten that are neither masculine or feminine. The original form had twice the number of questions in each section—60 questions in total. Participants are presented with characteristics (e.g., *'Independent'* or *'Sympathetic'*) and asked to rate how much the characteristic relates to them. The inventory uses a seven-point Likert scale that ranges from 1 = *Never true* to 7 = *Always true*. Masculine and feminine items are summated, then averaged, giving each participant a separate masculine and feminine score. As per Bem [11], the ten items that are neither masculine or feminine are discarded. A higher score on these scales means the respondent exhibits more masculine or feminine characteristics. The full inventory is detailed in appendix D.

2. *Self- and Other-interest Inventory* [40]:

   In Study One, we found that participants with a higher social motivation to perform security behaviours were more likely to report performing secure behaviours in general. We found a smaller correlation between personally motivated behaviour and self-reported security behaviours. As such, we test this

result to see if the finding holds up with a generic scale of self-interest and other-interest.

The self- and other-interest inventory was developed as a measure of assessing the extent to which a respondent's behaviour is driven by self-interest and/or interest in others (i.e., prosocial behaviours). The inventory contains two sub-scales (one each for self- and other-interest) each containing nine statements. Participants are asked to rate on a seven-point Likert scale to what degree they agree with the statements presented; the scale ranges from 1 = *Strongly agree* to 7 = *Strongly disagree*. Two examples of statements are: *'Doing well in my pursuits is near the top of my priorities'*—part of the self-interest sub-scale; *'I look for opportunities to help people I know achieve higher social status'*—part of the other-interest sub-scale. Items are summated and averaged to give each respondent separate measures of self-interest and other-interest. In a similar fashion to the Sex Role Inventory, participants have the ability to score high on both scales, low on both scales, or anywhere in-between. Higher on either of these scales means that the respondent exhibits a higher degree self- or other-interest (depending). The full inventory is detailed in appendix D.

3. *The Risk Propensity Scale* [63]:

   We included a risk propensity scale in our second study as a way to understand the impact of participants' risk taking on their security behaviour. Previous research has show that users that are more risk-averse are more likely to display secure behaviour than those that engage in risk-taking behaviour [27, 76]. We investigate whether we will see the same relationship between behaviour and a general propensity to take risk measure.

   The risk propensity scale is an eight question scale measuring respondents' general risk-taking tendencies. Participants are asked to read the eight statements and then to rate on a seven-point Likert scale their level agreement with each one; the scale ranges from 1 = *Strongly agree* to 7 = *Strongly disagree*. For example, one statement reads, *'I usually view risks as a challenge'*. Items are summated, then averaged, to give the respondent an overall risk propensity

score. A higher score on the risk measure means the respondent is more likely to exhibit risk taking behaviour. The full scale is detailed in appendix D.

5.3 Methodology

Similar to Study One, we used the CrowdFlower online service to deliver our survey. We amended our survey to include the three extra measures mentioned at the beginning of this chapter and doubled the amount that participants were paid to $1.00 (USD) in order to reflect the extra work required of the longer survey. In terms of delivery, most details were kept the same; that is:

1. We chose only participants from the US, UK, Canada and Australia.
2. We filtered so that only CrowdFlower's top contributors were able to complete the survey.
3. Participants were required to be fluent in English, over 18 years old and use the Microsoft Windows operating system on their main computer.

The one difference between the delivery of the two surveys was that we stipulated a longer minimum amount of time to complete the the current study, compared to the first. This was due to the extra questions that we required participants to answer. The current study stipulated that participants who completed the survey faster than 480 seconds would be removed by CrowdFlower. The study protocol was reviewed and cleared by the Carleton University research ethics board.

5.4 Participants

We initially recruited 300 participants for our study. We removed 22 participants that did not use Microsoft Windows as their main operating system, and we removed 2 further participants that reported that they were under 18 years old. We were left with 276 participants, 140 males and 136 females, ranging in age from 18 years to 74 years ($M = 37.77$, $SD = 11.80$). Participants originated from: Australia ($n = 3$), Canada ($n = 59$), the United Kingdom ($n = 76$), and the United States ($n = 138$).

Only two participants did not own their own computer; however, these participants did use a computer daily for work, thus we assume they are familiar enough with computers to keep them in our dataset. In regard to previous education, 16% of participants ($n = 44$) had an IT related degree and 19% ($n = 52$) of participants reported that they had completed a computer security related course. 70% ($n = 192$) of participants used a computer daily for work. All further data analysis within this chapter is conducted on our subset of 276 participants.

5.5 Hypotheses

Based on the results of Study One and our preliminary study, we make the following hypotheses:

H1 We predict that the feminine sub-scale of the sex role inventory will show a stronger relationship with participants' motivation to complete secure computer behaviours than the masculine sub-scale of the sex role inventory.

H2 We predict that the feminine sub-scale of the sex role inventory will show a stronger relationship with participants' self-report of secure computer behaviour than the masculine sub-scale of the sex role inventory.

H3 Expanding on findings from Study One, we expect to find significant positive relationships between both the self-interest scale and behaviour, as well as the other-interest scale and behaviour (**H3a**). Further, we expect other-interest to show a stronger relationship with behaviour than self-interest (**H3b**).

H4 We expect to see an inverse relationship between participants' propensity to take risk and their secure behaviours.

5.6 Results

5.6.1 Internal consistency of scales

We again use Cronbach's alpha to measure the internal consistency of our scales. Table 5.1 details the alpha values for each scale. Similar to our Study One, we found

good levels of consistency throughout our scales. Two of our scales, the motivation scale and the risk scale, were below Nunnally's [69] criteria of $\alpha = .70$ for 'good' consistency; however, they were still within the 'acceptable' range.

Table 5.1: Internal consistency of scales (Cronbach's alpha)

Measure	α
Original Measures	
Knowledge	.89**
Behaviour	.83**
Motivation	.69*
Social Motivation	.79**
Personal Motivation	.79**
New Measures from Existing Literature	
Confidence	.92***
Risk	.65*
Self-interest	.90***
Other-interest	.92***
Bem Masculine	.88**
Bem Feminine	.92***

Note: According to Nunnally [69]: *'Acceptable'; **'Good'; ***'Excellent'.

5.6.2 Distribution of participant responses

Similar to Study One, we found that a similar distribution of score across our four original factors; again, all were non-normally distributed as indicated by significant Shapiro-Wilk tests. The new factors for this study (risk, self-interest, other-interest, masculine and feminine) also show non-normally distributed responses. Distributions for all factors can be seen in Table 5.2.

With regard to participants' scores on the Security Potential score (the combined score of knowledge, motivation and behaviour), results are similar to Study One and show a skewed distribution; however, Shapiro-Wilks test indicate that distribution is normally distributed. Figure 5.1 details this distribution of scores. Theoretically, participants could score between 3 and 15 on this measure; results show participants ranged in their scores from from 6.83 to 15.00 ($Mdn = 11.53$, $M = 11.48$, $SD = 1.40$).

Table 5.2: Distribution statistics for nine factors

Factors	Descriptives						Shapiro-Wilk
	Min.	Max.	Median	*S.D*	Skewness	Kurtosis	*W*
Original							
Knowledge	2.21	5.00	4.43	.53	-1.07	1.42	.92**
Behaviour	2.06	5.00	3.75	.68	-.39	-.24	.98**
Motivation	1.67	5.00	3.00	.69	.30	-.40	.98**
Confidence	1.56	5.00	4.00	.72	-.62	.10	.95**
New							
Risk	1.00	5.83	2.83	.88	.34	.04	.98**
Self-interest	1.00	7.00	4.56	1.16	.05	-.25	.99**
Other-Interest	1.22	7.00	4.83	1.17	-.30	.04	.98**
Bem Masc.	1.30	7.00	4.50	1.02	.04	-.12	.99**
Bem Fem.	1.60	7.00	5.40	1.04	-.75	.62	.96**

Note: Original measures range 1-5, new measures range 1-7. **Significant at the $p < .01$ level.

5.6.3 Security potential groupings

Following procedure from the Study One, we split our participants into three groups: *high*, *medium*, and *low* security potential. This was achieved by demarcating the groups at the 34.4 and 67.0 percentiles. We checked to see if the results from this study aligned with the results from Study One in regard to the relationship between Security Potential scores and secure behaviour; the following analysis indicates that they did.

A Kruskall-Wallis test indicated that self-reported security behaviour was significantly different between our high, medium, and low groups, $H(2) = 118.68$ $p < .001$. We followed up this result with Mann-Whitney test and applied a Bonferroni correction to control for type one error, thus significance was reduced to the .025 level. Results show that participants in the high Security Potential group were significantly more likely to report behaving securely than participants in the medium Security Potential group, $U = 2186.00$, $p < .001$, $r = -.40$. Further, participants in the low Security Potential group were less likely to report secure behaviour than participants in the medium security potential group, $U = 1782.50$, $p < .001$, $r = -.50$. Similar Study One, effect sizes for these findings are substantial, Figure 5.2 shows the dispersion in security behaviour scores for these three groups. A radar diagram detailing the three security potential groups and their score on our original 4 factors can be

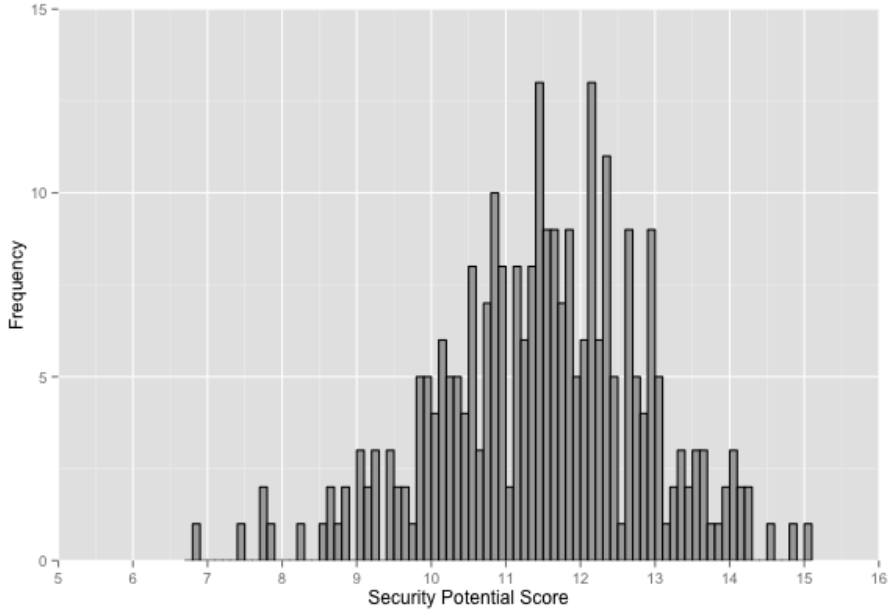


Figure 5.1: Histogram of security potential scores

seen in Figure 5.3.

5.6.4 Confirmatory regression and correlations

To confirm results from Study One, we created a regression model that uses participants' knowledge, motivation, and confidence to predict participants' behaviour scores. We followed the same procedure as Study One and found a similar result. Again, we found that knowledge was the biggest predictor of participants' security behaviour scores; however, all factors significantly improved the model fit with the final model accounting for around 54.5% of the variance in security behaviour scores, F (3, 272) = 108.58, $p < .001$, $R^2 = .545$, $R^2_{\text{ADJUSTED}} = .540$. Although this model does not account for the same amount of variance that we found in the Study One (65.4%), we argue that, in context, accounting for over 50% of the variance in participants' behaviour scores using these three factors is reasonable.

As a further confirmation measure, we investigated the relationships between our four original factors. Results from Study One indicated that knowledge, motivation and confidence were all significantly correlated with participants' security behaviour. We find similar results in the current study, Table 5.3 details these relationships.

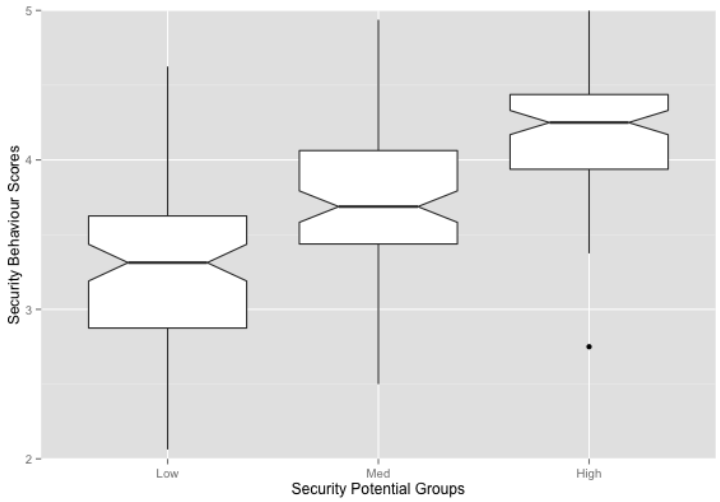


Figure 5.2: Dispersion of security behaviour scores for security potential groups

Table 5.3: Spearman's rho correlations between four original factors

Factor	1	2	3	4
1. Knowledge Score	—			
2. Behaviour Score	**.65****	—		
3. Motivation Score	.23**	**.45****	—	
4. Confidence Score	.58**	**.46****	.01	—

Note: **Correlation is significant at the $p < .01$ level.

5.6.5 Sex and sex-typed characteristics

Results from our first study indicated there were sex differences between our participants with regard to their motivation to perform secure behaviours and their reported secure behaviours. To gain deeper insight into these potential differences, we added the Bem Sex Role Inventory to our survey (discussed in section 5.2). Descriptive statistics showing the distribution of male and female scores on the masculinity and femininity scales can be seen in Table 5.4. To test our first hypothesis (**H1**) we first looked to see if the same sex differences from Study One were present in the current study.

We investigated the difference in motivation scores between males and females, with the expectation that females be more motivated than males. We conducted a Mann-Whitney test and found that there was difference, and that females were more motivated behave securely, $U = 7286.00$, $p < .001$, $r = -.20$; a box plot detailing the

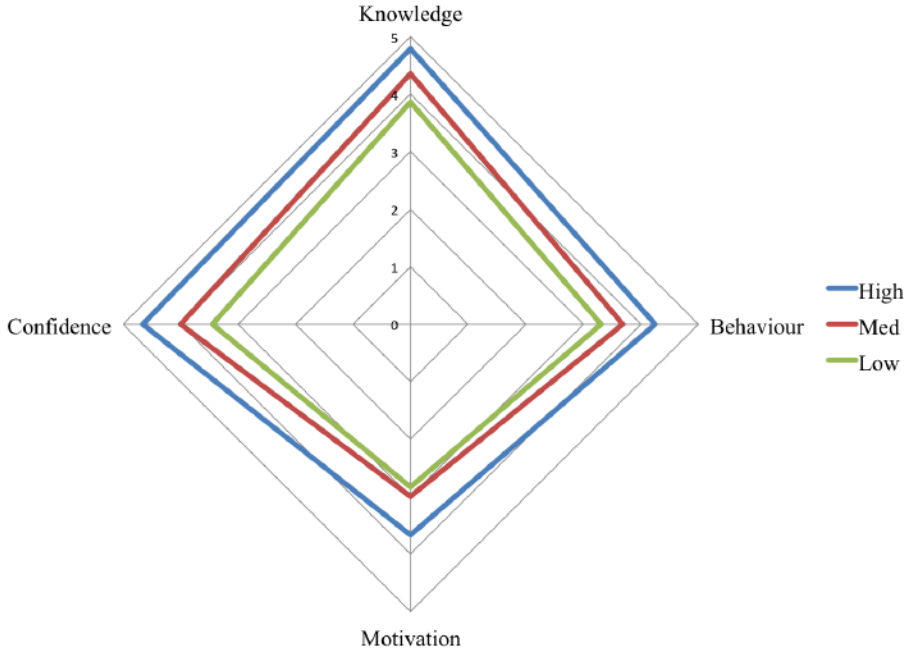


Figure 5.3: Three security potential groups' average scores on four original factors

Table 5.4: Descriptives for males and females in relation to masculine and feminine Bem scales

Bem Scale	Descriptives				
	Sex	Min	Max	Median	*S.D.*
Masculine	Male	1.30	7.00	4.60	.99
	Female	2.10	7.00	4.30	1.03
Feminine	Male	3.00	7.00	5.20	.93
	Female	1.60	7.00	5.50	1.13

dispersion of these scores can be seen in Figure 5.4. Next we looked at differences between males and females with respect to their reports of secure behaviour; contrary to the Study One (and in line with our preliminary study) we found no difference, $U = 9358.00$, $p = ns$. A box plot of male and female score with respect to security behaviour can be seen in Figure 5.5.

To further investigate these findings, we refer back to our hypothesis that there would be a stronger relationship between the feminine Bem scale and motivation than there would be between the masculine Bem scale and motivation (**H1**). We

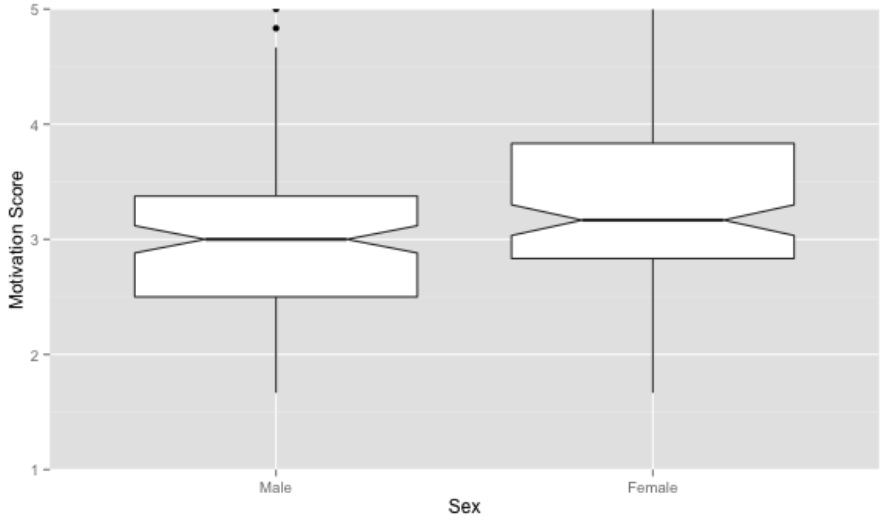


Figure 5.4: Motivation scores for males and females

found that this was the case and that the feminine Bem scale did show a significant relationship with participants' motivation scores ($r_s = .15$, $p < .01$), whereas the masculine Bem scale did not ($r_s = $ -.05, $p = ns.$); a scatter plot of participants' scores on the masculine and feminine scales, and their relationship to motivation can be seen in Figure 5.6. We compared these correlations by evaluating the difference in t statistic to see if they were significantly different from each other [29], we found that the difference was significant, $p < .01$. This supports our first hypothesis (**H1**), insomuch that it indicates that certain characteristics that make up the feminine Bem scale show a stronger relationship with security motivation than those characteristics found in the masculine Bem scale.

Our second hypothesis (**H2**) predicted that we would find a stronger relationship between the feminine Bem scale and security behaviour scores than between the masculine Bem scale and security behaviour scores. We find that the feminine Bem scale does show a stronger relationship with behaviour scores ($r_s = .38$, $p < .001$) than the masculine Bem scale ($r_s = .26$, $p < .001$). The difference in t statistic indicates that these correlations are significantly different, $p < .05$. These findings support our second hypothesis (**H2**) and indicate participants that report as being more secure are more likely to identify with characteristics within the feminine Bem scale than the masculine Bem scale. The relationship between masculine, feminine,

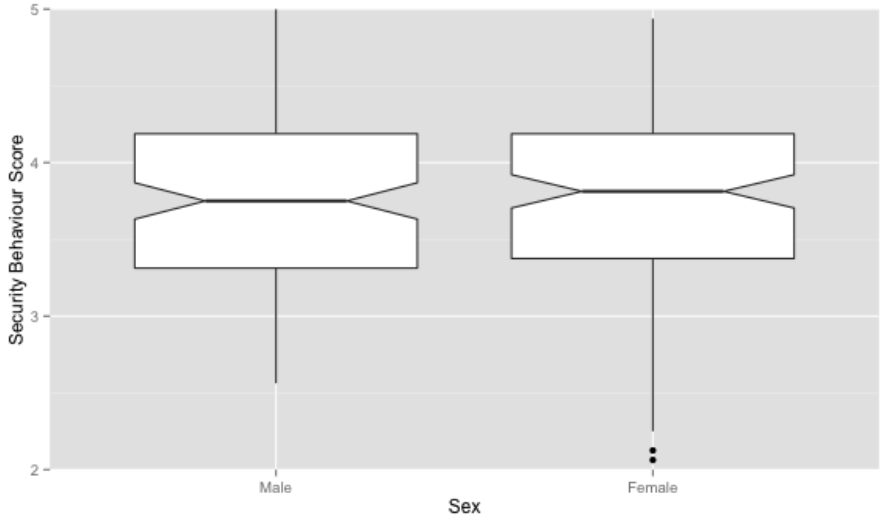


Figure 5.5: Security behaviour scores for males and females

and security behaviour scores can be seen in Figure 5.7.

5.6.6 Self- and other-interest

In Study One, we found that the social motivation questions within our motivation factor showed a stronger relationship with secure behaviour than questions relating to personal motivation. We hypothesised (**H3**) that the same will hold true with a general measure of self- and other interest. We explore if security behaviour is related to this psychological construct at a general level or if it is domain specific.

Results indicate that security behaviour is significantly correlated with self-interest ($r_s = .24$, $p < .001$), and other-interest ($r_s = .37$, $p < .001$). The difference in t statistic indicates that these correlations are significantly different from each other, $p < .01$. Scatter plots of both self- and other-interest with respect to security behaviour scores can be see in Figure 5.8.

We believe that these results show support for **H3**. That is, participants with greater levels of interest in the well-being of others may be more likely to exhibit secure computer behaviours than those that do not. Further, participants that show high levels of self-interest are also more likely to exhibit secure computer behaviours; however, not to the same extent.

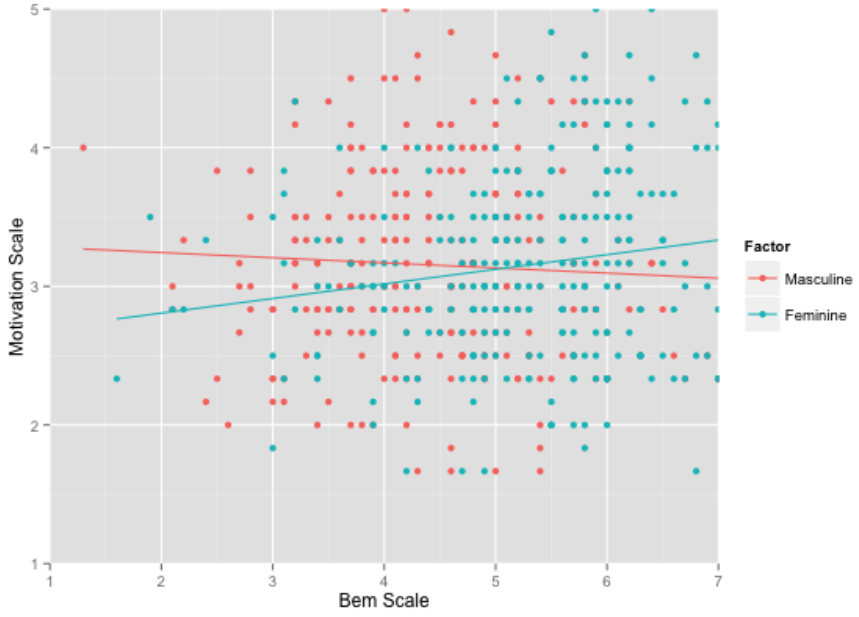


Figure 5.6: Motivation scores against Bem Scales

5.6.7 Risk

In the current study, we also look at participants' propensity to take risk as a factor that may be indicative of a participant's computer security behaviour. Our results indicate that we find support for our hypothesis (**H4**): there is a negative relationship between participants' propensity to engage in risk taking behaviour and their reported security behaviour, r_s = -.20, $p < .01$; this relationship can be seen in Figure 5.9

Post-hoc risk analysis

Following up on our finding regarding risk and behaviour, we further investigated risk with respect to sex and the Bem masculine and feminine scales. We performed a Mann-Whitney test to investigate potential sex differences with regard to participants' propensity to take risk. We find that males report a higher propensity to take risk than females $U = 6926.00$, $p < .001$, r = -.24. A box plot showing dispersion of male and female risk scores can be seen in Figure 5.10.

We investigate propensity to take risk with regard to participants' scores on the both the masculine Bem scale and the feminine Bem scale. We find a significant

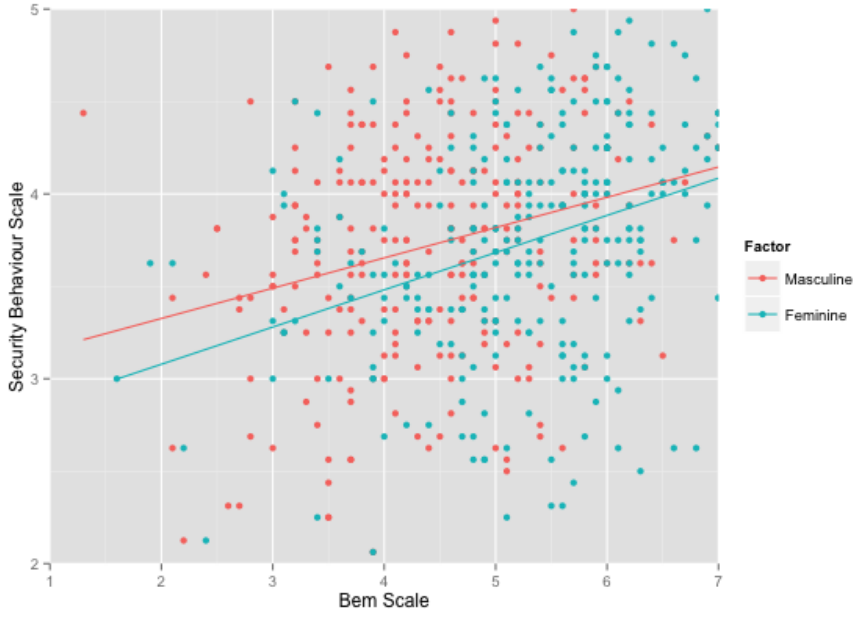


Figure 5.7: Security behaviour scores against masculine and feminine Bem scales

positive relationship between the masculine Bem scale and risk ($r_s = .22$, $p < .001$), whereas we find a significant negative relationship between the feminine Bem scale and risk ($r_s = -.22$, $p < .001$). Difference in t statistic indicates that there is a significant difference between these correlations, $p < .001$. Figure 5.11 details the relationships between both the masculine and feminine Bem scale, and participants' risk scores.

Overall, we find good support for our hypothesis regarding risk (**H4**), such that, participants that are more risk taking appear to exhibit more insecure behaviour. We find that there is a significant sex difference between males' and females' propensity to take risk. Further, idealised masculine and feminine characteristics, as measured by the two Sex Role Inventory scales, show significantly different relationships (positive and negative respectively) with participants' score on the propensity to take risk scale. Our results from the preliminary study showed a similar relationship between scores on the masculine scale and risk propensity; however, it did not find a relationship between the participants' scores on the feminine scale and risk. The results from the the current study are more in line with the literature on risk.

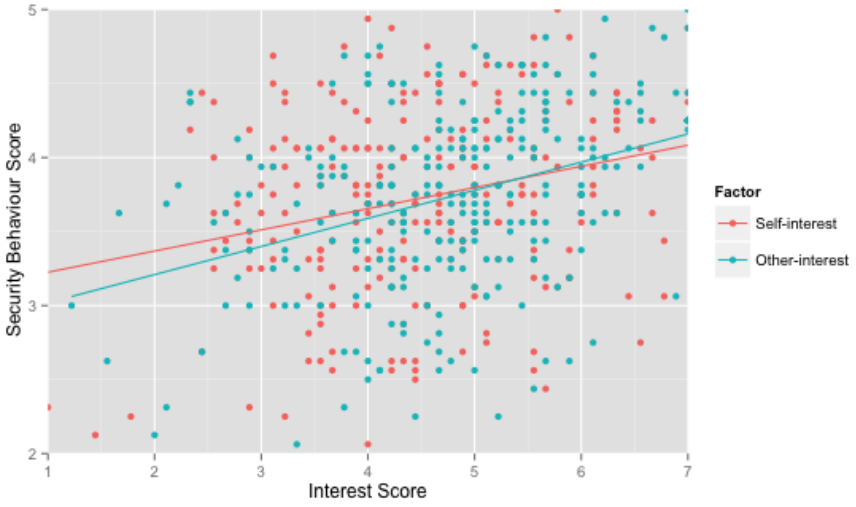


Figure 5.8: Scatterplot of relationship between self- and other-interest scores and security behaviour

5.6.8 Overall impact of factors

As an exploration of the overall impact of the factors on security behaviour, we conducted a Relative Weight Analysis [53] in an attempt to understand which factors have the most impact on security behaviour scores. Regression analysis is geared toward explaining incremental prediction; however, when predictor variables are correlated, variables that show significant correlational relationships with the outcome variable may not show significant incremental prediction due to shared variance. Relative Weight Analysis highlights which predictor variables explain significant variance in outcome variables, regardless of the degree of correlation with other predictor variables.

In our model, we enter the following factors as predictor variables: knowledge score, social motivation score, personal motivation score, confidence score, masculine score, feminine score, other-interest score, self-interest score, and risk score. We conducted the analysis using RWA-WEB[1]. Results from this analysis are detailed in Table 5.5. We followed the recommended procedure of Tonidandel *et al.* [82] and thus confidence intervals for the individual relative weights were bootstrapped with 10,000 replications, as were the corresponding tests of significance. Our results

[1]http://relativeimportance.davidson.edu/

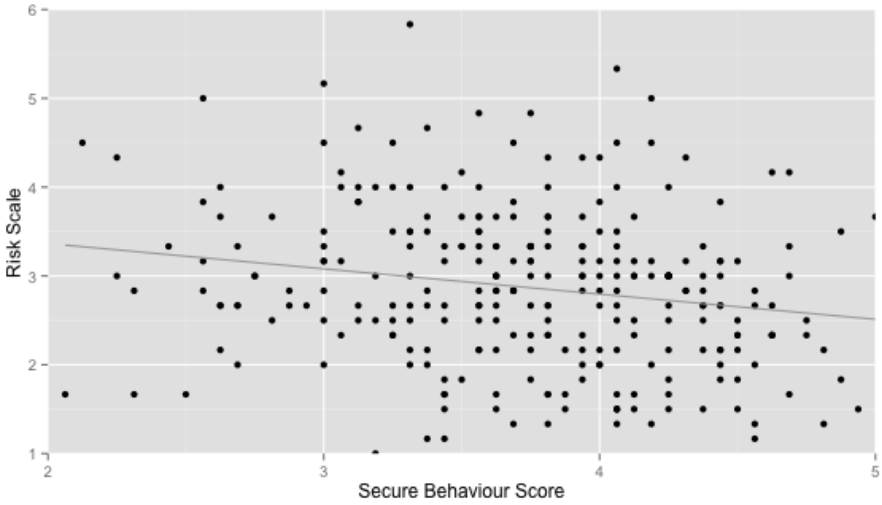


Figure 5.9: Scatterplot of risk scores and security behaviour scores

indicate that the combination of these nine variables were able to explain around 60% of the variance in behaviour scores (R^2 = .60); the most important variables being Knowledge (Relative Weight = .19), Social Motivation (Relative Weight = .13), Confidence (Relative Weight = .08), and Personal Motivation (Relative Weight = .06)—accounting for 19%, 13%, 8%, and 6% of independent variance in behaviour scores respectively.

Table 5.5: Relative weights of factors

Factor	Relative Weight (R^2)
Original	
Knowledge	.19
Social Motivation	.13
Confidence	.08
Personal Motivation	.06
New	
Feminine Bem	.04
Other Interest	.03
Masculine Bem	.02
Self Interest	.02
Risk	.02

To test the results of the Relative Weight Analysis using a regression model, we created two models. The first inputting all nine variables (the same ones we entered

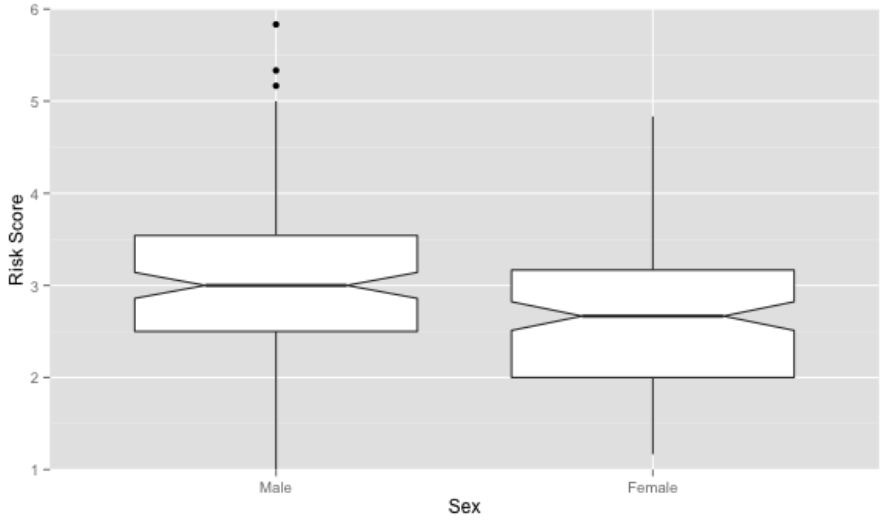


Figure 5.10: Male and female risk scores

in the Relative Weight Analysis) into the model using the hierarchical method, in order of weighted importance (relative importance derived from the Relative Weight Analysis). The second model we will input only the four variables highlighted as most important by the Relative Weight Analysis. We expect that the additional variables found in the first model will only make a trivial difference in explained variance when compared to the second model containing the most important predictors. We find that this is the case. The first model (all predictors included) accounts for 60% of the total variance in behaviour scores F (9, 266) = 44.64, $p < .001$, $R^2 = .60$, $R^2_{\text{ADJUSTED}} = .59$. The second model (only those factors highlighted by the Relative Weight Analysis) accounts for 57% of total variance in behaviour scores, F (4, 271) = 89.14, $p < .001$, $R^2 = .57$, $R^2_{\text{ADJUSTED}} = .56$.

Our results indicate that, between our variables, our original variables were the most important indicators of security behaviour. This is not entirely unexpected as the original variable as specifically use language that relates to security behaviour in the first place, whereas, the new scales that were added for the second study did not directly reference security behaviour. That is not to say however that the information gained is irrelevant; the study still highlights that even general personality traits may have an influence on security behaviour that needs to be accounted for.

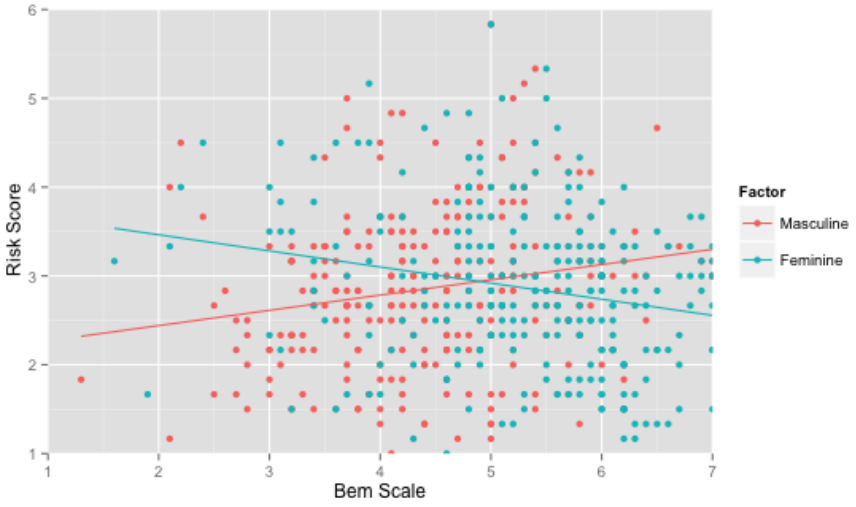


Figure 5.11: Scatterplot of Bem scales and risk scores

5.7 Summary

We found support for our first hypothesis (**H1**): the feminine sub-scale of the Bem sex role inventory showed a stronger relationship with participants' motivation scores compared to the masculine sub-scale. Further, we found that the feminine sub-scale also showed a stronger relationship with security behaviours than the masculine sub-scale, lending support to our second hypothesis (**H2**). These results indicate that there are certain characteristics measured within the feminine Bem scale that are more likely to be found in people who exhibit secure computer behaviour.

We find support for **H3** insomuch as there were significant relationships between self-interest and other-interest scales (**H3a**) and, further, the other-interest scale exhibited a stronger relationship with participants' behaviour scores than the self-interest scale (**H3b**). Participants who are more pro-social were more likely to report secure computer behaviours.

Finally, we find support for our hypothesis regarding risk (**H4**). We found that participants that were more prone to taking risk were less likely to report behaving securely. Further, post-hoc analysis found that males had a higher propensity to take risks than females. This finding was also mirrored when we investigated participants' scores on the masculine and feminine Bem scales and participants' propensity to take

risk, such that the masculine scale showed a stronger relationship with a propensity to take risks than the feminine scale.

Chapter 6

Discussion and conclusion

6.1 Summary

The aim of the current research was to look at the ways in which people's individual differences affects their computer security behaviour. We focused on five main areas: knowledge surrounding computer security issues, confidence in enacting secure behaviours, motivation to enact secure behaviours, propensity to take risks, and the exhibition of sex-typed characteristics (masculine and feminine).

In Study One, we created a survey to look at how participants' knowledge, confidence and motivation impact their security behaviour. Analysis of our data indicated that participants' knowledge of security threats and preventative measures had the most impact on final reported security behaviour. That is, the more participants knew, the more likely they were to be secure. We also found significant relationships between participants' confidence scores and their behaviour, as well as their motivation and behaviour. During our analysis, we uncovered differences between males and females with respect to motivation to perform secure behaviours, such that females were more motivated than males. We also found that females were more likely to report behaving securely with regard to preventative security behaviours (e.g., ensuring that software updates were completed in a timely manner). Furthermore, participants that were more socially motivated to perform security behaviours were more likely to report performing secure behaviours.

We followed up with a second online survey. In Study Two, we asked participants to complete the same survey as in Study One; however, we included three existing psychological scales. We added a risk measure to assess the relationship between participants' propensity to take risk and their security behaviour. Following up on the finding from Study One that indicated social motivation was a better indicator of security behaviour than personal motivation, we added a measure that assessed

Table 6.1: Summary of hypotheses

Hypotheses	Supported/Not Supported
Study One	
H1: Higher scores on the Security Potential measure would be positively correlated with increased security behaviour.	Supported
H2a: Higher scores on the knowledge measure would be positively correlated increased security behaviour.	Supported
H2b: Higher scores on the motivation measure would be positively correlated increased security behaviour.	Supported
H2c: Higher scores on the confidence measure would be positively correlated increased security behaviour.	Supported
H3: No difference between males and females with regard to computer security scores.	Not supported; females had higher security behaviour scores
Study Two	
H1: Feminine scale will show a stronger relationship to security motivation than the masculine scale.	Supported
H2: Feminine scale will show a stronger relationship to security behaviour than the masculine scale.	Supported
H3a: Both self- and other interest will be positively correlated with security behaviour.	Supported
H3b: Other-interest will show a stronger relationship with security behaviour than self-interest.	Supported
H4: Security scores will show a negative relationship with respect to risk scores.	Supported

participants' degree of self-interest or interest in others. The final measure was a sex role inventory that assessed the degree to which participants identified with sex-typed characteristics from a masculine and feminine scale—this enabled us to investigate the sex differences found in Study One and in the preliminary study.

Results from Study Two mirrored our first with respect to knowledge, confidence, and motivation. That is, they all showed significant relationships with participants'

reported security behaviours. Further, we found that risk was also significantly correlated with security behaviour, such that, participants with a greater propensity to take risk were less likely to report behaving securely. In addition, we found that there were distinct sex difference in risk taking—males were more likely to take risks that females; as well as differences with our sex role scales—the masculine scale showed a positive relationship with propensity to take risk (i.e., the higher participants scored on the masculine scale, the more likely they were to take risks), while the feminine scale showed the opposite relationship (participants that scored higher on the feminine scale were less likely to take risks). Further analysis found that while there was no sex difference found in Study Two with respect to security behaviour, we did find significant differences between the masculine and feminine scales and their relationship to security behaviour. The feminine scale was a better predictor of security behaviour than the masculine scale. Table 6.1 summarises our hypotheses from both studies and whether we found support for them.

6.2 Factors

Our research question asked: *what personality characteristics and factors affect participants' security behaviour?* As such, we identify the following factors (in order of influence) as having an impact:

6.2.1 Knowledge

Overall, our research found that participants' knowledge of the issues surrounding computer security (both threats and protectives measure) was the strongest predictor of reported security behaviour. This result agrees with the literature concerning the effect of education on security behaviour, such that, improving users' understanding of their security systems has an impact on their ability to perform in a secure manner [4, 55,94]. Further, these results support Dinev and Hu's [25] model of security behaviour that finds awareness of technology, described by the authors as a, "...user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them", as a key determinant of acceptance and implementation of security measures. This finding is not entirely unexpected—it stands to reason that the more

knowledge participants have regarding security issues, the more likely they are to implement at least *some* security measures.

Our results also speak to the importance of implementing education plans within organisations. Albrechtsen and Hovden [4] showed improved user security behaviour by opening up dialogue between users within an organisation, as well as educating them via the use of workshops—our findings highlight the importance of security education as one of the most effective ways to improve users' behaviour. This education not only refers to exposing users to protective strategies, but also to helping them understand, at some level, how such protective strategies work. For no matter how easy one makes it for users to be secure, one also has to ensure that users harbour the correct mental models [94], as well as knowing the limitations of any protective measure so that the users know exactly when they may be exposed to risk [35].

Our results found that user knowledge and user confidence were related, such that, participants showing a higher degree of knowledge were also more likely to report as being more confident in their ability to perform secure behaviours. This result seems intuitive; it makes sense that users with a deeper understanding of possible threats, and knowledge of ways to protect against them, would feel more confident in their ability to perform secure behaviours. This finding further highlights how knowledge can impact security behaviour, as improving user confidence has been shown to have a direct impact on improved security behaviour [46, 59, 72].

6.2.2 Motivation

Our research indicates that motivation is significantly related to users' security behaviour. We found that both personal motivation and social motivation were significantly correlated with security behaviour. Further, we found that users who reported greater levels of social motivation were more likely to engage in secure behaviours. We found this result in general terms (with the measure of other-interest), as well as in domain specific terms (with our social motivation sub-scale). Our results are in line with previous research that indicates motivation is a significant factor in users' security behaviour [32]. Further, our research agrees with previous studies in finding that social motivation is an influencing factor on security behaviours [5, 80]; however,

it is not fully understood whether the social motivations driving these security actions are, at their core, altruistic or self-interested in nature. For example, Anderson and Argawal's example [5] that users may act securely because they fear passing on a virus via an email attachment could be understood in terms of altruistic prosocial behaviour, or in terms of self-interested behaviour, motivated by one's social standing. Gabriel *et al.* [38] found that *altruism* was significantly related to security behaviour so there may be merit in this line of thought. Furthermore, these results fit in with previous findings that subjective norms are an influencing factor in determining security behaviour [46, 68].

Understanding that motivation impacts users' security behaviour is only a small part of the picture. We have to be cognisant of the possible factors that affect users' motivations to begin with, for example, these could be risk related, reward related, financial or time related. Having a clear picture of these factors is difficult because the model, and its inter-related factors, quickly becomes complicated; however, understanding that these factors *do* have an influence is important for researchers so that they can control or measure these factors to take them into account.

Our analysis found that females were more motivated to behave in a secure manner than males, and that the feminine Bem scale was a better predictor of motivation than the male Bem scale. We argue that many characteristics encompassed by the feminine Bem scale are characteristics that are related to prosocial behaviours. For example, *'Understanding to the needs of others'*, and, *'Compassionate'*, these, and other items on the feminine scale, relate to a sensitivity toward others which, we believe, translates into this socially motivated security behaviour.

Implications of this finding are hard to draw—the way in which traditional sex-typed traits are slowly being re-appropriated by both sexes (e.g., it is much more socially acceptable now for males to show a more sensitive side, traditionally thought of as feminine, than it was twenty years ago), may over time make such findings obsolete. However, at the moment, the relationship of these characteristics to security behaviour warrant further exploration. For example, certain characteristics within the scales (both masculine or feminine) may be more strongly related to security

behaviour than others. As an hypothetical example, this re-appropriation of characteristics may lead to some persons exhibiting characteristics from both the masculine and feminine scale that are highly correlated with insecure behaviour, As such, it would serve to be able to identify these persons so that they may be supported, if possible, in improving their security behaviour.

6.2.3 Confidence

Participants' confidence in their ability to complete security tasks was positively related to their security behaviour, that is, the more confident participants were in completing security behaviours, the more likely they were to perform them. This is in agreement with previous research on self-efficacy and indicates that by increasing users' confidence in their ability to perform secure actions may result in increased security behaviour (assuming that they have the required knowledge to start with) [46, 59, 72]. These results are also in agreement with the predictive model created by Ng *et al.* [67]. We have already discussed the relationship between confidence and knowledge, such that increasing users' knowledge may result in increased confidence; therefore, it starts to become apparent that these three factors are closely related—greater knowledge affects security behaviour, but it may also inspire confidence which, in turn can result in increased security behaviours providing that users have the required knowledge. Further research into how these three factors are related would be of interest. For example, does improving confidence in an area in which a user has knowledge improve the likelihood that the user will then proceed to want to improve their knowledge of other areas? That is, can confidence influence further knowledge? These findings have organisational implications in that they speak to the efficacy of employee and user training: by improving employee confidence in their ability to use security measures, it may be possible to improve organisations' security overall. These training sessions would likely improve users' overall knowledge of security protocols, thus in turn increasing their confidence also.

6.2.4 Risk

We found that participants' propensity to take risk was related to security behaviour, such that, participants that were more risk-averse were also more likely to report secure behaviour. Our post-hoc analysis indicated that males were more likely to take risks than females. Further, analysis uncovered that risk was positively related to the masculine Bem scale (higher masculine score indicated a greater propensity to take risk); and negatively related to the feminine Bem scale (higher femininity score indicated a propensity to be more risk-averse). Our results are in line with the general literature on risk in that males are seen as more prone to take risks than females (e.g., [28, 44]); as well as the literature with regard to computer security and risk, such that, risk perception [33] and risk taking behaviour [27] are related to user security behaviours.

Analysing user risk behaviour is often done through an economic lens. Each user is assumed to make cost/benefit decisions with respect to their available resources and the potential payoff of making such decisions. While this view accounts for the types of variables that may moderate risk-taking actions in users, it does not account for the individual differences within users. We argue that understanding users' propensity to take risk gives us a base level to start from—some users are naturally more likely to take risks, or make decisions that are insecure. Understanding this difference enables researchers adequately assess the impact of other variables and their affect on behaviour. For example, it would be interesting to see if education and training with regard to computer security, over an extended period of time, reduces users' propensity to take risk as well as their insecure behaviour. This would only be possible by knowing users' baseline risk propensity level for comparison.

6.2.5 Sex and sex-typed characteristics

The results from our analysis using the Bem masculinity and femininity scales were interesting. With regard to security behaviour, we found that these scales were better indicators of security behaviour than relying on sex alone. We also found that they showed significant relationships with risk, motivation and confidence: high propensity to take risk was strongly associated with the masculine scale; motivation was

associated to a greater degree with the feminine scale; confidence was associated to a greater degree with the masculine scale. The literature surrounding sex and security behaviour has been mixed, with some researchers finding sex differences [51, 76], whilst others found none [57, 65]. We argue that any difference hypothetically present would be socially constructed one, not a genetically caused one and, as such, it necessitates looking toward sex-typed characteristics as the expression of idealised gender expression, rather than looking at sex alone.

We understand that comparing sex to the sex role inventory is not a straightforward comparison. The sex role inventory comprises of a set of characteristics that, according to Western standards, are socially desirable; however, these characteristics, especially in the case of the masculine scale, may also be characteristics that account for insecure behaviours. It is clear that not every male will embody the masculine characteristics or every female the feminine ones; if that were the case we would see a significant difference in security behaviour when we look at sex alone.

As previously discussed, if we are able to refine this measure to understand exactly which characteristics are responsible for the largest variance in security behaviour, it may be possible to target groups of individuals that are most likely to possess characteristics that relate to those insecure behaviours. It would then be possible to provide them with security training and education. For example, it may be that the characteristics that are responsible for the most variance in security behaviours are few; extracting these variables would enable reduction in size of the measure as well as increasing its efficacy and deployment.

6.3 Preliminary study

Our preliminary study found that risk propensity was related to both security behaviour and the masculine Bem scale. Contrary to existing literature, we did not find a relationship between the feminine Bem scale and risk. However, Study Two is in line with the literature, such that, higher scores on the masculine Bem scale are associated with a greater propensity to take risk, whilst higher scores on the feminine Bem scale are associated with greater risk-averseness.

Our preliminary study was not able to associate the masculine or feminine scales

with security behaviour. Study Two used an improved security behaviour measure and was able to show these relationships directly, such that both the masculine Bem scale and the feminine Bem scale were associated with increased security behaviour; however, the feminine scale indicated a stronger relationship overall.

6.4 Limitations

The main limitation with the current study is that we use a self-report measure of security behaviour. Criticisms of self-reported behaviour measures are generally argued from the point that participants often do not behave the same way in real life that they report on such measures [52]. However, a study by Workman [93] found that strong relationship between self-reported behaviour and actual behaviour (correlation of .89). This indicates that 79% of the variance in actual behaviour was explainable by self-reported behaviour, as such, arguments as to the validity of self-reported behaviour should not be dismissed. Further, though there has been success with assessing users' security behaviour in the wild [57], the methodology involved is not easily deployable and is cost prohibitive. A such, we acknowledge this limitation, whilst understanding that it is the norm within usable security research at the current time.

Our collection of data was via the online CrowdFlower service. As part of our collection protocol, we allowed participants to remain anonymous and did not ask them any sensitive information. Donaldson *et al.* [26] would argue that this anonymity, confidentiality and lack of sensitive questioning would be enough to reduce participants' need to provide socially desirable answers, thus reducing bias towards providing socially desirable 'secure' answers.

We acknowledge the limitations that may arise due to online collection of data. For example, it has been suggested that participants may be susceptible to decreased attention due to completing other tasks at the same time [62], or that participants may feel less accountable when completing tasks [54]; however, comparisons of manually collected data and online data have found that there are no significant differences in the data collected [90]. We are also aware of the limitations in using online services such as CrowdFlower and Amazon's Mechanical Turk. To compensate, we applied

filters and removed participants that we felt may have 'gamed' the system; however, due to the inherent anonymity of such research methods, we cannot be 100% certain that every case has been excluded from our data. We do believe, however, that the sample sizes within our studies would have adequately balanced out this noise within the data. Further, we acknowledge that results may not be generalisable at this time without further research comparing the population samples recruited from CrowdFlower to the general population.

6.5 Recommendations

We understand that it is not practical, or desirable, to ask respondents a battery of questions regarding risk, confidence, sex roles, motivation, and so forth, when conducting computer security research. However, we feel that the current research highlights the fact that asking too few questions regarding the individual differences between participants may be detrimental to the thorough interpretation of research results. For example, in small lab-based user studies (that can be prone to a lack of diversity in participants), understanding if participants have a propensity to exhibit insecure behaviours may enable researchers to control for these characteristics, or at least interpret their data with sensitivity to them. Having a measure that is able to provide researchers with basic information regarding personality factors that affect security behaviour would enable researchers to interpret their data more comprehensively. We look to the design of the Myers-Briggs as an example of the type of output (rather than content) we could hope to see from such a measure. For example, after administering such a measure, a researcher may find that a participant has high confidence, high risk propensity, average knowledge and low motivation. Understanding how these factors interact and interpreting such interactions' effects on security behaviour would be a useful measure in the researchers' toolbox.

In a broader sense, our research highlights the fact that the three main factors that influence security behaviour are factors that education might improve. We found that knowledge, motivation, and confidence were the most important factors, and further, that knowledge and confidence were highly related. Educating users may in turn provide them with more confidence to carry out secure computer behaviours

and thus improve their security overall. We note that education should go beyond prescriptive lists of dos and don'ts and should instead aim to improve users' mental models and critical thinking skills relating to security, so that they are better prepared to handle new risks that arise. Changing a user's motivation may be harder; however, research indicates that participants' degree of self- and other-interest can be fluid and change depending on the situation at hand [40]. Further, via integration of persuasive technologies into security systems it may be possible to change the way users' are motivated to perform needed but less desirable tasks [83].

Following from these points, we make the following recommendations:

R1 When collecting research data that assesses security behaviour, security researchers should include instruments to adequately assess personal characteristics that influence computer security behavioural outcomes. Doing so allows for more comprehensive interpretation of data and provides the ability to control for such factors.

R2 Development of a single scale to measure respondents' security potential could aid in identifying individuals that fall into a high risk category. Clearly not everyone falling into this category would exhibit insecure behaviours; however, it would serve as a good benchmark. This tool would enable researchers to better understand their participants. Further, it may be a useful aid for organisations and service providers to enable them to provide targeted security training to those users in need.

6.6 Future work

In future work, we would like to refine some of the measures used in the current research. That is, we would like to identify items within each of the scales that provide good predictive power so that we can refine and reduce the items to a single workable measure. We believe that the Security Potential Score (combining knowledge, motivation and confidence) was a strong indicator overall of security behaviour (better than any single measure alone); however, it is too long to be used as a quick assessment tool in research studies. Further, we would like to add elements from psychological

the scales that did not originally make up the Security Potential score to provide with a more holistic approach to understanding participants' propensity act securely.

6.7 Conclusion

This thesis explored the potential factors that impact a users' computer security behaviour. We iteratively developed a survey of factors influencing secure behaviour based on previous literature and input from experts. We administered this survey to 650 participants across two studies and performed statistical analysis to identify relationships between the factors and secure behaviour.

We identified five main factors: knowledge, motivation, confidence, propensity to take risk, and sex-typed characteristics. We found that, to some extent, all of these factors had a role to play in the behavioural outcomes of participants with regard to computer security; however the largest determinant of security behaviour was users' knowledge regarding security threats and how to protect against them.

We argue that by educating users in regard to specific threats, not only do we provide those users with the information they need to successfully defend against the threat, but we also enhance their confidence in performing those security behaviours. Our research has shown that an understanding of users' individual differences can play a role in determining their security behaviour—these differences include the users' propensity to take risk, their motivation and even their affinity to certain sex-typed characteristics. Researchers should fully consider these factors when interpreting the results of usable security studies.

Bibliography

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] Icek Ajzen. The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2):179–211, 1991.

[3] Eirik Albrechtsen. A qualitative study of users' view on information security. *Computers & security*, 26(4):276–289, 2007.

[4] Eirik Albrechtsen and Jan Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4):432–445, 2010.

[5] Catherine L Anderson and Ritu Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613–643, 2010.

[6] Nalin Asanka, Gamagedara Arachchilage, and Steve Love. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38(0):304 – 312, 2014.

[7] Kregg Aytes and Terry Connolly. Computer security and risky computing practices: A rational choice perspective. *Advanced Topics In End User Computing*, 4:257, 2005.

[8] Kregg Aytes and Terry Conolly. A research model for investigating human behavior related to computer security. *AMCIS 2003 Proceedings*, page 260, 2003.

[9] Albert Bandura. Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2):191, 1977.

[10] Adam Beautement, Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, pages 47–58. ACM, 2009.

[11] Sandra Bem. *Bem Sex-Role Inventory: Professional Manual*. Consulting Psychologists Press, 1981.

[12] Bruce L Bowerman and Richard T O'Connell. *Linear statistical models: An applied approach*. PWS-Kent Boston, 1990.

[13] Schneier Bruce. Secrets and lies: Digital security in a networked world. *New York. John Wiley & Sons Inc. ISBN: 0-471-25311-1*, 4:100–15, 2000.

[14] Z Byrne, J Weidert, J Liff, M Horvath, C Smith, A Howe, and I Ray. Perceptions of internet threats: Behavioral intent to click again. In *Proceedings of the 27th Annual Conference of the Society for Industrial and Organizational Psychology*, 2012.

[15] Jean Camp, Farzaneh Asgharpour, and Debin Liu. Experimental evaluations of expert and non-expert computer users' mental models of security risks. *Proceedings of WEIS 2007*, 2007.

[16] Simon Cassidy and Peter Eachus. Developing the Computer User Self-efficacy (CUSE) scale: Investigating the relationship between computer self-efficacy, gender and experience with computers. *Journal of Educational Computing Research*, 26(2):133–153, 2002.

[17] Yan Chen, K Ramamurthy, and Kuang-Wei Wen. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3):157–188, 2012.

[18] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *Usenix Security*, volume 6, 2006.

[19] Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags. It's all about the Benjamins: An empirical study on incentivizing users to ignore security advice. In *Financial Cryptography and Data Security*, pages 16–30. Springer, 2012.

[20] Deborah R Compeau and Christopher A Higgins. Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, pages 189–211, 1995.

[21] CrowdFlower. Crowdflower job settings guide. `https://success.crowdflower.com/hc/en-us/articles/201855719-Job-Settings-Guide-to-Basic-Job-Settings-Page`. Accessed: February 11, 2015.

[22] Cyveillance. The cost of phishing: Understanding the true cost dynamics behind phishing attacks. `http://docs.apwg.org/sponsors_technical_papers/WP_CostofPhishing_Cyveillance.pdf`. Accessed: 28th February, 2015.

[23] Fred D Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, pages 319–340, 1989.

[24] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 581–590. ACM, 2006.

[25] Tamara Dinev and Qing Hu. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7):23, 2007.

[26] Stewart I Donaldson and Elisa J Grant-Vallone. Understanding self-report bias in organizational behavior research. *Journal of Business and Psychology*, 17(2):245–260, 2002.

[27] Serge Egelman and Eyal Peer. Scaling the security wall. In *Computer Human Iinteraction (CHI) 2015*. ACM, 2015.

[28] Helga Fehr-Duda, Manuele De Gennaro, and Renate Schubert. Gender, financial risk, and probability weights. *Theory and Decision*, 60(2-3):283–313, 2006.

[29] Andy Field. *Discovering statistics using IBM SPSS statistics*. Sage, 2013.

[30] Joseph L Fleiss. Measuring nominal scale agreement among many raters. *Psychological Bulletin*, 76(5):378, 1971.

[31] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, pages 657–666. ACM, 2007.

[32] Donna L Floyd, Steven Prentice-Dunn, and Ronald W Rogers. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2):407–429, 2000.

[33] Batya Friedman, David Hurley, Daniel C Howe, Helen Nissenbaum, and Edward Felten. Users' conceptions of risks and harms on the web: a comparative study. In *CHI'02 Extended Abstracts on Human Factors in Computing Systems*, pages 614–615. ACM, 2002.

[34] S.M. Furnell, P. Bryant, and A.D. Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410 – 417, 2007.

[35] Steven Furnell. End-user security culture: a lesson that will never be learnt? *Computer Fraud & Security*, 2008(4):6–9, 2008.

[36] Steven Furnell and Anish Rajendran. Understanding the influences on information security behaviour. *Computer Fraud & Security*, 2012(3):12 – 15, 2012.

[37] Steven Furnell, Valleria Tsaganidi, and Andy Phippen. Security beliefs and barriers for novice internet users. *Computers & Security*, 27(7):235–240, 2008.

[38] Trevor Gabriel and Steven Furnell. Selecting security champions. *Computer Fraud & Security*, 2011(8):8 – 12, 2011.

[39] V Garg and LJ Camp. Risk characteristics, mental models, and perception of security risks. In *ASE Conference 2014*. Academy of Science and Engineering, USA, 2014.

[40] Margaret E Gerbasi and Deborah A Prentice. The self-and other-interest inventory. *Journal of Personality and Social Psychology*, 105(3):495, 2013.

[41] Nathaniel Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan. Stopping spyware at the gate: a user study of privacy, notice and spyware. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, pages 43–52. ACM, 2005.

[42] Mark Grimes, Jim Marquardson, and Jay Nunamaker. Broken windows, bad passwords: Influencing secure user behavior via website design. In *Twentieth Americas Conference on Information Systems*, 2014.

[43] The Stricture Group. Top 100 adobe passwords with count top 100 adobe passwords with count top 100 adobe passwords with count. `http://stricture-group.com/files/adobe-top100.txt`. Accessed 26 February, 2015.

[44] Per E Gustafson. Gender differences in risk perception: theoretical and methodological perspectives. *Risk analysis*, 18(6):805–811, 1998.

[45] SM Taiabul Haque, Shannon Scielzo, and Matthew Wright. Applying psychometrics to measure user comfort when constructing a strong password. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[46] Tejaswini Herath and H Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009.

[47] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New security Paradigms*, pages 133–144. ACM, 2009.

[48] Incapsula. What DDOS attacks really cost businesses. `http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf`. Accessed: 26 Feb 2015.

[49] Ponemon Institute. 2014 cost of data breach study. `http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/`. Accessed: 08 October, 2014.

[50] Blake Ives, Kenneth R Walsh, and Helmut Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75–78, 2004.

[51] Tom N Jagatic, Nathaniel A Johnson, Markus Jakobsson, and Filippo Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007.

[52] Carlos Jensen, Colin Potts, and Christian Jensen. Privacy practices of internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63 (1-2)(1-2):203–227, July 2005.

[53] Jeff W Johnson. A heuristic method for estimating the relative weight of predictor variables in multiple regression. *Multivariate Behavioral Research*, 35(1):1–19, 2000.

[54] John A Johnson. Ascertaining the validity of individual protocols from web-based personality inventories. *Journal of Research in Personality*, 39(1):103–129, 2005.

[55] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[56] Hazel Lacohée, Andrew D Phippen, and Steven M Furnell. Risk and restitution: assessing how users establish online trust. *Computers & Security*, 25(7):486–493, 2006.

[57] Fanny Lalonde Levesque, Jude Nsiempba, José M. Fernandez, Sonia Chiasson, and Anil Somayaji. A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 97–108, New York, NY, USA, 2013. ACM.

[58] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *Biometrics*, pages 159–174, 1977.

[59] Robert LaRose, Nora J. Rifon, and Richard Enbody. Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3):71–76, March 2008.

[60] Huigang Liang and Yajiong Xue. Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7):394–413, 2010.

[61] Winter Mason and Siddharth Suri. Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, 44(1):1–23, 2012.

[62] Adam W Meade and S Bartholomew Craig. Identifying careless responses in survey data. *Psychological Methods*, 17(3):437, 2012.

[63] Ree M. Meertens and René Lion. Measuring an individual's tendency to take risks: The risk propensity scale. *Journal of Applied Social Psychology*, 38 (6)(6):1506–1520, 2008.

[64] Scott Menard. *Applied logistic regression analysis*, volume 106. Sage, 2nd edition, 2002.

[65] George R Milne, Lauren I Labrecque, and Cory Cromer. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3):449–473, 2009.

[66] Gary C Moore and Izak Benbasat. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2(3):192–222, 1991.

[67] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie Xu. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4):815 – 825, 2009.

[68] Boon-Yuen Ng and Mohammad Rahim. A socio-behavioral study of home computer users' intention to practice security. *PACIS 2005 Proceedings*, page 20, 2005.

[69] Jum Nunnally. *Psychometric theory*. New York: McGraw-Hill, 1978.

[70] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42:165–176, 2014.

[71] Paul A Pavlou and Mendel Fygenson. Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS Quarterly*, pages 115–143, 2006.

[72] Hyeun-Suk Rhee, Cheongtag Kim, and Young U Ryu. Self-efficacy in information security: its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, 2009.

[73] Ronald W Rogers. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1):93–114, 1975.

[74] Irwin M Rosenstock. The health belief model and preventive health behavior. *Health Education & Behavior*, 2(4):354–386, 1974.

[75] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 2. ACM, 2010.

[76] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie 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*, pages 373–382. ACM, 2010.

[77] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security*, 2015.

[78] Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. Analysis of end user security behaviors. *Computers & Security*, 24(2):124 – 133, 2005.

[79] Patryk Szewczyk and Steven Furnell. Assessing the online security awareness of Australian internet users. In *Proceedings of 8th Annual Security Conference*, pages 58–1 to 58–9, 2009.

[80] John F Tanner Jr, James B Hunt, and David R Eppright. The protection motivation model: A normative model of fear appeals. *The Journal of Marketing*, pages 36–45, 1991.

[81] Shirley Taylor and Peter Todd. An integrated model of waste management behavior a test of household recycling and composting intentions. *Environment and Behavior*, 27(5):603–630, 1995.

[82] Scott Tonidandel, James M LeBreton, and Jeff W Johnson. Determining the statistical significance of relative weights. *Psychological Methods*, 14(4):387, 2009.

[83] Tammy Toscos, Anne Faber, Shunying An, and Mona Praful Gandhi. Chick clique: persuasive technology to motivate teenage girls to exercise. In *CHI'06 extended abstracts on Human Factors in Computing Systems*, pages 1873–1878. ACM, 2006.

[84] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo

Bauer, Nicolas Christin, and Lorrie Faith Cranor. How does your password measure up? The effect of strength meters on password creation. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, pages 5–5, Berkeley, CA, USA, 2012. USENIX Association.

[85] Joop van der Pligt. Risk perception and self-protective behavior. *European Psychologist*, 1(1):34, 1996.

[86] Viswanath Venkatesh and Fred D Davis. A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science*, 46(2):186–204, 2000.

[87] Viswanath Venkatesh, Michael G Morris, Gordon B Davis, and Fred D Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, pages 425–478, 2003.

[88] Rossouw Von Solms and Basie Von Solms. From policies to culture. *Computers & security*, 23(4):275–279, 2004.

[89] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[90] Arne Weigold, Ingrid K Weigold, and Elizabeth J Russell. Examination of the equivalence of self-report survey-based paper-and-pencil and internet data collection methods. *Psychological Methods*, 18(1):53, 2013.

[91] Alma Whitten and J Doug Tygar. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Usenix Security*, volume 1999, 1999.

[92] Jacob O Wobbrock, Leah Findlater, Darren Gergle, and James J Higgins. The aligned rank transform for nonparametric factorial analyses using only ANOVA procedures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 143–146. ACM, 2011.

[93] Michael Workman. Gaining access with social engineering: an empirical study of the threat. *Information Systems Security*, 16(6):315–331, 2007.

[94] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *Anti-Phishing Working Group (APWG) eCrime Researchers Summit*, pages 1–11. IEEE, 2013. Conference Papers.

[95] George Kingsley Zipf. *Human behavior and the principle of least effort.* Addison-Wesley Press, 1949.

Appendix A

CrowdFlower recruitment notice

Carleton UNIVERSITY
Canada's Capital University

Research Ethics Board
1325 Dunton Tower
Tel: 613-520-2517
ethics@carleton.ca

Recruitment Notification on CrowdFlower

I am a Master's student and Human-computer Interaction researcher from Carleton University (Ottawa, Canada), working under the supervision of Dr. Sonia Chiasson.

Our goal is to understand how everyday end-users protect themselves online. This survey asks about your experiences with regard to online security.

Filling out this anonymous survey should take approximately 15 minutes and will be rewarded with a payment $0.50.

Participants must be at least 18 years of age, fluent in English and use a computer that uses Microsoft Windows as their main computer.

This project has been reviewed and cleared by the Carleton University Research Ethics Board +1-613-520-2517 or ethics@carleton.ca.

Appendix B

Consent form

Carleton UNIVERSITY
Canada's Capital University

Questionnaire/Survey Online Consent Form

Title: Investigation of Factors Relating to Users' Computer Security Behaviours

Funding Source: NSERC Discovery

Date of ethics clearance: 17 February 2015

Ethics Clearance for the Collection of Data Expires: 31 May 2015

Our goal is to understand how everyday end-users protect themselves online. This survey asks about your experiences with regard to online security. The researcher for this study is Matthew Hull in the School of Information Technology at Carleton University. He is working under the supervision of Dr. Sonia Chiasson in the School of Computer Science.

This study involves one 15 minute survey that will take place online. You will be paid $0.50 for your participation.

There are no known personal or physical risks associated with this survey. If you are uncomfortable discussing the topic of computer security, we recommend that you do not participate in this survey.

You have the right to withdraw from the survey at any time, for any reason, up until you hit the "submit" button. You can withdraw by exiting the survey at any time before completing it. If you withdraw from the study, all information you provided will be immediately destroyed. As the survey responses are anonymous, it is not possible to withdraw after the survey is submitted.

All research data will be password protected. The company running the online survey is Crowdflower, based in the United States of America. As the survey responses will be stored on US servers, the data may be subject to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act, H. R. 3162, 107th Cong. (2001).

The survey company will keep a copy of the survey responses on its servers in the United States. This data will be deleted from our Crowdflower account once data collection is complete.

Research data will only be accessible by the researcher (Matthew Hull) the research supervisor (Dr. Sonia Chiasson) and the survey company. The survey company may

associate your IP and location (city) with the collected data. No further identifying information will be collected and the researchers will not be using this information to de-anonymize participants in any way.

Once the project is completed, all anonymized research data will be kept for five years and potentially used for other research projects on this same topic.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. Should you have questions or concerns related to your involvement in this research, please contact:

REB contact information:
Professor Louise Heslop, Chair
Professor Andy Adler, Vice-Chair
Research Ethics Board
Carleton University
511 Tory
1125 Colonel By Drive
Ottawa, ON K1S 5B6
Tel: 613-520-2517
ethics@carleton.ca

Researcher contact information:
Matthew Hull
School of Information Technology
Carleton University
Email: matthew.hull@carleton.ca

Supervisor contact information:
Dr. Sonia Chiasson
School of Computer Science
Carleton University
Email: chiasson@scs.carleton.ca

By clicking "submit", you consent to participate in the research study as described above.

Appendix C

Survey

Carleton UNIVERSITY
Canada's Capital University

Research Ethics Board
1325 Dunton Tower
Tel: 613-520-2517
ethics@carleton.ca

Questionnaire

Questions (all questions use a 5-point Likert scale)

Questions relating to participants' computer security knowledge:

1. I am aware of at least some of the security threats to personal computer users.
2. Of the security threats that I know about, I am aware of the actions that I need to take to protect my computer.
3. I understand the possible security implications of reusing passwords.
4. I understand why it is important to make passwords as complex as possible.
5. I understand why one should avoid using personal information for the basis of passwords.
6. I understand what the term Phishing means.
7. I understand what the padlock icon in my web browser means when I am connecting to websites.
8. I understand what a website's certificate indicates with regard to computer security.
9. I understand, in a broad sense, the purpose of my computer's firewall.
10. I understand, in a broad sense, the purpose of anti-virus software.
11. I understand the possible security implications of running programs downloaded from unofficial sources.
12. I understand the ways in which malicious software can be unintentionally downloaded to my computer.
13. I understand why it is important to install software updates as soon as possible after they are available.
14. I understand the possible security implications of ignoring software updates.

Questions relating to participants' computer security behaviour:

15. No matter the situation, I always follow computer security advice.
16. When I find out about a security threat, I research ways to protect myself against it.
17. I re-use passwords across different websites.
18. I always try to make my passwords as complex as I can.
19. I sometimes use personal information (e.g., my pet's name) as the basis for passwords.
20. When I am asked to log in to a website, I make sure to check for the padlock icon in my web browser.
21. I always look at the address of a web page to ensure its legitimacy.
22. I always check the certificate of a website if I am unsure about its legitimacy.

23. I made sure I had anti-virus software installed when first setting up my personal computer.
24. I periodically check the status of my anti-virus software.
25. I made sure the firewall was activated when first setting up my personal computer.
26. I would click on an unsolicited pop-up or banner advertisement if it seemed interesting.
27. I only download from websites that I trust.
28. I only click on links in emails if I am sure of the legitimacy of the sender.
29. I always install software updates as soon as I possibly can.
30. If possible, I set my software to install updates automatically.

Questions relating to participants' motivation to perform computer security actions:

31. I would ignore computer security advice if it benefitted me to do so.
32. I may ignore computer security advice if it doesn't benefit me personally.
33. By following computer security advice when possible, society as a whole benefits.
34. I have a responsibility to other people to ensure that I follow computer security advice whenever possible.
35. If I incur a financial cost by following computer security advice then I am less likely to follow the advice.
36. If following computer security advice is time consuming, I am less likely to do it.

Questions relating to participants' confidence in performing computer security actions.

37. I am confident I could secure my data and personal information even if there was no one around to show me.
38. I am confident I could secure my data and personal information even if I hadn't taken similar measures before.
39. I am confident I could secure my data and personal information using only reference materials.
40. I am confident I could secure my data and personal information if I had previously seen someone else complete a similar task.
41. I am confident I could secure my data and personal information if I could call someone to help if I got stuck.
42. I am confident I could secure my data and personal information if someone else helped me get started.
43. I am confident I could secure my data and personal information if I had lots of time.
44. I am confident I could secure my data and personal information if someone showed me how to do it first.
45. I am confident I could secure my data and personal information if I had used similar measures before.

Demographic section

46. What is your age in years? [text box]

47. What is your sex?
    Male
    Female

48. What is the highest level of education you have completed?
    No schooling completed
    Some high school
    High school
    Bachelor's degree
    Master's degree
    Doctoral degree
    Professional degree

49. What is your nationality? [text box]

50. In what country do you currently reside? [text box]

51. What is your profession?
    Administrative Support (e.g., secretary, assistant)
    Art, Writing, Journalism (e.g., author, reporter, sculptor)
    Business, Management and Financial (e.g., manager, accountant, banker)
    Education (e.g., teacher, professor)
    Legal (e.g., lawyer, law clerk)
    Medical (e.g., doctor, nurse, dentist)
    Science, Engineering, and IT professional (e.g., researcher, programmer, IT consultant)
    Service (e.g., retail clerk, server)
    Skilled Labour (e.g., electrician, plumber, carpenter)
    Student
    Unemployed
    Retired
    Other

52. Do you use a computer daily for work?
    Yes
    No

53. Do you own a personal computer?
    Yes
    No

54. On the computer you use most often, is the operating system:

Microsoft Windows
Apple OSX
Linux

55. Please mark on the scale below how much help require or provide when using computers (selecting 1 would indicate you often ask for help whereas selecting 7 would mean others ask you for help):

I often ask for help 1 2 3 4 5 6 7 Others as me for help.

56. Do you have a degree in an IT related field?
Yes
No

57. Have you ever taken a course on computer security?
Yes
No

Appendix D

Additional scales

Carleton UNIVERSITY
Canada's Capital University

Risk Propensity Scale

Participants are asked to respond to the following using a 7-point Likert scale; Strongly disagree to Strongly agree.

1. Safety first
2. I do not take risks with my health.
3. I prefer to avoid risks.
4. I take risks regularly.
5. I really dislike not knowing what is going to happen.
6. I usually view risks as a challenge.
7. I view myself as a…

Risk Avoider 1 2 3 4 5 6 7 Risk Seeker

Self- and Other Interest Scale

Participants are asked to respond to the following using a 7-point Likert scale; Strongly disagree to Strongly agree.

Self-interest subscale

1. I am constantly looking for ways to get ahead.
2. Hearing others praise me is something I look forward to.
3. Doing well in my pursuits is near the top of my priorities.
4. I try to make sure others know about my successes.
5. I look for opportunities to achieve higher social status.
6. Success is important to me.
7. Having a lot of money is one of my goals in life.
8. I keep an eye out for my own interests.
9. I am constantly looking out for what will make me happy.

Other-interest subscale

1. I am constantly looking for ways for my acquaintances to get ahead.
2. Hearing others praise people I know is something I look forward to.
3. I want to help people I know to do well.
4. I try to help my acquaintances by telling other people about their successes.
5. I look for opportunities to help people I know achieve higher social status.
6. The success of my friends is important to me.
7. I look out for ways for my friends to have more money.

8. I keep an eye out for other's interests.
9. It is important to me that others are happy.

Bem Sex-Role Inventory—Short Form

This psychological scale is copyrighted so is unable to be reproduced in this thesis. Further information on the scale can be found here:
http://www.mindgarden.com/products/bemss.htm

Appendix E

Preliminary study

Gender Expression, Risk, and Computer Security

Matthew Hull
Carleton University
Ottawa, Canada
matthew.hull@carleton.ca

Sonia Chiasson
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

***Abstract*—It is understood that people employ different models for assessing and reacting to threats depending on their experience, context, economic judgements and other attributes. As yet, research in usable security has not attempted to understand the way socially constructed attributes of personality such as masculinity and femininity, as opposed to genetic sex, can moderate the way that value judgements are made and their potential effect on users' secure computer behaviour.**

The current study investigates the relationship between participants' propensity to take risk, their exhibition of masculine and feminine traits, and how these constructs affect the way in which secure computer behaviour is implemented or disregarded. Results indicate that there is a relationship between participants' exhibited masculine traits and their propensity to take risk; further, we found that risk-takers were more likely to perceive their general computer security behaviour as less secure than risk-avoiders. Post-hoc analysis indicates positive relationships between participants' perceptions of general computer security behaviour and their self-reported security behaviours.

I. Introduction

Increases in the usability of security systems are generally promulgated through acts such as teaching a user how to correctly use a system or ensuring the users' mental model of the system is correct. It is clear, however, that the efficacy of these acts have varying degrees of success and are strongly mediated by exosystemic factors [1], [2]. For example, a user's previous experience with similar systems or the value of the assets that they wish to protect may affect a user's experience of using, and value of, a security system. Designing a system to account for a broad spectrum of users' individual differences and experiences can be challenging, as such researchers often endeavour to improve a security system's usability by focusing on areas that tend to see maximum usability improvements across a wide range of users. For example, diminishing the cognitive load of the user so that they may more easily use a system—as can be seen in novel password schemes that leverage the pictorial superiority effect [3]. While these methods can be effective in improving the objective usability of the system, they still do not account for the idiosyncrasies in relation to users' individual differences.

Individual differences that can affect a user's judgement of a security system can be mediated by constructs that are innate in all of us—for example, we may be more willing to disregard a security protocol if we have a propensity for taking risk; or a trusting person may be more likely to share their computer password with a work colleague. These aspects of human personality can account for many of the choices people make, either consciously or unconsciously; however, these differences are yet to be rigorously studied as they relate to usable security. Researchers in the fields of psychology and economics understand that people's individual differences play a significant part in how they make decisions; however, when the research focuses on the differences between sexes, participants are split according to genetic sex and, as a consequence, the underlying personality traits that may cause those 'sex' differences are often ignored.

Examples of sex as predictors of behaviour can be seen in the following examples. In research carried out by Jagatic *et al.*, it was concluded that participants' sex seemed to be a mediating factor in deciding if they were susceptible to phishing attacks—females were found more likely to be at risk (female = 77%, male = 65%) [4]. This finding seems to be in contrast to research conducted by Milne and Lalonde-Levesque *et al.* [5], [6]—both concluding that gender *does not* have an impact on users' risk of infection with viruses or malware. The use of genetic sex as a predictor of behaviour in these cases, however, does not allow for an overarching, multi-faceted view on users' behaviour, but is merely an arbitrary separation of users by genetics.

Research results such as these can be problematic in that they hypothesise that genetic sex is a predictor of behaviour, ignoring the underlying traits that cause these behaviours and, as a consequence, disallow that a trait may be a good predictor of behaviour even if the person displaying this trait is of the opposite sex to which the trait is normally associated. If the possibility to exhibit both masculine and feminine traits is provided, regardless of genetic sex, it is then possible to evaluate the relationship between a person's propensity to perform these traits and their behaviour — independent of the view that these traits only exist when they are situated in a specific and appropriate (to cultural norms) body.

We conducted a questionnaire study looking at this interplay between participants' propensity to take risks, their exhibition of culturally specific masculine and feminine traits, as well as their self-reported secure computer behaviour. The study was conducted online and evaluated participants' exhibition of these constructs in an attempt to identify if there was any relationship between them. 155 participants took part in the study and results suggest gender expression (specifically of masculine traits) has a stronger relationship with risk-taking behaviour than the genetic sex of the individual. Further, levels of risk taking behaviour are related to participants' perceived levels of general security behaviour which, in turn, are related to their self-reported security security behaviours.

II. Background

It seems logical that individual differences could play an important part in a users' perception of, and decision to use, a device or security protocol. Normally, sex-typed individual

differences are thought about only when they are situated within the 'correct' body (e.g., a trait considered masculine exhibited by a male) and, in this context, are a well studied area in psychology.

Traditionally, masculinity and femininity are seen as being at polar ends of a spectrum. More recently though, academics have understood that it is possible for persons to exhibit both masculine and feminine traits concurrently. For example, Bem [7] argues that it is possible for someone to be caring (traditionally thought of as a feminine trait), and at the same time assertive (traditionally thought of as a masculine trait) depending on the situation and context. Expression of these traits are not mutually exclusive—when someone is being 'masculine' it does not mean that at the same time they cannot be 'feminine' [7].

To further explore this problem space, Bem created the sex-role inventory [7]. The inventory helped understand of both sides of the human condition (masculine and feminine) without, as traditional implementations had seen, one negating the other. The inventory is able to provide a score of both masculinity and femininity, regardless of the person's genetic sex and is based upon temporal-cultural definitions of sex-typed 'appropriate' behaviour for the masculine of feminine role—as such, it necessitates the assumption that persons completing the inventory have a reasonably well developed internal construct of what those gender roles are, and how they are externally viewed.

Extensive research into the area of risk and sex has been conducted in various fields—a common theme throughout this research is that males are more likely to engage in risk taking behaviour than females. For example, in a study by Tyler & Lichenstien [8] it was found that male youths were more likely to engage in risk-taking behaviour in respect to drug and alcohol use. Poppen [9] found that in sexual encounters, males were more likely to take risks in partner selection. In a meta-analysis of many risk studies, Byrnes *et al.* [10] concluded that males tend to engage in more risk-taking behaviour than females and, furthermore, this risk taking behaviour tends to be greater at a younger age.

A. Hypotheses

It is clear that there is a complicated relationship between expressions of masculinity and femininity, risk, and security behaviour. From our understanding of the literature, we hypothesise the following:

H1: We expect to see a positive relationship between masculine behavioural traits and risk-taking behaviour, further, this relationship should be stronger than using genetic sex.
H2: We expect to see a negative relationship between risk-taking behaviour and secure computer behaviour.
H3: We expect, as a consequence of H1 and H2, a negative relationship between masculine behavioural traits and security behaviour.

III. Methodology

For this study, a survey was constructed to understand the relationship between participants' exhibition of masculine and feminine traits, risk-taking behaviour, and participants' secure computer behaviour. The survey consisted of an introduction to the study (and consent page), followed by five sections of questions. The questionnaire was created using LimeSurvey[1] and hosted on our research lab's server. As this study dealt with human participants, the study protocol was reviewed and cleared by the Carleton University research ethics board.

TABLE I. Participants' Education Level

Education Level	Number
No High School	—
High School	21
College	31
Undergraduate Degree	53
Graduate Degree	38
Professional Degree	9
No Answer	3

A. Participants

Participants were recruited via email and social media using snowball sampling. Participants were required to be over 18 years of age and fluent in English to take part in the study. The participants ranged in age from 18 years to 77 years (N = 155, M = 33.88, SD = 10.96). 78 Males and 77 females took part in the study. Participants received no compensation, financial or otherwise, for participating.

The participants' educational level is shown in Table I. The distribution of education levels seems reasonable although the percentage of participants with a university degree is still above the national norm. Of the 155 respondents, 143 participants stated that they use a computer daily for work, and 152 participants stated that they own a personal computer—of the three respondents that did not own a computer, all had access to a computer (e.g., at work or as a family computer). 38 of the respondents indicated that they had a degree in an IT related field, thus the study shows a relatively broad range of IT and non-IT professionals.

B. Questionnaire

The survey was broken down in the following way[2]:

1) Demographic questions. These questions included standard demographics such as age and sex.
2) Computer expertise questions. These included participants' education in an IT related field and extent of computer use.
3) Risk-taking inventory questions. This inventory is taken from the work of Meertens & Lion [11] and consists of a set of seven questions designed to provide a non-domain specific measure of risk-taking behaviour. These questions are 7-point Likert items ranging from 1 = 'Strongly disagree' through to 7 = 'Strongly agree'. Items are summative to form a measure of risk.
4) Bem Sex-role Inventory - Short-Form [7]. This inventory measures participants' masculinity and femininity on a culturally-defined scale (i.e., it has items that

[1] https://www.limesurvey.org/

[2] Many items of the questionnaire were reverse coded to ensure participants were actively reading the questions. A standard trust inventory was also administered but this analysis is left to future work.

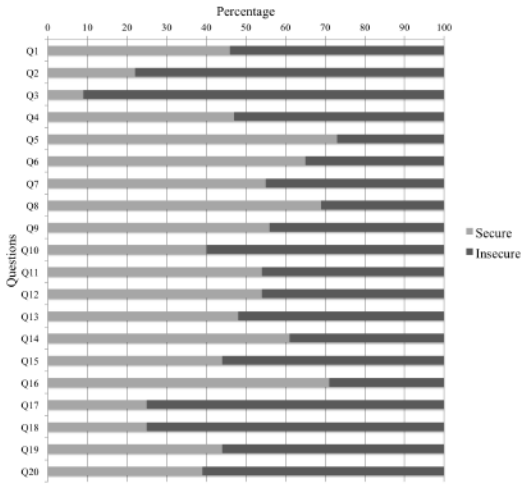


Fig. 1. Participants' responses to secure behaviour questions (as percentage)

are deemed, for example, masculine within a western cultural context), regardless of their sex. It consists of 30 Likert items with a 7-point scale (10 masculine, 10 feminine and 10 neutral) that summate into two scales—one for masculinity and one for femininity (as per Bem [7], neutral answers are disregarded).

5) Security behaviour questions. Participants were asked to respond *agree*, *disagree*, or *N/A*. These questions followed five separate themes, each containing five questions unless otherwise specified. The questions can be seen in Table II.
   a) *Protective behaviour* (Q1-5): measures participants undertake to ensure their computer is protected from harmful actions (e.g., do participants take measures to ensure that their anti-virus is always up-to-date).
   b) *Passwords* (Q6-10): mechanisms users employ to deal with passwords (e.g., do they write down their passwords).
   c) *Connecting with unknown entities* (Q11-15): how participants connect with unknown entities or let unknown entities connect with them (e.g., do they use peer-to-peer networks or connect to open wifi sources).
   d) *Privacy* (Q16-20): measures participants take to protect their privacy (e.g., do they try to limit data collection when visiting websites).
   e) *Perceptions* (Q21-23): participants' general perceptions of their security compliance behaviour (three questions).

IV. Results

As a measure of general security behaviour, we gave participants one point for each 'secure' answer they gave in response to the 20 security behaviour questions (5(a) to 5(d), excluding 5(e)), therefore participants were able to score a theoretical 0 through to 20—their actual scores scores ranged: min = 0, max = 17 (M = 8.88, SD = 3.77). Frequency of participants' responses to the 20 questions can be seen in Figure 1.

TABLE II. Security behaviour questions

Q #	Questions
Q1*	In the past, I have disclosed personal passwords with other people so that they were able to use my account (e.g., computer, email, bank PIN).
Q2	I use a password manager.
Q3*	I sometimes re-use passwords across different websites.
Q4*	Sometimes I write down my passwords.
Q5*	I make my passwords as easy as the system will let me.
Q6	I try to make sure my anti-virus software is up to date.
Q7*	I rarely read dialogue boxes when installing new software.
Q8	When my computer prompts me to grant permissions to a certain applications, I make sure I know the consequences of granting those permissions before I agree to do so.
Q9	When I am required by my operating system to install updates, I try to do it as soon as possible.
Q10	I use two-factor authentication when websites permit.
Q11	I would never run an application downloaded from an unknown source.
Q12*	I would connect to an unknown Wi-Fi signal if it meant free internet access.
Q13*	I sometimes download files from peer-to-peer networks.
Q14	I only use my computer with the firewall on.
Q15	I will check the certificate of a website if I am unsure of its legitimacy.
Q16	I make an effort to limit the amount of data that websites collect about me.
Q17	I prefer to send my emails with encryption where possible.
Q18	I will assess a website's privacy policy before I make an account with them.
Q19	I have set my browser to prefer HTTPS connections.
Q20	I use the 'Do not Track' setting in my browser.
Q21	I feel confident that I take appropriate security measures when entering sensitive information online (e.g., credit card details).
Q22	I feel that my overall computer security behaviour is secure.
Q23	Adding extra security measures when using my computer would not be worth my time or effort.

Note—* these questions were reverse coded for statistical analysis.

TABLE III. Descriptive statistics for masculine, feminine, and risk measures

Measure	*N*	*M*	*SD*	Min	Max	Range
Risk	155	31.45	6.70	13	47	34
Masculine	155	47.88	7.98	21	68	47
Feminine	155	54.19	8.93	24	70	46

Note—theoretical ranges for scales are: Risk 0-49 (greater is more risk-averse); Masculine 0-70 (greater is more masculine); Feminine 0-70 (greater is more feminine)

It was decided that use of the Bem Sex-role Inventory [7] would be limited to finding participants' scores on masculine and feminine scales only; Bem's work categorizes participants into masculine, feminine, androgynous and undifferentiated based on a split-mean model [7]. Not only can split-means be problematic [12], the process also returns our thinking back to a single continuum of masculinity and femininity, and disallowing for a person to present as high (or low) on both the masculine and feminine scale. The focus of the study is not to categorize individuals, but rather to understand what traits individuals' possess that may affect their secure computer behaviour. As a result we left all participants with a masculine measure and feminine measure and did not categorise them. Participants were able to score between 0 and 70 on each scale; the descriptive statistics for these scales, along with those for the risk measure are shown in Table III.

A. Internal Consistency of Scales

The risk measure developed by Meertens & Lion [11] and the sex-role inventory developed by Bem [7] were both validated in their original papers as being uni-dimensional, therefore we assume the same uni-dimensionality. Nunnally [13] argues that Cronbach's alpha greater than .70 indicates

good internal consistency of measures; the current study returned values at the following levels: risk $\alpha = .74$, masculinity scale $\alpha = .84$; femininity scale $\alpha = .91$.

B. Sex and Age

We looked at potential correlations between participants' age and their scores on the risk and security measures; we found no significant relationships. We performed independent-samples t-tests to check for differences between males and females and their scores on the risk and security measures, again we found no significant relationships. When comparing genetic sex, as is normally done in the literature, males and females performed similarly on both the risk and security measures.

We found a significant difference between male and female participants and their feminine behaviour score, such that males score significantly less on the feminine scale than females—Male: $n = 78$, $M = 51.99$, $SD = 8.22$; Female: $n = 77$, $M = 56.42$, $SD = 9.12$, $t = -3.18$ (153), $p = .002$. A difference was not found between sexes when looking at the masculine scale score, indicating that both females and males were just as likely to exhibit these masculine traits.

C. Risk Measure

Results show a negative relationship between participants' masculine scores and their scores on the risk measure (higher score on risk measure indicate greater *risk-averseness*, r (155) = -.41, $p < .000$. In other words, a higher masculinity score is positively correlated to risk-taking behaviours; a scatterplot of this relationship is shown in Figure 2. We found no such relationship between participants' risk scores and their feminine scores. Our results indicate that although there is a difference between the sexes in their scores on the feminine scale, these scores do not correlate in a significant manner with risk scores. However, masculine scores, in which there was no significant difference found between the sexes in their scores (i.e., both sexes were equally as likely to score within similar ranges), were significantly correlated with risk scores. This is in contrast to the results that we would expect as indicated by the literature on risk (i.e., males are more risk taking and females are more risk averse). Our results show it is the exhibition of these masculine traits, regardless of sex, that serve as a better indicator of risk-taking behaviours.

D. Security Measure

We analysed possible relationships between between participants' scores on the masculine and feminine scales, and their scores for security behaviour—we found no significant correlations. Further, we found no significant correlation between participants' scores on the risk measure and their scores on the security measure. Knowing there is a relationship between the masculinity scale and risk, the lack of relationship between the masculinity scale and the security scale suggests that there may be other mediating variables involved, no relationship at all, or an issue with our measurement.

For analysis, we looked at two security measures: (1) participants' score on the security behaviour measure, scored out of 20 (questions 5(a) to 5(d)), (2) participants' answers to the three general perception of security behaviour questions.

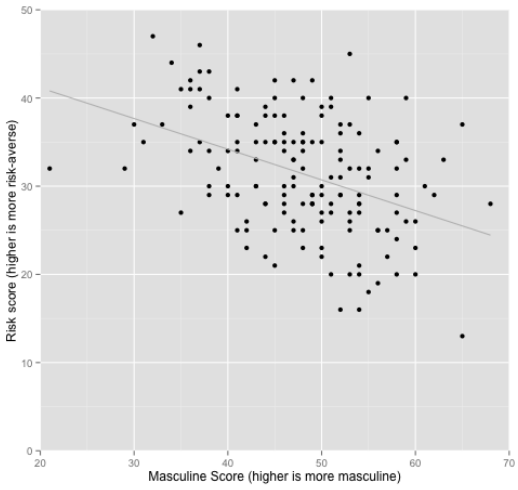


Fig. 2. Correlation between participants' masculine scores and risk scores

We found that reliability scores for the four groups of items that make up the security score were not consistent: protective behaviour $\alpha = 0.21$, passwords $\alpha = 0.62$, connecting with unknown entities $\alpha = 0.53$, privacy $\alpha = 0.69$. These scores indicate that there there is a lack of uni-dimensionality to the constructs; it could be that participants exhibit one security behaviour within a construct but not another—the questions within a construct were not collecting information on the same security behaviours (e.g., within the grouping relating to protective behaviour, it is conceivable that the same participant would always make sure their anti-virus was up to date but never use two-factor authentication).

We employed independent samples t-tests to understand the relationship between participants' answers to the general perceptions of security questions, and participants' scores on the risk-taking measure. We found significant relationships for two of the questions such that, participants who felt confident that they took appropriate security measures when entering sensitive information online (Q21) were more risk-averse (scored higher), than participants that were not confident—Agree: $n = 107$, $M = 32.35$, $SD = 6.47$; Disagree: $n = 42$, $M = 29.26$, $SD = 7.17$, $t = 2.54$ (147), $p = .012$. Participants that felt their overall computer security behaviour was secure (Q22) were also more risk-averse—Agree: $n = 99$, $M = 32.43$, $SD = 6.69$; Disagree: $n = 51$, $M = 29.92$, $SD = 6.56$, $t = 2.19$ (148), $p = .030$.

For both of these questions, participants that were more risk averse (scored higher on the risk scale) indicated that they felt more secure about their computer behaviour. We subsequently confirmed these results using binomial logistic regression.

E. Post-hoc Analysis

Given that the themes within our security behaviour score were not internally consistent, we explored answers to the individual questions relating to computer security, and their relationships to two of the general questions regarding perceived security behaviour (Q21 and Q22)—we rejected Q23 due to ambiguous wording. We do this in an attempt to understand if participants' perceived sense of security matches with their

exhibition of security behaviours—something that was not possible due to the scaling and reliability issues we faced when looking at security behaviour as a whole.

General perception vs individual security behaviour questions: Chi-square analyses for the security behaviours and Q21 uncovered one significant association, with Q19, after correcting for familywise type 1 error (Bonferroni; significant p value after correction = 0.002). Based on the odds ratio, the odds of participants feeling confident that they took appropriate security measures when entering sensitive information online were 6.5 times higher for participants who had set their browser to use only HTTPS connections, compared to those that did not: χ^2 (1, n = 124) = 14.75, $p < 0.000$.

Analyses for the behaviour questions and Q22 (again with a Bonferroni correction, significant p = 0.002) can be seen in Table IV. It is clear that there are a few strong associations between participants' perceived levels of computer security, as shown by their answers to Q21 and Q22, and their self-reported security behaviours. Of the four questions that showed significant relationships, all relationships were in the same direction, that is, the more participants' perceived their behaviour to be secure, the more likely they would be to report that they performed secure actions.

It is unclear whether Bonferroni corrections are necessary under these circumstances, but we applied them out of caution. Without correction, 14/20 individual questions show a positive significant relationship with one or both of the general perception questions.

General perception vs security behaviour score: We further explored these results by comparing differences between the participants' mean scores on the security behaviour measure. Although we found that the scale was not internally consistent across our *theme* areas, we still expect to see some difference when comparing the scores of those participants that perceived themselves to be secure to those that believe they practice insecure behaviours. We grouped participants by agreement or disagreement to the perception of secure behaviour questions (Q21 and Q22) and employed an independent samples t-test for both questions.

We found that participants who felt confident that they took appropriate security measures when entering sensitive information online (Q21), actually practiced more secure behaviours in total—Agree: n = 101, M = 9.53, SD = 3.51; Disagree: n = 42, M = 6.86, SD = 3.68, t = 4.09 (141), $p < .000$. Participants who felt that their overall computer security behaviour was secure(Q22) were also more likely to practice more security behaviours in total—Agree: n = 93, M = 9.71, SD = 3.45; Disagree: n = 51, M = 6.86, SD = 3.53, t = 4.70 (142), $p < .000$. These results indicate that participants do seem to have general perception of their own security behaviour that correctly aligns (within the limitations of our measurement) with their self-reported secure or insecure behaviours.

We are aware of the limitations of inferring relationships from post-hoc analysis of data; as such, we plan to confirm these relationships using *a priori* hypotheses in future research.

F. Support for Hypotheses

We found the following support for our hypotheses:

H1: We expected to see a positive relationship between increasing masculine behavioural traits and risk-taking behaviour. We did find a significant relationship indicating that increasing scores on the masculinity scale would predict increasing risk-taking behaviour over and above the predictive power of genetic sex alone.
H2: We expected to see a negative relationship between risk-taking behaviour and secure computer behaviour. We found no direct evidence to support this hypothesis. We found indirect evidence that participants who were more risk-averse (scored higher on the risk measure) were more likely to self report that they were secure in their behaviours. Further, these perceptions of secure behaviour were found to be positively related to secure behaviours.
H3: We expected to see, as a consequence of H1 and H2, a negative relationship between masculine behavioural traits and security behaviour. We found no direct relationship between these variables.

TABLE IV. CHI-SQUARE TESTS SHOWING ASSOCIATIONS BETWEEN INDIVIDUAL SECURITY QUESTIONS AND Q22

Question	χ^2	n	p	Odds Ratio
Q1	9.27**	150	.002	3.5
Q14	14.52**	146	.000	3.9
Q15	13.27**	143	.000	4.1
Q19	15.98**	125	.000	5.5

Note—for all questions df = 1. ** $p < .01$.

V. DISCUSSION

Our results indicate that participants' exhibition of masculine traits are a better indicator of participants' risk taking behaviour than relying on their genetic sex alone. As cultural norms have changed and what is considered masculine or feminine behaviour has become more fluid, it is likely that the traits that were once dominantly seen as masculine or feminine will be observed in persons of *both* sexes. As this happens, researchers will need to look at the traits that cause such behaviours separated from the genetic sex of the individual. Although employing an instrument to identify masculine or feminine behaviours can seem laborious for regular user studies, in instances where research is directly investigating sex differences, we argue that usage of such an instrument can provide a richer understanding of behaviour.

With respect to sex as a predictor of users' secure computer behaviour, recent research indicate that there is no difference between the males and females [5], [6]. Those results are in line with the findings from this study. Again, the way in which traditional sex-typed traits have been re-appropriated by both sexes may give rise to this situation–it no longer seems possible to say that certain traits that relate to risk-taking behaviour are predominantly male. We will need to look further at the underlying process that create these individual differences to understand their role in security behaviour.

Relationships between participants' scores on the risk measure and their overall thoughts about their computer security were logically as expected. Participants that were more risk-averse also perceived their computer security behaviour as more secure. It does not seem surprising that risk-taking behaviour was correlated with masculine defined traits. Many of these traits are indeed traits that carry with them an element of risk—for instance, questions on the sex-role inventory as

include items such as: *defend my own beliefs, forceful* and *willing to take risks*. Clearly these traits are more overtly linked to risk-taking behaviour than, for example, traits such as caring on the feminine scale.

Whether participants' computer behaviour was actually secure, we are unable to tell—unfortunately it seems as though the questions that we created were too varied to provide a good indicator. For example, there is every possibility that a person may be relatively secure in certain aspects of their computer behaviour, but much less so in others. For example, many participants that indicated that they felt their behaviour to be secure when answering the question: *I feel that my overall computer security behaviour is secure*, still stated that they shared passwords with other people.

Unlike physical security, it is extremely hard to define what behaviour people view as insecure as it is dependent on their attitude, context and value judgement of the assets to be secured. It is not as simple as, for instance, knowing that leaving an expensive laptop unattended in a busy café is an insecure behaviour—this situation has a clear dollar value as the worst case scenario whereas many situations related to computer security do not have such overt and present risk.

Results from the post-hoc analyses indicate that participants' self-reported security behaviours are linked to their overall perception of security. Thus, across the study, we see relationships between masculine traits and risk-taking behaviours; between risk-taking behaviours and general perceptions of security; and between general perceptions of security and secure behaviours. It is not possible to infer causation from the data collected, however, these relationships do serve to highlight the possible interplay between participants' individual differences and how these may be indicators of secure computer behaviour. We acknowledge there are some inherent issues with the current study but we do see future potential for refining the survey instrument to possibly identify 'at risk' individuals (or to provide targeted security education).

A. Limitations

It is understood that the questions in the current study relating to participants' secure computer behaviour may be too broad in helping decide if participants exhibit *overall* secure computer behaviour. As previously mentioned, it is possible that participants are secure in certain areas and less secure in others. We also acknowledge the limitations of survey research—it is noted by Jensen *et al.* [14] that participants often do not behave the same way in a real world setting as they self-report on questionnaires.

For future research, we plan to develop a more standardized questionnaire that is validated as uni-dimensional and that can be applied to evaluate secure computer usage. Development of this scale would likely have to forgo questions targeting specific secure/insecure behaviours and instead concentrate on overall security and perceived security although, as yet, possibilities of how this could happen are unclear.

VI. Conclusion

We present the results of a questionnaire study investigating the interplay between risk-taking behaviour, masculine and feminine traits, and secure computer behaviour. The study aimed to provide insight into how masculine traits are more reasonable indicators of risk-taking behaviour than genetic sex alone—our data showed a distinct relationship between risk-taking behaviour and masculine traits. We also found a relationship between participants' risk-taking behaviour and their general perceptions of their computer security. Finally, through post-hoc analyses, we found relationships between participants' general perceptions of personal computer security and certain secure computer behaviours. We believe that the current study can act as a foundational block for the further exploration of the usable security space with regard to participants' individual differences. Measures of participants' masculine and feminine tendencies over two dimensions rather than a single, bi-polar dimension enabled a more in-depth review of participants' behaviour as a product un-tethered from their genetic sex.

References

[1] 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*. Berkeley, CA, USA: USENIX Association, 1999, pp. 14–14.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42 (10), pp. 40–46, Dec. 1999.

[3] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63 (1), pp. 102–127, 2005.

[4] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50 (10), pp. 94–100, 2007.

[5] 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 (3), pp. 449–473, 2009.

[6] F. Lalonde Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji, "A clinical study of risk factors related to malware infections," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 97–108.

[7] S. Bem, *Bem Sex-Role Inventory: Professional Manual*. Consulting Psychologists Press, 1981.

[8] J. Tyler and C. Lichtenstein, "Risk, protective, aod knowledge, attitude, and aod behavior. factors associated with characteristics of high-risk youth," *Evaluation and Program Planning*, vol. 20 (1), pp. 27–45, 1997.

[9] P. J. Poppen, "Gender and patterns of sexual risk taking in college students," *Sex Roles*, vol. 32 (7-8), pp. 545–555, 1995.

[10] J. P. Byrnes, D. C. Miller, and W. D. Schafer, "Gender differences in risk taking: A meta-analysis." *Psychological Bulletin*, vol. 125 (3), p. 367, 1999.

[11] R. M. Meertens and R. Lion, "Measuring an individual's tendency to take risks: The risk propensity scale," *Journal of Applied Social Psychology*, vol. 38 (6), no. 6, pp. 1506–1520, 2008.

[12] D. L. Streiner, "3 breaking up is hard to do: The heartbreak of dichotomizing continuous data," *A Guide to the Statistically Perplexed: A Compilation of Readings from the Canadian Journal of Psychiatry*, vol. 47, p. 20, 2013.

[13] J. Nunnally, *Psychometric theory*. New York: McGraw-Hill, 1978.

[14] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of internet users: self-reports versus observed behavior," *Int. J. Hum.-Comput. Stud.*, vol. 63 (1-2), no. 1-2, pp. 203–227, Jul. 2005.