Understanding Individual Differences: Factors Affecting Secure Computer Behaviour

Matthew Hull[a] and Leah Zhang-Kennedy[b] and Khadija Baig[a] and Sonia Chiasson[a]

[a]Carleton University, Ottawa, Canada; [b]University of Waterloo, Waterloo, Canada

ARTICLE HISTORY
Compiled April 7, 2022

ABSTRACT
Understanding users' individual differences may provide clues to help identify computer users who are prone to act insecurely. We examine factors that impact home users' reported computer security behaviour . 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 impacted security behaviour, with knowledge as the most important predictor. We further show that a user's affinity to feminine or masculine characteristics is a better determinant of security behaviour than using binary male/female descriptors. Our study enabled us to confirm earlier results in the literature in a non-organizational setting, and to extend the literature by studying additional factors and by comparing the relative importance of each factor as a predictor of security behaviour.

KEYWORDS
Computer security behaviours; behaviour modelling; user characteristics; individual differences; survey

1. Introduction

Understanding users' behaviour pertaining to computer security is necessary for protecting against threats and enabling users to perform secure actions. The Ponemon Institute and IBM Security [81] estimates that 24% of data breaches can be attributed to negligent human causes and estimate the cost of these human-related errors at $3.5 million.

Prior research suggests that users' privacy attitudes and behaviours are related to individual factors [66, 72] such as demographic variables, privacy literacy, and online experiences [11]. So far, researchers [15,26,43,63,77] have adapted empirically validated behaviour models relating to predictive security behaviour from dominant theoretical frameworks, including Theory of Planned Behaviour [3], the Technology Acceptance Model [24], and Protection Motivation Theory [84]). However, whilst these models individually show relationships between behavioural antecedents and security outcomes, they have different classifications for behaviour factors that make comparisons between them difficult. Additionally, many existing models are centred around organizations;

Authors' copy. Published 2021 in Behaviour & Information Technology (TBIT): https://doi.org/10.1080/0144929X.2021.1977849

CONTACT Author. Email: lzhangke@uwaterloo.ca

there is limited research on models that focus on in-home security behaviour. Our research focuses on home-users: we (1) synthesize security behaviour factors from the literature and (2) expand the understanding of which personal factors are most relevant to home users' secure behavioural outcomes.

Based on our review of existing models, we noted that a individual's potential to act securely appears to be based on their knowledge, motivation and confidence towards practicing secure behaviour. By combining these together, we use the term "Security Potential" to describe the potential that an individual has to act securely at a given moment in time. We explored the relationship between participants' Security Potential Score (an aggregate of responses across all three factors) and their self-reported computer security behaviour. In other words, we explored whether participants with a higher Security Potential score were more likely to exhibit secure behaviours. Additionally, we assessed the participants' propensity to take risks, and sex-typed characteristics (masculine and feminine) using existing scales to explore the relative importance of these factors on users' security behaviour. We assessed 650 participants' Security Potential across two studies. We show that these are important factors indicative of security behaviour, but users' knowledge about computer security threats and protective strategies was the strongest predictor of reported security behaviour.

The main contributions from our work include:

- Confirming the existence of a relationship between several personal factors (knowledge, motivation, confidence) and security behaviour. Many prior studies were done in an organizational context; we demonstrate its applicability for home users.
- Identifying the relationship between security behaviour and (i) general propensity to take risk, (ii) self- and other-motivation, and (iii) sex-typed characteristics. First, we showed that feminine and masculine characteristics have a stronger relationship with security behaviour than sex traits alone. Second, those who are more socially motivated are more likely to behave securely than those who are personally motivated. Third, those who generally take more risk are less likely to behave securely.
- Identifying the relative importance of each of the above factors as a predictor of security behaviour. We showed that users' knowledge regarding security threats and protective strategies is the strongest determinant of security behaviour from among the factors studied.

2. Literature review

Recognizing the importance of user behaviour in computer security has led to increased research about individuals' security behaviour. Early research primarily focused on security behaviour and compliance from an organizational context. Employees were identified as a weak link in the security chain due to their ignorance of security risks, non-compliance, and deliberate circumvention of an organization's security policies [57, 58]. Therefore, early solutions focused on deterring and preventing computer security misuse and computer abuse (e.g., [95, 105]). Others suggested that identifying what motivates employees' compliance with security policies would help to improve their behaviour [4, 17]. A range of compliance drivers and deterrents have been identified within organizations, including aspects of management and socialization [17], work culture [22], morality and values [76], fear appeals [40, 46, 50, 84], attitudes and

normative beliefs [79], and computer security awareness [23], influencing employees' compliance with security policies.

While early research primarily focused on the workplace setting, more recent research has emphasized the vulnerability of home users and the need to understand their security behaviours in personal computer usage [6,63,75,97]. For example, users' compliance with password guidelines is affected by their perceptions of passwords and of security threats [75, 109]. While there are similarities between organizational and home security behaviour, there are many contextual factors that differentiate the two [61], such as home users are usually not subject to mandatory security awareness training, security policies, and monitoring.

Studies in computer security behaviour have typically investigated the relationship between attitude and security intentions (e.g., [26, 40, 43, 50]), but some argue that intention may not be the best predictor of actual behaviour because there are several (possibly unknown) variables that impact an individual's behavioural intention (e.g., good intention to comply with security policies) and actual behaviour (e.g., real computer security usage choices) [91]. Differences between individual based on personality traits [2, 22, 34, 67, 73, 91], sex-typed characteristics like gender [7, 69], and cultural differences [25, 88] may provide insights into computer security behaviour. However, these studies offer mixed results, indicating more research is needed to confirm these effects. In particular, some researchers have found sex differences in computer security behaviour [7,69,90]. For example, recent studies suggest that females exhibit fewer security behaviours overall [69], or report fewer specific behaviours such as secure password generation, proactive awareness, and updating [37]. Other studies suggest that males are more likely victims of malware [108]. However, others have found no significant differences between genders with respect to security behaviours [54, 73, 102]. Further discussion on how our work differs from prior work on sex differences and gender relating to computer security is provided in Section 6.1.5.

Researchers have developed predictive security behaviour models using related theoretical frameworks from psychology, health, and technology to understand and predict individuals' computer security behaviour, Dinev and Hu [26] and Bulgurcu et al. [15] studied security behavioural intentions based on the framework of Theory of Planned Behaviour [3]. In conjunction with Protection Motivation Theory [84], this framework was also used by Ifinedo [43] in exploring user security policy compliance behaviours. These studies found that technology awareness, computer security awareness, perceived vulnerability, attitudes toward compliance, subjective norms, normative beliefs, response efficacy, and self-efficacy had main effects on computer security behaviour. Others have adapted and extended the Protection Motivation model [84]: Mamonov and Benbunan-Fich [64] developed a research model [84] to study factors that affect perceptions of privacy breach among mobile app users; Warkentin and Siponen studied fear appeals in the context of Protection Motivation theory [51].

Ng et al. [77] used the Health Belief Model [85] adapted from the healthcare literature to study users' computer security behaviour and found that perceived benefits, perceived susceptibility, and self-efficacy are the main determinants of email-related security behaviour, while perceived severity moderates the effects of other security behaviour factors. Liang and Xue [63] tested a research model derived from the Technology Threat Avoidance Theory [62], and found several determinants related to avoidance motivation, such as perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived susceptibility, and perceived severity.

There are both research and practical applications for measuring users' security behaviour. For example, researchers can measure differences in behaviours between

different populations, and practitioners can use these scales to identify strengths and weaknesses in their systems [27]. Although many research models have been developed to investigate individual factors affecting computer security behaviour, most of the research focused on an organizational context. There is a lack of an overarching model that describes individuals' security behaviour in the home context. We address this research gap by developing an integrated model from existing predictive models of security behaviour. The goal is to understand the relative importance of various factors that are most relevant for assessing home users' core security proficiency. Using these factors, we then created the Security Potential questionnaire to as a measure of participants' self-reported security behaviour.

3. Development of our research instrument

We selected nineteen factors that influence computer security behaviour from five research models. These include Dinev and Hu's Awareness Centric model [26] and Bulgurcu et al. Information Security Awareness model [15] based on the theory of planned behaviour; Ifinedo's Information Systems Security Policy (ISSP) compliance behavioural intention model based on the theory of planned behaviour and protection motivation theory [43]; Ng et al.'s Computer Security Behaviour model based on the health belief model [77], and Liang and Xue's [63] Variance Model of technology threat avoidance theory. We included all factors with main effects derived from these studies to develop the portion of our questionnaire investigating end-users' Security Potential. We chose these particular models because they are based on established theoretical frameworks, they have evaluated the factors' main effects on computer security behaviour in empirical studies, and they are relevant for studying end-users' security behaviours.

All five models are supported by collected user data analyzed through regression or structural equation modelling techniques to identify which factors had more (or less) effects on behavioural outxcomes. For our classification, we carefully looked at the individual models and considered the main effects as understood by the authors' analysis of their data. We included the factors where a main effect was found. A list of the factors by author and descriptions for each are summarized in Table 1.

We analyzed the hierarchical relationship between the remaining factors. Some models were more specific in their identification of factors; therefore, a factor from one model may be placed as a sub-category of another model's factor. For example, *Information security awareness* is a factor identified by Bulgurcu et al. [15] that describes an employee's general knowledge about information security and *Technology awareness* is a factor described by Dinev and Hu [26] as a user's interest and knowledge about technological issues and strategies to deal with them. *Information security awareness* is classified as a sub-factor of *Technology awareness* because it is more specific. Factors with equivalent meanings are grouped together. For instance, self-efficacy was similarly defined in four models as a user's self-confidence and ability in practicing computer security and therefore grouped under the label *Confidence*. In some cases, differences in how the researchers approached their topics meant that a clear organization was impossible.

In a few instances, we noted in the diagram that, in our best interpretation, a sub-factor is related to multiple parent factors. For example, *Attitude toward compliance* (near the center of the diagram) is defined as the individual's positive or negative feelings toward engaging in a specified behaviour [43]. Attitudes towards complying with

Research Model	Framework	Description
Awareness Centric Model of User Behaviour [26]	TPB	*Technology awareness:* the user's raised consciousness of and interest in knowing about technological issues and problems and strategies to deal with them.
Computer Security Behaviour [77]	HBM	*Perceived benefits:* the user's belief in the perceived effectiveness of practicing computer security. Thus, higher perceived benefits are likely to lead to greater computer security behaviour. *Self-efficacy:* the user's self-confidence in his/her skills or ability in practicing computer security, which is likely to increase computer security behaviour. *Perceived susceptibility:* the user's perceived likelihood of a security incident taking place. When an individual perceives greater susceptibility to security incidents, he will be likely to exhibit a greater level of computer security behaviour. *Perceived severity:* the user's perceived seriousness of a security incident, which should lead to greater computer security behaviour.
Information Security Awareness [15]	TPB	*Normative beliefs:* an employee's perceived social pressure about compliance with the requirements of the information security policy caused by behavioural expectations of such important referents as executives, colleagues, and managers. *Self Efficacy:* an employee's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the information security policy. *Information security awareness:* an employee's general knowledge about information security and his cognizance of the information security policy of his organization.
ISSP Compliance Behaviour Intention [43]	TPB, PMT	*Subjective norms:* an individual's perception of what people important to them think about a given behaviour. *Response efficacy:* the belief about the perceived benefits of the action taken by the individual. *Self Efficacy:* the individual's ability or judgment regarding his/her capabilities to cope with or perform the recommended behaviour. *Perceived vulnerability:* an individual's assessment of the probability of threatening events. *Attitude toward compliance:* the individual's positive or negative feelings toward engaging in a specified behaviour.
Variance Model of TTAT [63]	TTAT	*Self Efficacy:* the users' confidence in taking the safeguarding measure. *Perceived threat:* the extent to which an individual perceives the malicious IT as dangerous or harmful. * (Note: determined by perceived susceptibility and severity and fully mediates their effects.) *Safeguard cost:* refers to the physical and cognitive efforts — such as time, money, inconvenience and comprehension — needed to use the safeguarding measure. *Safeguard effectiveness:* the subjective assessment of safeguarding measures regarding how effectively it can be applied. *Perceived susceptibility:* an individual's subjective probability that a malicious IT will negatively affect him/her. *Perceived severity:* the extent to which an individual perceives that negative consequences caused by a malicious IT will be severe.

Table 1.: Factors from theoretical frameworks with main effects on security behaviour. TPB: Theory of Planned Behaviour; HBM: Health Belief Model; PMT: Protection Motivation Theory; TTAT: Technology Threat Avoidance Theory.

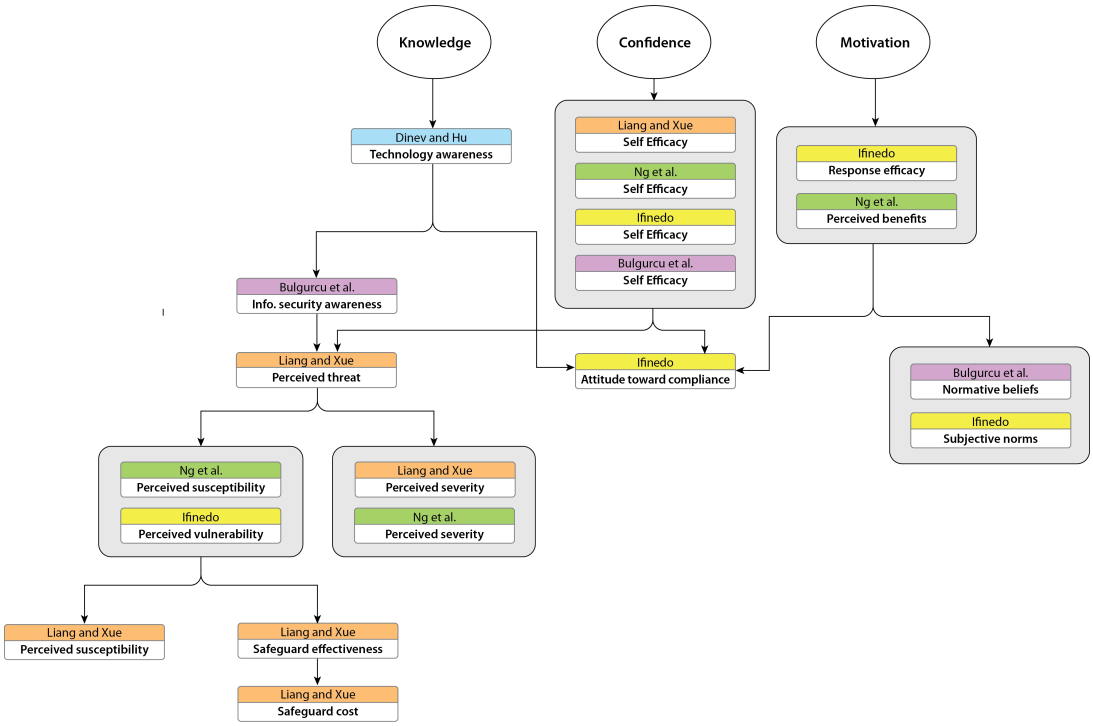


Figure 1.: Tree diagram showing hierarchy of security factors. Refer to Table 1 for a description of each factor.

acceptable security practices is shown in previous studies to positively impact users' behavioural intentions [15, 40, 76, 79]. We categorized it as a sub-factor of Knowledge, Confidence, and Motivation for the following reasons. Regarding Knowledge, individuals who have requisite knowledge about the effectiveness of recommended security advice in protecting against security threats are more likely to comply with the advice [56, 106]. Similarly, individuals in an organization who are more aware of the organization's information security guidelines and protective mechanisms are more likely to comply with them [40]. Regarding Confidence, prior studies have shown the pertinence of self-efficacy for determining users' intention to comply with information security policy [15, 40, 56, 79, 107]. It is expected that individuals with higher security competencies will be more likely to comply with security advice. For Motivation, the relative response cost (e.g., time, effort, money) to adopting certain behaviour can influence the likelihood of the person complying with a recommended behaviour [59, 73, 107].

Two researchers conducted the hierarchical classification of factors. In the first iteration, the two researchers worked independently and created draft diagrams. Then, they met to discuss their classifications and merged the results of their analysis using a collaborative online whiteboard platform. The researchers resolved any disagreements between their analysis by discussing their rationale for the classification, referencing the literature, and rearranging the factors' hierarchical position until they reached an agreement. Next, one of the researchers visually refined the diagram using graphical software. The two researchers met again to discuss the integrated diagram and made further refinements.

The final hierarchy of factors is shown in Figure 1. At the highest level, the factors are integrated into three main constructs that are predictive of users' security behaviours: (i) Knowledge, (ii) Confidence, and (iii) Motivation. We used the three constructs as the

foundation for our Security Potential measure; however, because our Security Potential Measure (Appendix A1) is designed to assess participants' *potential* to practicing core protective computer security behaviours , we also include *Behaviour* as an additional factor (Appendix A2) for us to assess the relationship between the participants' security potential and their self-reported security behaviour regarding basic security functions.

- **Knowledge:** relates to users' understanding of the threats to which they may be susceptible when using technology or navigating online spaces. It also relates to the users' understanding of possible preventative measures or actions that may be taken to protect against such threats.
- **Confidence:** relates to "...an individual's belief in his or her capacity to execute behaviours necessary to produce specific performance attainments..." [10]. This refers to users' confidence in their ability to perform protective security measures.
- **Motivation:** refers to participants' social and personal motivations for carrying out secure behavioural practices. These may include benefits to oneself, benefits to others, or even benefits to society as a whole.
- **Behaviour:** refers to users' self-reported security behaviours.

3.1. *Refinement of the Security Potential measure*

We refined our Security Potential measure through formative studies with usable security experts: including an online poll, a focus group, and two rounds of card sorting. We summarize the process and results below. More detailed result summaries are included in Appendix B.

We first decided what core proficiencies we expected users' to possess by consulting four usable security researchers from our research lab. We asked the researchers to complete an online form with their recommended list of core security proficiencies that users should have. We also asked for the reasoning behind their decisions (examples in Appendix B1). The process was anonymous; they could not see others' recommendations and suggestions, so they were not influenced by their peers.

The responses from the online poll guided open round-table focus group discussions to expand on the suggested proficiencies. We invited two different computer security researchers to speak openly about what proficiencies they felt were the most important to the everyday users. Our researchers reiterated sentiments from the previous poll that password management best practices and 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 necessary 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: 1) password best practice, 2) phishing (understanding, detection, and prevention), 3) user understanding of how malware can be downloaded unintentionally and how to avoid such situations, and 4) 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 an overarching factor relating to 5) *preventative security measures* (e.g., behaviours that reduce the likelihood that a user's personal computer will be infected/subject to attack).

We operationalized the constructs by first looking to see if we were able to adapt questions from previous literature, something that Ng et al. [77] describe as drawing "...representational questions from a universal pool". We were able to do this for participants' confidence with computer security practices. These questions were adapted from Compeau et al. [19] who constructed and validated a scale of computer self-efficacy. This scale has been widely used in the literature and has shown good construct validity [8, 63]. We opted to create new questions for the other parts of our instrument (knowledge, behaviour, and motivation).

After the first round of item creation, we conducted a card-sorting test with four security researchers from our research lab to further develop and refine the measure items. In a variation on the technique proposed by Moore and Benbasat [74], we presented a set of possible questions to the researchers in random order on slips of paper (example in Appendix B2, Figure 1). Working individually, they placed each question underneath the construct heading that they believe best fit each question. The researchers had unlimited time to complete the exercise; however, on average, it took around ten minutes to complete the task.

As a measure of inter-rater reliability (i.e., the degree of consensus between participants), we use Fleiss' Kappa ($\varkappa$) [31] for measuring reliability of agreement between a fixed number of raters. The first round of card sorting yielded a kappa value of $\varkappa = 0.47$. According to Landis and Koch [55], this is a moderate agreement between raters. The exercise served to highlight items within the instrument that needed to be modified.

After modifying the confusing questions, we performed a second round of card sorting that followed the same general format as the first, with five researchers. However, rather than being conducted in the lab setting with physical pieces of paper, this round of card sorting was conducted electronically. We presented the items and the construct headings to the researchers in an Excel spreadsheet and asked them to group the items under the appropriate construct headings (example in Appendix B2, Figure 1). This round of card sorting yielded a 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) [55].

Following this second round of card sorting, the only alterations made to the instrument were removing 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. A more detailed description of the two-rounds of card sorting is include in Appendix B2.

The final instrument consisted of 29 five-point Likert-scale questions from strongly agree to strongly disagree across three categories (Appendix A1). We created 14 questions for measuring computer security *knowledge*, 6 questions for measuring *motivation* to perform computer security actions (4 questions for personal motivation and 2 questions for social motivation), and 9 questions for measuring *confidence*. A additional 16-item questionnaire for measuring *performed* security behaviour is also included (Appendix A2). The security topics covered in the measure include password practices, phishing, malware, software updates, and general compliance to mainstream computer security advice and best practices.

We also developed a demographic questionnaire that collected participants' age, sex, educational background, nationality, profession, and answers to contextual questions about the participants' technical knowledge, such as whether they have an IT background or have taken a course in computer security. The full questionnaire is detailed in Appendix A4.

4. Methodology: Study One

We delivered our instrument to participants using the CrowdFlower online service[2]. At the time, CrowdFlower was a micro-task recruitment system for persons to post jobs and surveys, similar to Amazon's Mechanical Turk[3] (MTurk). Extensive research has been carried out examining the use of 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 [65]). MTurk workers tend to be higher educated and more technologically aware than the general population [100]. We did not use MTurk workers directly because, at the time, it was 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 cognizant of this assumption's implications (i.e., without research comparing the CrowdFlower workers to the MTurk workers we cannot be 100% sure).

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) CrowdFlower's highest-rated contributors were invited to complete the survey. According to CrowdFlower's website at the time of the study, these contributors accounted for 7% of monthly judgements made on the platform and maintained a high level of accuracy across various jobs posted to the platform [20].
(2) We chose participants in the United States, United Kingdom, Canada and Australia as our targeted countries because this would most likely result in participants' first language being English.
(3) We set the minimum time to complete the job at 300 seconds. Before posting the survey, we asked three volunteers to fully read through the online survey questions but did not require them to respond 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, they are automatically removed from the job by CrowdFlower's system.
(4) We allowed each participant to complete the survey one time only.

4.1. *Survey presentation*

A posting on the CrowdFlower platform announced the name of the job and provided the recruitment notice. The study protocol was reviewed and cleared by our university's Research Ethics Board.

4.2. *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. 374 participants took part in our study, 189 males and 185 females—their ages ranged from 18 years to 79 years (M = 37.87, SD = 12.22). As per the recruitment notice for the job, participants received

[2] `https://www.crowdflower.com/`; Crowdflower has since changed its business focus
[3] `https://www.mturk.com/`

$0.50 (USD).

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 could participate in our study and create and use an account with CrowdFlower to earn money. Regarding 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[4]. Roughly two-thirds of the participants used a computer daily for work (n = 262).

4.3. *Hypotheses*

We made several hypotheses regarding participants' overall *Security Potential*, a term that we use to describe users' ability to act securely based on their responses to our Security Potential measure that assesses three factors: Knowledge, Motivation, and Confidence. The questions for each factor are detailed in Appendix A1.

Considering existing literature, the following observations provided foundation for our hypotheses. First, users' existing *knowledge* of security risks and how to use security mechanisms influences their security behaviour [9, 16, 103, 104]. Second, users' *motivation* to act securely could be affected by several factors, including their perceived susceptibility to a threat, economic trade-offs [41], perceived benefits [91], and fear appeals [46, 50]. Third, the perceived efficacy of a threat response and one's own capabilities in completing tasks required for the desired response is correlated to secure behaviours [83, 89]. Fourth, users' self-reported security behaviour could function as an acceptable proxy for real behaviour [27] when the measurement of actual security behaviour could be unethical and sometimes impossible without putting users in compromising situations.

Additionally, while some studies suggest gender differences in security behaviour between male and females [69, 90], other research found are no such differences. For example, Lalonde et al. [54] and Milne et al. [73] found no significant gender differences in self-reported security behaviour. Further, McCormac et al. [68] found gender differences in knowledge disappeared when participants' *conscientiousness* and *agreeableness* were taken into account. Given that the results in the literature are mixed, we opted to conservatively hypothesize that there were no differences.

Based on the literature and these considerations, we present the following hypotheses:

H1 We expect that, overall, participants that score higher on our Security Potential measure will self-report more secure computer behaviours with respect to our proficiencies.

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

- **H2a** Participants that report as having more *knowledge* of our computer security proficiencies will self-report more secure behaviours with regard to those same proficiencies.

[4]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.

Table 2.: Descriptive statistics for the four factors.

Factors	Min	Max	Median	SD
Knowledge	1.07	5.00	4.36	0.884
Motivation	1.00	5.00	3.17	0.688
Confidence	1.00	5.00	3.89	0.931
Behaviour	1.31	5.00	3.69	0.676

H2b Participants that report as having increased *motivation* to perform security behaviours will self-report more secure computer behaviours with respect to our proficiencies.

H2c Participants that have more *confidence* in their ability to perform computer security behaviours will self-report more secure behaviours with regard to our proficiencies.

H3 We expect no significant differences between males and females on any of the four factors measured.

4.4. *Results*

4.4.1. Internal consistency of measures

We use Cronbach's alpha [78] to measure internal consistency within our four factors: knowledge, behaviour, motivation, and confidence. 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, and $\alpha = .78$ for social motivation.

In the presence of good internal consistency, we calculated the mean score per participant for each of the four factors. For example, participants answered 14 five-point Likert-scale questions regarding their computer security knowledge and we calculated the average score out of 5. Higher mean scores per factor indicate an individual who is more knowledgeable, motivated, confident, or who behaved more securely, respectively. Table 2 summarizes the descriptive statistics for the four factors. Since the set of mean scores were not normally distributed, we report the median of those (mean) scores for each factor instead.

4.4.2. Security Potential scores

We calculated an overall *Security Potential* score for participants by summing their scores on the knowledge, motivation, and confidence measures. We use this terminology to 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 (i.e., a participant scored the minimum of 1 on each of the three measures) and a maximum of 15 (i.e., if they scored the maximum of 5 on each measure). Our participants' Security Potential scores ranged from 4.10 to 15.00 ($Mdn = 11.24$, $M = 11.08$, $SD = 1.90$). A scatterplot suggesting a positive relationship between be-

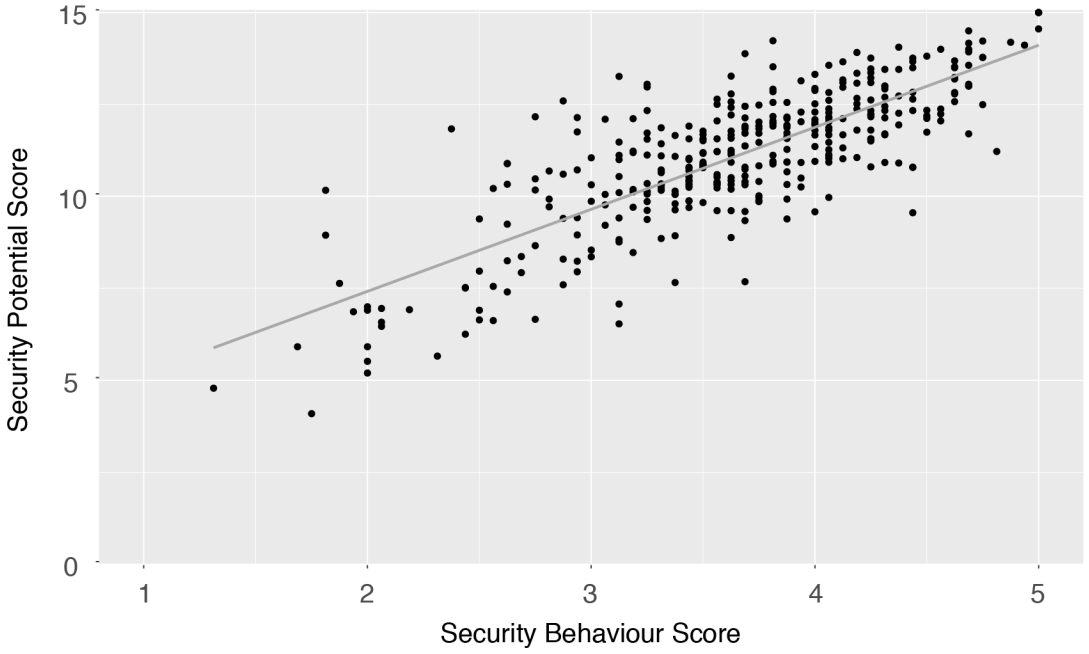


Figure 2.: Scatterplot of Security Potential score and security behaviour

tween the Security Potential score and self-reported security behaviour can be seen in Figure 2.

To investigate our first hypothesis (**H1**), we sorted our participants in increasing order based on Security Potential scores and evenly split the participants into three groups (at the 33rd and 66th percentile); the divisions occurred at scores of 10.52 and 12.00. This enabled us to create *low*, *medium*, and *high* Security Potential groups, which facilitated interpretation in relation to the specific security behaviours and served as a way to understand the dispersion of Security Potential scores (e.g., the inter-quartile range for the low Security Potential group is more spread out than those in the medium or high groups) . We hypothesized that our three groups would differ in the degree to which they self-report secure behaviours.

A Kruskall-Wallis test indicates that participants' levels of self-reported security behaviour is significantly different between the three groups, $H(2) = 171.87$, $p < .001$. 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 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 medium security group were significantly more likely to report secure behaviours than participants in the low Security Potential group, $U = 3037.00$, $p < .001$, $r = -.53$. Effect sizes for these results indicate that both findings are substantive.

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

Table 3.: Comparison of specific security behaviours between Low-Medium-High Security Potential groups. Items in bold are statistically significant.

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.

4.4.3. Specific security behaviours

We ran further Kruskall-Wallis tests to compare how the groups differed for the four theme areas within the behaviour measure; for example, how the Security Potential groups differed for the set of password questions in the behaviour measure. If differences were found, we followed up using Mann-Whitney tests with a Bonferroni correction (significance was reduced to the .006 level). Table 3 details the results of these analyses.

Across all four behavioural themes, participants in the *high* Security Potential group were significantly more likely to report 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 themes except password behaviours—although the significance value is $< .05$, it does not meet our Bonferroni-corrected significance threshold of $< .006$.

4.4.4. Predicting Security Potential

Using multiple regression analysis, we investigated how well our predictor variables (the knowledge, motivation, and confidence factors included in the Security Potential score) can predict participants' responses on our outcome variable—self-reported security behaviour. We use multiple regression analysis as opposed to Structural Equation Modelling (SEM) because SEM requires a causal relationship between variables and an a priori theoretical model of these causal relationships. We do not believe that our data adequately captures causal relationships, thus we use regression to identify the linear relationships between our observed variables. For example, we may identify a relationship between increased confidence and increased security behaviour, but cannot say that confidence *causes* an increase in security behaviour or that security behaviour *causes* an increase in confidence.

We used a standard hierarchical regression, inputting knowledge scores first, then motivation, and finally confidence. Table 4 outlines the final model.

Further diagnostics reveal no unacceptable levels of multicollinearity. We also examined our data for standardized residuals and can conclude that our model should be fairly representative of the population, and none of the outlying data points were unduly influencing the model.

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

Table 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**

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

Table 5.: Spearman's rho correlations between the behaviour measure score and the three factors

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

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

Interpreting Table 4, for every 1 full unit increase in knowledge score, we see an increase of .38 units on the behaviour measure (Step 3: Knowledge). This is true only if the effects of confidence and motivation are held constant. Similarly, a unit increase in motivation results in an increase of 0.35 units on the behaviour measure, and confidence in an increase of 0.16 units, assuming that the other two factors are held constant. Of the three measures, knowledge has the largest impact on participants' self-reported behaviour scores. That is, the more knowledgeable participants are about core security behaviours, the more likely they are to report that they exhibit 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, $p < .001$, $R^2 = .654$, $R^2_{\text{ADJUSTED}} = .652$.

4.4.5. Relationships between factors

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 5 details these correlations. We use Spearman's correlation coefficient (Spearman's *rho*, r_s) unless otherwise stated. [5]

As indicated by Table 5 (values in bold), 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

[5]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) [30].

Table 6.: Spearman's rho correlations between confidence, motivation, and sub-themes of the Behaviour Score

Factors	Behaviour Questions				
	Total Behaviour	(1) General	(2) Password	(3) Phishing	(4) 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.

respect to our proficiencies. All of our factors are significantly related to each other except confidence and motivation, which appear orthogonal.

4.4.6. Post-hoc correlations for confidence and motivation

We further analyzed whether motivation and confidence scores were correlated to the *individual* sub-themes within the security behaviour measure: (1) general questions; (2) password behaviour questions; (3) phishing questions; and (4) preventative behaviour questions. We apply a Bonferroni correction to control for type 1 error—significance is therefore reduced to the .0025 level. Table 6 details these relationships.

We found significant positive relationships between participants' confidence scores and their self-reported behaviour across all four sub-themes. We found similar significant positive relationships for motivation scores. Breaking down the motivation measure into its *social* and *personal* components, we found that participants' responses to the social component of our motivation measure were better indicators of their reported security behaviour ($r_s = .55$, $p < .001$) than responses to the personal motivation component ($r_s = .24$, $p < .001$).

Support for H2: Overall, our data reiterates our findings from the earlier regression and supports **H2**: all three factors (knowledge, motivation, and confidence) have a positive relationship with participants' self-reported behaviour. We further investigated 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.

4.4.7. Sex

To address our third hypothesis (**H3**), we investigated the effect of participants' sex on each of our four measures. We hypothesized that there would be no significant difference between males and females' scores 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, $U = 14820.00$, $p < .01$, $r = -.13$. For 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 to understand on which specific behaviours males and females differed. We compared male and female responses to the: (1) general behaviour questions, (2) password behaviour questions, (3) phishing behaviour questions, and (4) preventative behaviour questions.

We found that the questions relating to preventative behaviour show a significant difference between males and females; the others were not significant. Specifically, we found that males reported less preventative security behaviour than females, $U = 13143.00$, $p < .001$, $r = -.22$.

Support for H3: We found small differences between males and females' reported preventative behaviours; therefore cannot support **H3**.

4.5. *Summary of Study One Results*

We found support for both (**H1**) and (**H2**). We found significant relationships between individual aspects of the Security Potential measure (knowledge, motivation and confidence) and participants' self-reported security 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 security behaviours.

We initially hypothesized that there would be no sex differences for participants' scores on the four factors evaluated (**H3**). However, our data indicate small differences between males and females in their scores on the motivation factor (males being less motivated than females to perform security behaviours) and their self-reported preventative security behaviours (males reported fewer preventative security behaviours than females).

5. Methodology: Study Two

For our second study, we made some additions to our instrument to expand Study One's findings. Specifically, we wished to understand the reason for the sex differences that we saw and expand on the motivational differences that we found. Further, we wished to explore if findings from Study One are replicable.

5.1. *Additional measures*

We kept all of the previous measures in our instrument and added three extra measures (detailed below). The first two further expand on results from Study One related to the sex difference and motivational differences. The third measure assessed participants' propensity to take risk. The addition of this scale is based on previous research [27, 90] showing participants who identify as engaging in riskier behaviour also report being less secure in their computer security. Our selected instrument differs in that it measures a general propensity to take risk rather than domain-specific risk.

5.1.1. Bem Sex-Role Measure:

Following up on the differences we found between males and females in Study One, we decided to investigate whether traditionally sex-typed characteristics influence participants' security behaviours. Bem Sex-Role measure (short form) [13] 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 measure is based upon standards of masculinity and femininity as they pertain to a western culture (the initial work was based on US ideals).

We use the short-form version of the measure [13] 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 nor feminine. Participants are presented with characteristics (e.g., *'Independent'* or *'Sympathetic'*) and asked to rate how much the characteristic relates to them. The measure uses a seven-point Likert scale that ranges from 1 = *Never true* to 7 = *Always true*. Responses for the masculine and feminine items are summed, then averaged, giving each participant a separate masculine and feminine score. As per Bem [13], the ten items that are neither masculine nor feminine are discarded. A higher score on these scales means the respondent exhibits more masculine or feminine characteristics. The full measure is detailed in Appendix A, Section 2.3.

5.1.2. Self- and Other-Interest Measure:

In Study One, we found that participants with a higher social motivation (e.g., other-interest) to perform security behaviours were more likely to report performing secure behaviours in general. We found a smaller correlation between personally (e.g., self) motivated behaviour and self-reported security behaviours. As such, we test this result to see if the finding holds up with a generic measure of self-interest and other-interest.

The self- and other-interest measure [36] was developed to assess the extent to which a respondent's behaviour is driven by self-interest and/or interest in others (i.e., pro-social behaviours). The measure 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*. Higher scores on these scales mean that the respondent exhibits a higher degree self- or other-interest, respectfully. The full measure is detailed in Appendix A, Section 2.2.

5.1.3. The Risk Propensity Measure:

We included a Risk Propensity measure [71] to understand the impact of participants' risk-taking on their security behaviour. It is an eight-question scale measuring respondents' general risk-taking tendencies. Participants are asked to read the eight statements and then to rate their level agreement with each one on a seven-point Likert scale; the scale ranges from 1 = *Strongly agree* to 7 = *Strongly disagree*. Responses are summed, then averaged, to give the respondent an overall risk propensity score out of 7. A higher score on the risk measure means the respondent is more likely to exhibit risk-taking behaviour. The full measure is detailed in Appendix A, Section 2.1.

5.2. *Methodology*

Similar to Study One, we used the CrowdFlower online service to deliver our survey. We doubled the amount that participants were paid to $1.00 (USD) to reflect the extra work required of the longer survey. In terms of delivery, the participant selection criteria were kept the same.

We stipulated a longer minimum time to complete this longer survey. Participants who completed the survey faster than 480 seconds were removed by CrowdFlower. The study protocol was reviewed and cleared by our university's Research Ethics Board.

5.3. *Participants*

We obtained usable data from 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 assumed they are sufficiently familiar 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.

5.4. *Hypotheses*

Prior research showed that most home computer users feel responsible for securing their personal computers [33], and those who believe online safety is their personal responsibility are significantly more likely to protect themselves [56]. In addition to personal motivation, the desire to act in a socially responsible manner may also influence users' motivation for security behaviour even though the benefit of acting securely may for the greater good rather than personal [6,34]. Though at times, socially induced security behaviours could be motivated by self-interested reasons such as the desire for social acceptance. Regarding risk propensity, research has found that users who identify as engaging in riskier behaviour also report being less secure in their computer security practices [27, 90].

Study One suggested that males are less motivated than females to perform security behaviour, and males practice fewer preventative security behaviours than females. Other studies of employee's security behaviour observed similar patterns. For example, Hearth and Rao [40] found females have higher policy compliance intentions than males. Ifinedo [44] found that males have lower security policy compliance intentions than females.

Traditionally, comparisons between males and females are studied as binary options. Bem [13] argues that it is possible for persons to exhibit both masculine and feminine traits concurrently and that these may be more descriptive than binary male/female categorizations. For example, 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. Therefore, previous studies (e.g., [7,69] that use gender (male vs female) as a predictor of behaviour could be confounding specific masculine and feminine traits.

Based on these considerations and the results of Study One, we make the following hypotheses:

H1 We predict that the feminine sub-scale of the Bem Sex-Role measure will show a stronger relationship with participants' motivation to complete secure computer behaviours than the masculine sub-scale.

H2 We predict that the feminine sub-scale of the Bem Sex-Role measure will show a stronger relationship with participants' self-report of secure computer behaviour than the masculine sub-scale.

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

Table 7.: Internal consistency of Study Two 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 [78]: *Acceptable; **Good; ***Excellent.

ship with behaviour than self-interest (**H3b**).

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

5.5. *Results*

5.5.1. Internal consistency of measures

Table 7 details the alpha values for each scale. Similar to our Study One, we found good levels of consistency throughout our scales. Responses from the motivation scale and the risk scale were below Nunnally's [78] criteria of $\alpha = .70$ for good consistency; however, they were still within the acceptable range.

A summary of the descriptive statistics for responses to all nine measures from the survey is provided in Table 8. Participants' Security Potential scores (the combined score of knowledge, motivation and behaviour) are similar to Study One; a Shapiro-Wilks test indicates that distribution is normally distributed. Theoretically, participants could score between 3 and 15 on this measure; participants ranged in their scores from from 6.83 to 15.00 ($Mdn = 11.53$, $M = 11.48$, $SD = 1.40$).

5.5.2. 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 and 67 percentiles. We checked to see if the results from this study aligned with the results from Study One regarding 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 tests with Bonferroni correction, thus

Table 8.: Descriptive statistics for the nine scaled factors from Study Two.

Factors	Min	Max	Median	SD
Knowledge	2.21	5.00	4.43	0.53
Motivation	1.67	5.00	3.00	0.69
Confidence	1.56	5.00	4.00	0.72
Behaviour	2.06	5.00	3.75	0.68
Risk	1.00	5.83	2.83	0.88
Self-interest	1.00	7.00	4.56	1.16
Other-interest	1.22	7.00	4.83	1.17
Bem Masculine	1.30	7.00	4.50	1.02
Bem Feminine	1.60	7.00	5.40	1.04

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

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 medium Security Potential group were more likely to report secure behaviour than participants in the low Security Potential group, $U = 1782.50$, $p < .001$, $r =$ -.50. Similar to Study One, effect sizes for these findings are substantial.

5.5.3. 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 accounts for less of the variance than in 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. As in Study One, we found that knowledge, motivation and confidence were all significantly correlated with participants' security behaviour. Table 9 details these relationships.

5.5.4. Sex and sex-typed characteristics

Results from our first study indicated sex differences with regard to participants' motivation to perform secure behaviours and their reported secure behaviours. To gain deeper insight into these potential differences, we added the Bem Sex-Role measure to our second survey (discussed in section 5.1). Descriptive statistics showing the distribution of male and female scores on the masculinity and femininity scales can be seen in Table 10.

Table 9.: Spearman's rho correlations between four original factors

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

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

Table 10.: Descriptives for males and females in relation to masculine and feminine Bem scales

	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

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, expecting that females would be more motivated than males. We conducted a Mann-Whitney test and found that females were more motivated behave securely, $U = 7286.00$, $p < .001$, $r = -.20$. Next we looked at differences between males and females with respect to their reports of secure behaviour; contrary to the Study One we found no difference, $U = 9358.00$, $p = ns.$

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 (**H1**). We found 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 ($r_s = -.05$, $p = ns.$); We compared these correlations by evaluating whether their t statistic were significantly different from each other [30], 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. 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 who report as being more secure are more likely to identify with characteristics within the feminine Bem scale than the masculine Bem scale.

5.5.5. *Self- and other-interest*

We hypothesized (**H3**) that there would be a stronger relationship between other-interest and behaviour, than between self-interest and behaviour. As these are two separate measures (rather than opposite ends of the same scale), it is possible for an individual to score high on both the other- and self-interest measures. Results indicate that security behaviour is significantly correlated with other-interest ($r_s = .37$, $p < .001$), and with self-interest ($r_s = .24$, $p < .001$). The difference in t statistic indicates that these correlations are significantly different from each other, $p < .01$.

We believe that these results show some support for **H3**: participants with greater levels of interest in the well-being of others are more likely to report secure computer behaviours than those that do not. However, we also found that participants who show high levels of self-interest are also more likely to exhibit secure computer behaviours than those that do not; albeit, not to the same extent.

5.5.6. *Risk*

We also look at participants' propensity to take risk as a factor that may predict a participant's computer security behaviour. Our results indicate support for our hypothesis (**H4**): we found a negative relationship between participants' propensity to engage in risk-taking behaviour and their reported security behaviour, $r_s = -.20$, $p < .01$. In other words, participants who are risk-averse are more likely to report secure behaviour, and those who are more likely to take risks are less likely to report secure behaviour.

5.5.7. *Post-hoc risk analysis*

Following up on our finding regarding risk and behaviour, we further investigated risk with respect to sex and to the Bem masculine and feminine scales. We performed a Mann-Whitney test to investigate potential sex differences and participants' propensity to take risk. We found that males report a higher propensity to take risk than females $U = 6926.00$, $p < .001$, $r = -.24$.

We also found a significant 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, $p < .001$.

We find a significant sex difference between males' and females' propensity to take risk. Further, idealized masculine and feminine characteristics, as measured by the two sex-role scales, show significantly different relationships (positive and negative respectively) with participants' scores on the propensity to take risk scale. Our results from Study One 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 Study Two are more in line with the literature on risk that males are more prone to take risks than females [29, 38].

5.5.8. *Overall impact of factors*

To explore the overall impact of the factors on security behaviour, we conducted a Relative Weight Analysis [49] 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 sig-

Table 11.: Relative weights of factors

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

nificant 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[6]. Results from this analysis are detailed in Table 11. We followed the recommended procedure of Tonidandel et al. [98] and thus, confidence intervals for the individual relative weights were bootstrapped with 10,000 replications, as were the corresponding tests of significance. Our results 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.

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 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). In the second model, we input only the four variables highlighted as most important by the Relative Weight Analysis. 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, the original variables from Study One were the most important indicators of security behaviour. This is possibly due to the original variables used language related to security behaviour, whereas the new scales added in Study Two did not directly reference security behaviour. However, the information gained in Study Two confirmed that knowledge, social behaviour, confi-

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

dence, and personal motivation have the strongest influence in home users' computer security behaviour, among the factors tested.

5.6. *Summary of Study Two Results*

We found support for our first hypothesis (**H1**): the feminine sub-scale of the Bem Sex-Role measure showed a stronger relationship with participants' motivation scores compared to the masculine sub-scale. Supporting our second hypothesis (**H2**), we found that the feminine sub-scale showed a stronger relationship with security behaviours than the masculine sub-scale. 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 found support for **H3** insomuch as there were significant relationships between self-interest and other-interest scales (**H3a**) and behaviour. The other-interest scale exhibited a stronger relationship with participants' behaviour scores than the self-interest scale (**H3b**). In other words, participants who are more pro-social were more likely to report secure computer behaviours.

Finally, we found support for our hypothesis regarding risk (**H4**). Participants who were more prone to taking risk were less likely to report behaving securely.

Our post-hoc analysis of risk revealed that males had a higher propensity to take risks than females. Further, the masculine Bem scale showed a stronger relationship with a propensity to take risks than the feminine Bem scale.

6. Discussion

In this research, we explored ways in which people's individual differences affect 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).

6.1. *Factors*

We identify the following factors (in order of influence) as having an impact:

6.1.1. Knowledge

Similar to the findings that employees are more competent in managing security tasks when they are more aware of an organization's security policies and procedures [60], our results show that knowledge of the issues surrounding computer security (both threats and protective measures) was the strongest predictor of home users' reported security behaviour.

Security training within organizations has a positive effect on employees' security knowledge, attitudes, and behaviours [5, 87]. Our findings highlight that the same is likely also true for home computer users. Improving users' understanding of their security systems can positively affect their ability to perform in a secure manner, both within an organizational context [5,87] and outside of it [5,53,110]. Although our results do not explicitly show causality, they do show a strong positive relationship that further

supports and emphasises the importance of security education for users, and in this case, it is likely that knowledge leads to more secure behaviour. This education refers to both teaching users about protective strategies, and also to helping them understand, at some level, why such protective strategies work. Users need appropriate mental models [1, 14, 96], including understanding the limitations of protective measures [32].

Further, our results support Dinev and Hu's [26] 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", to be a key determinant of acceptance and implementation of security measures. Our findings further support related research showing that end users' security expertise could be reasonably measured by assessing computer security-related skills and knowledge [82], and that these could be significant determinants of security behaviour. 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, but we provide data supporting this intuition.

6.1.2. Motivation

Users' motivations to undertake secure behaviours can be complex and multi-faceted. *Protection Motivation Theory* [84] 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. Furthermore, pro-social motivation such as altruism has been associated with secure computer behaviours [34], and the pressure to be socially responsible can impact users' cost/benefit analysis even without direct benefit to the users themselves [6]. For example, a user may be careful not to spread a virus to friends via email. Although apparently altruistic, the user may be motivated more by self-interested reasons, such as what others think of them or a potential loss of social standing.

Our results align with previous research indicating motivation is a significant factor in users' security behaviour [6, 86, 86]. Through our analysis, we identified the importance of motivation in general terms (with the measure of other-interest; Study Two), and in domain-specific terms (with our social motivation sub-scale; Study One). Our participants who reported greater levels of social motivation were more likely to engage in secure behaviours. However, further research is need to understand whether the social motivations driving security actions are altruistic or self-interested in nature.

6.1.3. Confidence

Prior studies (e.g., [42, 43, 79, 92–94, 107]) showing that confidence has a significant impact on users' security compliance behaviour were primarily done in an organizational context and considering employee behaviour. A literature review of 42 studies on self-efficacy [39] confirmed the significance of the relationship between individuals' self-efficacy and organizations' information systems security adoption. Self-efficacy in the organizational context mainly concerns individuals' belief that they have the necessary IT training and experience, and are capable of complying with the organization's security policy [42]. Similarly, our participants' confidence in their ability to complete security tasks was positively related to their security behaviour: the more confident participants were in completing security behaviours, the more likely they were to perform them. Limited prior research with end-users in the home context shows that self-efficacy positively influences individuals' security practices [83, 97]. Our results indicate a close

positive relationship between knowledge, confidence, and behaviour. However, more research is needed to identify the causal relationships between these factors, for example, does improving users' confidence in their ability to perform security measures directly improve their security practices and how does confidence influence security knowledge? The relationship is not necessarily linear, for example, what users think they know about computer security could influence their security behaviour more than what they actually know [88].

6.1.4. Risk

In our study, those who were more risk-averse were more likely to practice secure behaviour. Our results align with the general literature on risk in that risk-taking behaviours are inversely related to users' security behaviours [27, 35, 101].

However, users' have also been found to make apparently unsound security decisions, for example, ignoring security advice for very little benefit, such as a negligible monetary compensation [18]. Users may have made these decisions because they saw the initial costs (e.g., cost of action rather than the potential cost if something went wrong) to be minimal. Some researchers have studied this behaviour from a purely economic perspective [12, 21, 41]. While this would account for some variables that moderate risk-taking actions, it does not account for individual differences.

Previous research has shown that users who are more risk-averse relative to security are more likely to display secure behaviour than those who engage in domain-specific risk-taking behaviour [27, 90]. We investigated whether the same relationship exists between security behaviour and a general propensity to take risk measure. We argue that a more general measure would be easier to maintain and re-use since it would not need to be modified as technology and security advice evolves. We did find a significant negative relationship between general risk-taking and security behaviour, but other factors had more impact on security behaviour scores, suggesting that our general risk measure should be used in conjunction with other measures rather than as the sole predictor.

Furthermore, understanding users' propensity to take risk provides a base level from which to start — some users are naturally more likely to take risks or make insecure decisions. Users' risk propensity is an individual characteristic that is more difficult to change than other factors, such as educating users to improve their knowledge. Understanding how risk propensity impacts users' security behaviour enables researchers to account for its effects in designing experiments and allows for more accurate interpretation of data.

6.1.5. Sex and sex-typed characteristics

Prior research on the relationship between gender differences and security behaviour have treated gender as a binary trait (male vs female) [7, 29, 38, 69, 90], but this categorization is increasingly recognized as problematic. Results from these studies are often contradictory: some find that females are more at risk, others find that males are more at risk, and yet others find no differences in security behaviours.

Our study used the Bem Sex-Role scales to assess how people self-identify in relation to masculinity and femininity. We found that the Bem masculinity and femininity scales were better indicators of security behaviour than relying on sex alone.

Some studies find women to have poorer self-reported security security behaviour [7, 69], worse password practices [37], and more susceptible to phishing attacks ([45, 90]).

Alternate research suggests no differences between gender [54, 73]. Our analysis, however, found that individuals with feminine characteristics were more likely to behave in a secure manner, and that the feminine Bem scale was a better predictor of motivation.

Further, risk was positively related to the masculine Bem scale (higher masculine score indicated a greater propensity to take risk). We argue that many characteristics encompassed by the feminine Bem scale are characteristics that are related to pro-social 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 to socially motivated security behaviour. Additionally, the scales 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; and confidence was associated to a greater degree with the masculine scale.

Existing research is also contradictory with respect to knowledge. McCormac et al. [68] found that when certain personality traits are taken into account, gender differences in security awareness disappear. In contrast, Kruger et al. [52] studied the affect of culture on security information awareness. Amongst the factors measured, gender **did** have an effect on security awareness (albeit to a lesser extent). In a study looking at security awareness in university students [28], the authors found that male students performed better in demonstrating knowledge than female. However, our Study 1 findings found no significant relationship between gender and knowledge.

6.2. *Limitations*

As with other survey studies, the main limitation is that we use a self-reported measure of security behaviour, which may differ from real behaviour [47]. Other limitations may arise as a result of online collection of data. For example, participants may be susceptible to decreased attention due to completing other tasks at the same time [70] or feel less accountable when completing tasks [48]. There may be variability in the quality of data collected from CrowdFlower. However, our sample sizes should have adequately balanced out the noise within the data. Furthermore, population samples recruited from CrowdFlower may not fully represent the general population.

6.3. *Recommendations*

When collecting research data that assesses security behaviour, we recommend that security researchers include instruments to identify 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. 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 take risks may enable researchers to control for these characteristics, or at least interpret their data with sensitivity to them. Furthermore, we encourage researchers to move beyond binary male/female descriptors when collecting demographics and consider instruments such as the Bem Sex Role questionnaire for more nuanced analysis. 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 recommend that the development of a single scale to measure respondents' Security Potential could aid in identifying high-risk individuals. Clearly not everyone falling

into this category would exhibit insecure behaviours; however, it would serve as an indicator. This tool would enable researchers to better understand their participants. Further, it may be a useful aid for organizations and service providers to enable them to provide targeted security training to those users in need. Our survey instrument may serve as a reasonable starting point, but would likely need to be shortened.

Since we found user knowledge about computer security is the most powerful predictor of security behaviour, we recommend addressing users' lack of security knowledge through education. Educating users may in turn provide them with more confidence and motivation 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 [36]. 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 [99].

From a practical perspective, our Security Potential measure could be used by security practitioners to measure users' knowledge, motivation, self-efficacy, and behaviour concerning security. For example, measuring the effectiveness of a public information security awareness campaign by comparing users' Security Potential scores before and after an intervention. Existing measurements like the HAIS-Q [80] focus primarily on business contexts, and the SEBIS scale [27] assesses the computer security behaviour of end-users, but focuses on measuring users' self-reported adherence to computer security advice. Our Security Potential measure focuses specifically on personal factors that influence computer security behaviour. We believe that our measures can provide a reasonable approximation to predict users' overall security behavioural outcomes, especially when measuring actual behaviour is potentially harmful (e.g., putting users in compromising situations) or is prohibitively costly.

While many information security research models are derived from established theoretical frameworks, such as the frameworks summarized in Table 1(e.g., Protection Motivation Theory), they primarily focused on studying security behaviour from an organizational context (See literature review in Section 2). Prior work that extended these theoretical frameworks to reflect the under-studied personal computer security domain are few, including studies by Johnston and Warkentin [50] that explored the role of social motivation on home users' security behaviour, Anderson and Agarwal [6] that studied both social and psychological components, and Thompson et al. [97] that studied the possible differences between home computer and mobile device users' personal computing security behaviour. Adding to this body of work, we show other nuances in individuals' determinants of personal computing behaviour, such as their propensity to take risk, personal and social motivation, and sex-typed characteristics.

6.4. *Future work*

Starting with the measures used in our studies, 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 form 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 likely too

long to be used as a quick assessment tool in research studies. Further, we would like to add elements from the psychological scales (risk propensity, self- and other-interest, Bem Sex Role questionnaire) that did not originally make up the Security Potential score to provide a more holistic approach to understanding participants' propensity act securely.

7. Conclusion

We explored 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 also note that users' affinity to certain sex-typed characteristics is a better determinant than using binary male/female categorization. Researchers should fully consider these factors when interpreting the results of usable security studies. Although some of these factors had been considered in previous work, our study enabled us to confirm earlier results and to extend the literature by studying additional factors and by comparing the relative importance of each factor as a predictor of security behaviour.

Acknowledgements

This work was supported by the Canada's Natural Sciences and Engineering Research Council under S. Chiasson's Discovery Grant RGPIN 06273-2017; and Canada Research Chair program under Grant 950-231002-2016.

Disclosure of interest

The authors report no conflict of interest.

References

[1] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei. Exploring user mental models of end-to-end encrypted communication tools. In *USENIX Workshop on Free and Open Communications on the Internet*, 2018.

[2] N. Aharony, D. Bouhnik, and N. Reich. Readiness for information security of teachers as a function of their personality traits and their assessment of threats. *Aslib Journal of Information Management*, 2020.

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

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

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

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

[7] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443, 2017.

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

[9] F. Asgharpour, D. Liu, and L. J. Camp. Mental models of security risks. In *Financial Cryptography and Data Security*, pages 367–377. Springer, 2007.

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

[11] L. Baruh, E. Secinti, and Z. Cemalcilar. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1):26–53, 2017.

[12] A. Beautement, A. Sasse, and M. Wonham. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, pages 47–58. ACM, 2009.

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

[14] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[15] B. Bulgurcu, H. Cavusoglu, and I. Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3):523–548, 2010.

[16] J. Camp, F. Asgharpour, and D. Liu. Experimental evaluations of expert and non-expert computer users' mental models of security risks. *Proceedings of WEIS*, 2007.

[17] M. Chan, I. Woon, and A. Kankanhalli. Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3):18–41, 2005.

[18] N. Christin, S. Egelman, T. Vidas, and J. 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.

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

[20] 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.

[21] 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.

[22] A. Da Veiga and J. H. Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010.
[23] J. D'Arcy, A. Hovav, and D. Galletta. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1):79–98, 2009.
[24] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, pages 319–340, 1989.
[25] T. Dinev, J. Goo, Q. Hu, and K. Nam. User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, 19(4):391–412, 2009.
[26] T. Dinev and Q. 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.
[27] S. Egelman and E. Peer. Scaling the security wall: Developing a security behavior intentions scale (SEBIS). In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2873–2882, 2015.
[28] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho. Information security awareness in educational institution: An analysis of students' individual factors. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 352–359. IEEE, 2015.
[29] H. Fehr-Duda, M. De Gennaro, and R. Schubert. Gender, financial risk, and probability weights. *Theory and Decision*, 60(2-3):283–313, 2006.
[30] A. Field. *Discovering statistics using IBM SPSS statistics*. Sage, 2013.
[31] J. L. Fleiss. Measuring nominal scale agreement among many raters. *Psychological Bulletin*, 76(5):378, 1971.
[32] S. Furnell. End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, 2008(4):6–9, 2008.
[33] S. Furnell, P. Bryant, and A. Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410 – 417, 2007.
[34] T. Gabriel and S. Furnell. Selecting security champions. *Computer Fraud & Security*, 2011(8):8 – 12, 2011.
[35] V. Garg and L. Camp. Risk characteristics, mental models, and perception of security risks. In *ASE Conference*. Academy of Science and Engineering, USA, 2014.
[36] M. E. Gerbasi and D. A. Prentice. The self-and other-interest inventory. *Journal of Personality and Social Psychology*, 105(3):495, 2013.
[37] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther. Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73:345–358, 2018.
[38] P. E. Gustafson. Gender differences in risk perception: Theoretical and methodological perspectives. *Risk analysis*, 18(6):805–811, 1998.
[39] M. A. Hameed and N. A. G. Arachchilage. Understanding the influence of individual's self-efficacy for information systems security innovation adoption: A systematic literature review. *arXiv preprint arXiv:1809.10890*, 2018.
[40] T. Herath and H. R. Rao. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009.
[41] C. 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.
[42] V. Hooper and C. Blunt. Factors influencing the information security behaviour

of it employees. *Behaviour & Information Technology*, 39(8):862–874, 2020.

[43] P. Ifinedo. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83–95, 2012.

[44] P. Ifinedo. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1):69–79, 2014.

[45] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, Oct. 2007.

[46] J. L. Jenkins, M. Grimes, J. G. Proudfoot, and P. B. Lowry. Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, 20(2):196–213, 2014.

[47] C. Jensen, C. Potts, and C. 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.

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

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

[50] A. C. Johnston and M. Warkentin. Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, pages 549–566, 2010.

[51] A. C. Johnston, M. Warkentin, and M. Siponen. An enhanced fear appeal rhetorical framework. *MIS quarterly*, 39(1):113–134, 2015.

[52] H. A. Kruger, L. Drevin, S. Flowerday, and T. Steyn. An assessment of the role of cultural factors in information security awareness. In *2011 Information Security for South Africa*, pages 1–7. IEEE, 2011.

[53] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[54] 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*, CCS '13, pages 97–108, New York, NY, USA, 2013. ACM.

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

[56] R. LaRose, N. J. Rifon, and R. Enbody. Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3):71–76, Mar. 2008.

[57] J. Lee and Y. Lee. A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 2002.

[58] S. M. Lee, S.-G. Lee, and S. Yoo. An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6):707–718, 2004.

[59] Y. Lee and K. R. Larsen. Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2):177–187, 2009.

[60] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45:13–24, 2019.

[61] Y. Li and M. T. Siponen. A call for research on home users' information security behaviour. In *Pacific Asia Conference on Information Systems PACIS*, page 112, 2011.

[62] H. Liang and Y. Xue. Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, pages 71–90, 2009.

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

[64] S. Mamonov and R. Benbunan-Fich. The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83:32–44, 2018.

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

[66] P. K. Masur and M. Scharkow. Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, 2(1):2056305116634368, 2016.

[67] O. Mazhelis and S. Puuronen. A framework for behavior-based detection of user substitution in a mobile context. *Computers & Security*, 26(2):154–176, 2007.

[68] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson. Individual differences and information security awareness. *Computers in Human Behavior*, 69:151–156, 2017.

[69] T. McGill and N. Thompson. Gender differences in information security perceptions and behaviour. In *Australasian Conference on Information System*, pages 1–11, 2018.

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

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

[72] M. H. Millham and D. Atkin. Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society*, 20(1):50–67, 2018.

[73] 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*, 43(3):449–473, 2009.

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

[75] F. Mwagwabi, T. McGill, and M. Dixon. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In *Hawaii International Conference on System Sciences*, pages 3188–3197. IEEE, 2014.

[76] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance. What levels of moral reasoning and values explain adherence to information security rules? an empirical study. *European Journal of Information Systems*, 18(2):126–139, 2009.

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

[78] J. Nunnally. *Psychometric Theory*. New York: McGraw-Hill, 1978.

[79] S. Pahnila, M. Siponen, and A. Mahmood. Employees' behavior towards is secu-

rity policy compliance. In *Hawaii International Conference on System Sciences*, pages 156b–156b. IEEE, 2007.

[80] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66:40–51, 2017.

[81] Ponemon Institute and IBM Security. 2019 cost of a data breach report. `https://databreachcalculator.mybluemix.net/executive-summary`. Accessed: 07 May, 2020.

[82] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp. Factors in an end user security expertise instrument. *Information & Computer Security*, 2017.

[83] H.-S. Rhee, C. Kim, and Y. U. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, 2009.

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

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

[86] N. S. Safa, C. Maple, T. Watson, and R. Von Solms. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications*, 40:247–257, 2018.

[87] M. Sas, G. Reniers, W. Hardyns, and K. Ponnet. The impact of training sessions on security awareness: Measuring the security knowledge, attitude and behaviour of employees. *Chemical Engineering Transactions*, 77:895–900, 2019.

[88] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2202–2214, 2017.

[89] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 2. ACM, 2010.

[90] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382. ACM, 2010.

[91] J. Shropshire, M. Warkentin, and S. Sharma. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security*, 2015.

[92] M. Siponen, S. Pahnila, and A. Mahmood. Factors influencing protection motivation and is security policy compliance. In *Innovations in Information Technology*, pages 1–5. IEEE, 2006.

[93] M. Siponen, S. Pahnila, and A. Mahmood. Employees' adherence to information security policies: an empirical study. In *IFIP International Information Security Conference*, pages 133–144. Springer, 2007.

[94] J.-Y. Son. Out of fear or desire? toward a better understanding of employees' motivation to follow is security policies. *Information & Management*, 48(7):296–302, 2011.

[95] D. W. Straub Jr and W. D. Nance. Discovering and disciplining computer abuse in organizations: A field study. *MIS quarterly*, pages 45–60, 1990.

[96] N. Thompson and T. McGill. Mining the mind–applying quantitative techniques

to mental models of security. In *Australasian Conference on Information Systems*, 2017.

[97] N. Thompson, T. J. McGill, and X. Wang. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70:376–391, 2017.

[98] S. Tonidandel, J. M. LeBreton, and J. W. Johnson. Determining the statistical significance of relative weights. *Psychological Methods*, 14(4):387, 2009.

[99] T. Toscos, A. Faber, S. An, and M. P. Gandhi. Chick clique: Persuasive technology to motivate teenage girls to exercise. In *CHI extended abstracts on Human Factors in Computing Systems*, pages 1873–1878. ACM, 2006.

[100] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. 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.

[101] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559, 2017.

[102] A. Vance, M. Siponen, and S. Pahnila. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3-4):190–198, 2012.

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

[104] R. Wash and E. Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security*, pages 309–325, 2015.

[105] R. Willison. Understanding the perpetration of employee computer crime in the organisational context. *Information and organization*, 16(4):304–324, 2006.

[106] I. M. Woon and A. Kankanhalli. Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human-Computer Studies*, 65(1):29–41, 2007.

[107] M. Workman, W. H. Bommer, and D. Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, 24(6):2799–2816, 2008.

[108] T.-F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels. An epidemiological study of malware encounters in a large enterprise. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1117–1130, 2014.

[109] L. Zhang and W. C. McDowell. Am i really at risk? determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4):180–197, 2009.

[110] L. Zhang-Kennedy, S. Chiasson, and R. 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.

Appendix A

1. Security Potential Measure

5-point scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

1.1 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.

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

Personal motivation

15. I would ignore computer security advice if it benefitted me to do so.
16. I may ignore computer security advice if it doesn't benefit me personally.
17. If I incur a financial cost by following computer security advice then I am less likely to follow the advice.
18. If following computer security advice is time consuming, I am less likely to do it.

Social motivation

19. By following computer security advice when possible, society as a whole benefits.
20. I have a responsibility to other people to ensure that I follow computer security advice whenever possible.

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

21. I am confident I could secure my data and personal information even if there was no one around to show me.
22. I am confident I could secure my data and personal information even if I hadn't taken similar measures before.
23. I am confident I could secure my data and personal information using only reference materials.
24. I am confident I could secure my data and personal information if I had previously seen someone else complete a similar task.
25. I am confident I could secure my data and personal information if I could call someone to help if I got stuck.
26. I am confident I could secure my data and personal information if someone else helped me get started.
27. I am confident I could secure my data and personal information if I had lots of time.
28. I am confident I could secure my data and personal information if someone showed me how to do it first.
29. I am confident I could secure my data and personal information if I had used similar measures before.

2. Security Behaviour Questionnaire

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.
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.
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.
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.

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.
15. I always install software updates as soon as I possibly can.
16. If possible, I set my software to install updates automatically.

3. Additional Questionnaires

2.1 Risk Propensity Questionnaire (Meertens and Lion, 2008)

7-point scale, ranging from 1 (strongly disagree) to 7 (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.

2.2 Self- and Other Interest Questionnaire (Gerbasi and Prentice, 2013)

7-point scale, ranging from 1 (strongly disagree) to 7 (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

10. I am constantly looking for ways for my acquaintances to get ahead.
11. Hearing others praise people I know is something I look forward to.
12. I want to help people I know to do well.
13. I try to help my acquaintances by telling other people about their successes.
14. I look for opportunities to help people I know achieve higher social status.
15. The success of my friends is important to me.
16. I look out for ways for my friends to have more money.
17. I keep an eye out for other's interests.
18. It is important to me that others are happy.

2.3 Bem Sex Role Questionnaire (Bem, 1981)

7-point scale, ranging from 1 (never true) to 7 (always true).

1. Defend my own beliefs
2. Affectionate
3. Conscientious
4. Independent
5. Sympathetic
6. Moody
7. Assertive
8. Sensitive to the needs of others
9. Reliable
10. Strong personality
11. Understanding
12. Jealous
13. Forceful
14. Compassionate

15. Truthful
16. Have leadership abilities
17. Eager to soothe hurt feelings
18. Secretive
19. Willing to take risks
20. Warm
21. Adaptable
22. Dominant
23. Tender
24. Conceited
25. Willing to take a stand
26. Love Children
27. Tactful
28. Aggressive
29. Gentle
30. Conventional

4. Demographic Questionnaire

1. What is your age in years? [text box]
2. What is your sex?
    - Male
    - Female
3. 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
4. What is your nationality? [text box]
5. In what country do you currently reside? [text box]
6. 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
7. Do you use a computer daily for work?
    - Yes
    - No
8. Do you own a personal computer?
    - Yes
    - No
9. On the computer you use most often, is the operating system:
    - Microsoft Windows

- Apple OSX
- Linux

10. 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 ask me for help.
11. Do you have a degree in an IT related field?
    - Yes
    - No
12. Have you ever taken a course on computer security?
    - Yes
    - No

Appendix B

1. Online Poll Results

In deciding what core security proficiencies, we reasonably expected users' to possess and to be able to implement regularly, we consulted a group of four usable security researchers from our lab. We asked the researchers to complete an online form with their recommended list of security proficiencies. 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 proficiencies 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.

2. Card Sorting Results

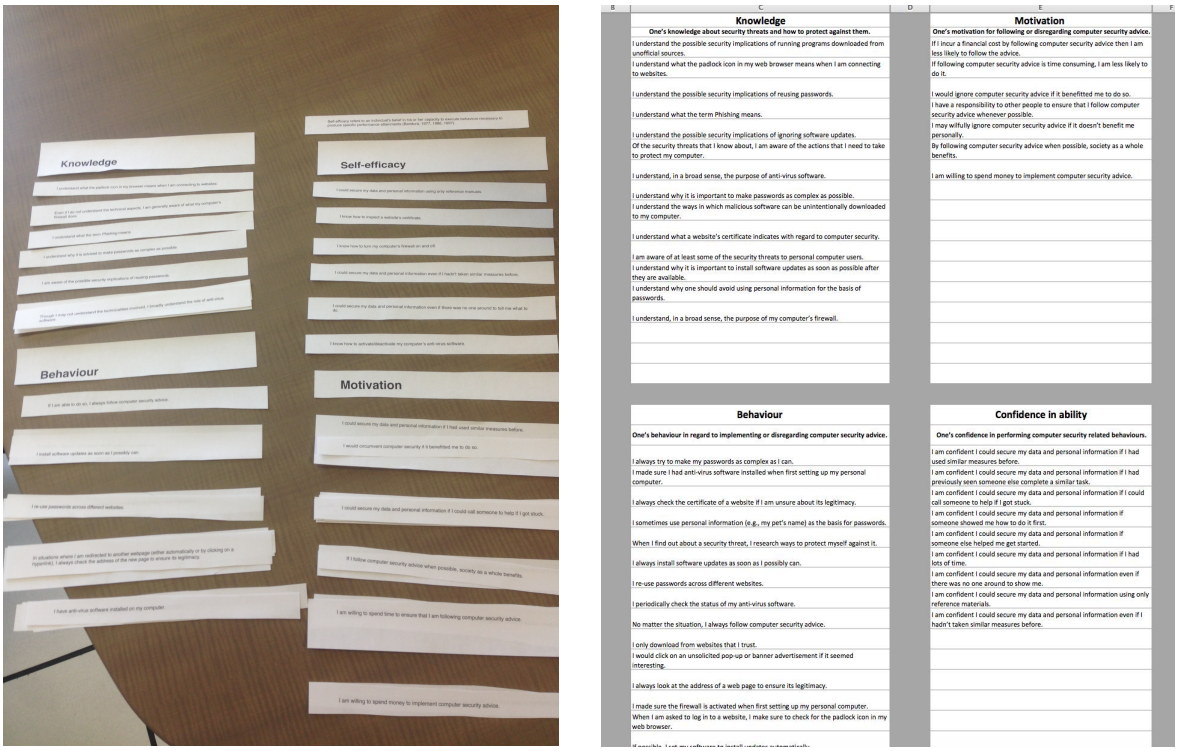
We conducted two rounds of card sorting with small groups of security researchers from our lab to test the content validity of the questions. All researchers had taken at least one graduate level course in usable security and all were actively researching in the usable security area.

In Round One, 46 individual question Items are presented to four security researchers on shuffled slips of paper. The researchers placed each question underneath the construct headings they believe best fit the question (See Figure 1). The researchers had unlimited time to complete the exercise; however, it took around ten minutes to complete the task on average.

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 worded ambiguously). We also asked the researchers to not force an item into a particular construct—if they were unsure of where it should reside, they could leave it out and note why they thought it did not fit. Figure 3.2 shows the completed Round One card sort from one of the groups.

The exercise served to highlight items within the instrument that needed to be modified. For example, based on the researchers' feedback, we changed one of the questions relating to phishing, "I would check the certificate of a website if I was unsure of its legitimacy" to "I *always* check the certificate of a website if *I am* unsure about its legitimacy" to clarify the behavioural aspects. 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 1 item, made 31 minor changes to existing items, and added 3 new items.

We performed a second round of card sorting that followed the same general format as the first with five researchers. However, rather than being conducted in the lab setting with physical pieces of paper, the second round of card sorting was conducted electronically. 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 1 shows part of the spreadsheet.



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.

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 1: Completed Round One *(left)* and Round Two *(right)* card sort from one of the researchers