View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by espace@Curtin

Gender Differences in Information Security Perceptions and Behaviour

Tanya McGill
School of Engineering and Information Technology
Murdoch University
Perth, Australia
Email: T.Mcgill@murdoch.edu.au

Nik Thompson
School of Management
Curtin University
Perth, Australia
Email: Nik.Thompson@curtin.edu.au

Abstract

Information security is of universal concern to computer users from all walks of life. Though gender differences in technology adoption are well researched, scant attention has been devoted to the study of gender differences in information security. We address this research gap by investigating how information security perceptions and behaviours vary between genders in a study involving 624 home users. The results reveal that females exhibit significantly lower overall levels of security behaviour than males. Furthermore, individual perceptions and behaviours in many cases also vary by gender. Our work provides evidence that gender effects should be considered when formulating information security education, training, and awareness initiatives. It also provides a foundation for future work to explore information security gender differences more deeply.

Keywords Information security, Gender, Home computer, Human factors, Security behaviour

1 Introduction

Information security is becoming increasingly important for individuals as well as organisations as information technology becomes part of all aspects of everyday life. Approximately 25% of data breaches in organisations are caused by end-users (Ponemon Institute 2013), similarly home users often fail to adopt basic security measures (Alshammari et al. 2015) or comprehend common security issues such as spam or phishing emails (Rajivan et al. 2017). Technical protections are part of the solution but human security behaviour is integral to effective protection. Security education, training, and awareness initiatives can help inform users' appraisals of security threats and provide guidance on how to effectively respond to these threats (Puhakainen and Siponen 2010). There has, however, been limited research on how demographic differences influence information security behaviour (Gratian et al. 2018), yet understanding this could be important in identifying users who may be more likely to have poor information security behaviour (McCormac et al. 2017). Understanding these differences can be used to tailor initiatives to increase their effectiveness.

This paper focuses on one key individual difference – gender – with the aim of investigating the role of gender differences in security behaviours and perceptions in order to identify differences that may have implications for securing home users' devices, software and data. It is the first large scale study that both targets a broad range of personal information security behaviours and considers gender differences in terms of the potential contributors to security behaviour proposed by Protection Motivation Theory (PMT) (Rogers 1975; Rogers 1983) and information security research that has arisen from it (e.g., Anderson and Agarwal 2010; Thompson et al. 2017; Tsai et al. 2016). It addresses the scarcity of research on gender differences in information security behaviour.

2 Background

Very little research has examined gender differences in information security behaviour, but differences have been identified in information technology use and perceptions associated with it. Women have been found to be more anxious about using information technology (Broos 2005; Chua et al. 1999; He and Freeman 2009). They also perceive software to be more useful than men do, but less easy to use (Gefen and Straub 1997; Venkatesh and Morris 2000). Women are also more influenced by ease of use in their e-learning adoption decisions (Ong and Lai 2006) and have less information technology experience, knowledge and computer self-efficacy (He and Freeman 2009).

The gender differences in security behaviour that have been found in the information security domain include females having a greater susceptibility to phishing attacks (Jagatic et al. 2007; Sheng et al. 2010), poorer password behaviour (Gratian et al. 2018), and lower likelihood of adopting privacy protecting behaviours (Milne et al. 2009). Females have, however, been reported to have higher levels of security concerns (Hoy and Milne 2010; Laric et al. 2009; Mohamed and Ahmad 2012). Findings such as these suggest that further research is needed to understand the reasons for these findings, and their implications.

Models such as PMT (Rogers 1975; Rogers 1983) have been used to help understand information security behaviour. PMT was originally developed in the context of health behaviour research and proposes factors that potentially influence intentions to undertake recommended behaviours. Studies applying PMT in the information security domain have successfully explained a substantial amount of the variance in information security behavioural intentions (Sommestad et al. 2015). Previous information security research that has used PMT suggests that user perceptions relating to perceived vulnerability, perceived severity, security self-efficacy, response costs and response efficacy can all influence security intentions (e.g., Boss et al. 2015; Liang and Xue 2010; Mwagwabi et al. 2018). In addition, subjective norm and descriptive norm have been shown to play a role in previous personal information security behaviour research, with subjective norm influencing intentions to protect personal computers and descriptive norm influencing intention to perform security behaviours relating to the Internet (Anderson and Agarwal 2010).

The role of gender is, however, less clear. Some studies have considered whether it has a direct influence on security intentions or behaviour (Gratian et al. 2018; Herath and Rao 2009; Mamonov and Benbunan-Fich 2018), whereas others model it as a precursor of constructs such as: perceived risk (Garbarino and Strahilevitz 2004); information privacy concern (Mohamed and Ahmad 2012); and perceived vulnerability, response efficacy and security self-efficacy (Chen and Zahedi 2016). It has also been modelled as a moderating influence (Luciano et al. 2010). This study provides a starting point for further investigation by exploring which security behaviour precursors exhibit gender differences.

3 Research Questions and Hypotheses

Home information technology users face numerous security threats (e.g. attacks on software vulnerabilities and phishing) and need to protect themselves by taking security measures such as backing up, creating secure passwords and installing security software. However, they generally have less access to security training and support. The research described in this paper is designed to compare the security behaviours and perceptions of males and females in order to identify differences that may have implications for securing home users' devices, software and data. As discussed above, PMT (Rogers 1975; Rogers 1983) proposes factors that potentially influence intentions to undertake behaviours and has been widely used in information security behaviour research. Research that has used PMT suggests that user perceptions relating to perceived vulnerability, perceived severity, security self-efficacy, response costs and response efficacy all influence security intentions (e.g., Boss et al. 2015; Liang and Xue 2010; Mwagwabi et al. 2018). In addition, subjective norm and descriptive norm have been shown to play a role in previous research (Anderson and Agarwal 2010). These constructs are briefly defined below in Table 1.

Perception	Definition
Perceived severity	The degree to which a user believes that the consequences of security threats would be severe
Perceived vulnerability	The degree to which a user believes that they are likely to experience security related threats
Security self-efficacy	The degree to which a user is confident in their own ability to take protective action against security threats
Response efficacy	The degree to which a user believes that available protective measures are effective
Response cost	The degree to which a user believes that there are costs associated with recommended protective behaviours
Subjective norm	A user's beliefs as to whether others want them to perform security behaviours
Descriptive norm	A user's beliefs as to what most other people do in terms of protective security behaviours

Table 1: Definitions of information security related perceptions considered in the study

These factors as well as common security behaviours were therefore considered in order to answer the central research questions:

> *RQ1: What, if any, differences are there in information security behaviours relating to personal computing between female and male users?*
>
> *RQ2: What, if any, differences are there in information technology experience and information security perceptions between female and male personal computing users?*

Some previous research has identified gender differences in security behaviour, but the results have been mixed. Sheng et al. (2010) found that female users were more likely to click on links in phishing emails and continue on to provide personal information. Gratian et al. (2018) also found that females had weaker password behaviours in terms of password strength, regularly changing passwords and using different passwords for different accounts; they also had weaker updating behaviours such as not immediately installing updates. However Gratian and colleagues (2018) did not find differences in terms of device securement, and Pattinson et al. (2015) found no significant gender differences in work related computer-based security behaviour. Based on this, we anticipate that there will be differences across individual security behaviours such as password use and backup behaviour, and as the current study focusses on personal information security behaviour, we hypothesise that:

H1: Females will have lower overall levels of information security behaviour than males

Early research on gender differences found that computer use may be seen as a masculine activity (Williams et al. 1993) and that females were more anxious about using computers in general (e.g., Broos 2005). They were also found to perceive a higher risk in online purchasing (Garbarino and Strahilevitz 2004). A more recent meta-analysis suggests that there has only been a minimal reduction of the general difference in attitudes between genders, but that differences may be more pronounced in

specific areas of attitude (Cai et al. 2017); for instance in the context of online privacy concerns, with females being more concerned (Hoy and Milne 2010; Laric et al. 2009; Mohamed and Ahmad 2012). Thus it is likely that gender differences may exist in information security perceptions that have been shown to influence security behaviour (e.g., Anderson and Agarwal 2010; Boss et al. 2015; Liang and Xue 2010; Mwagwabi et al. 2018) and we hypothesise that:

H2: Differences in information security perceptions will exist between females and males

In exploring possible reasons for why females were more susceptible to phishing attacks, Sheng et al. (2010) found that their female participants had less technical knowledge and training than the male ones and proposed this as a partial explanation for differences in susceptibility to phishing attacks. Therefore, we hypothesise that:

H3: Females will have less information technology skill and previous information security training than males

4 Method

The target population for this study was people who use information technology devices such as home computers, tablets and smartphones for personal use, and data was collected using an anonymous online questionnaire.

4.1 Participants and Procedures

In order to obtain participants from a wide spectrum of backgrounds a third party recruiting company used census balanced random sampling to identify potential participants from their panel members. Potential participants in the United States were contacted via email and invited to participate by completing an anonymous online questionnaire that was hosted on SurveyMonkey. All participants were 18 or over and had both a home computer and a mobile device.

4.2 Survey Instrument

The first section of the questionnaire asked about gender, previous information security training and self-reported level of skill with information technology. The second section of the questionnaire asked questions about the participants' security perceptions and behaviours relating to one of their devices. To get a broad range of responses, participants were randomly allocated to answer questions about either their home computer use, or about their mobile device use. The security perceptions measured were: perceived vulnerability, perceived severity, security self-efficacy, response efficacy, response cost, subjective norm, and descriptive norm (see Table 1 above for brief definitions of these constructs). To ensure validity and reliability of the items, we selected items that had been validated in previous information security research wherever possible and the items were modified for the personal computing domain as necessary.

The items to measure information security perceptions were measured on 7 point Likert scales from 1 "Strongly Disagree" to 7 "Strongly Agree" (see Appendix for all security perception items and their sources). Once data collection and preparation were completed, reliability testing was conducted to ensure that the constructs demonstrated sufficient internal consistency. All Cronbach alphas were above 0.9, and the scales were thus found to be reliable (Nunnally 1978). A summary measure of each of these constructs was then calculated for each respondent as the average of the responses to the items.

Security behaviour was measured using six items, each of which asked the participant about whether or not they performed a specific common security behaviour (see Table 2 for a list of these behaviours). These items were chosen as representative of recommended personal information security behaviours, and responses to each were coded as 1 for "Yes" or 0 for "No" or "Unsure". An overall measure of information security behaviour was also calculated as the sum of the responses to the six items.

5 Results

A total of 624 valid responses (62.5% female and 37.5% male) were used for the analysis. As can be seen from Table 2, there were significant differences between females and males for three of the six individual security behaviours. There were gender differences in whether users had recent backups of their device (χ^2 (2, N=624) = 11.064; p = 0.004), with females less likely to have recent backups (43.3% versus 53.8%). It was also interesting to note that females were more likely not to know whether they had recent backups (13.8% versus 6.4%). There were also significant differences between females and males in whether they had installed security software such as anti-malware themselves (χ^2 (2, N=624) = 7.805;

p = 0.020), with females less likely to have done so. But there were no differences in terms of whether they used security software (χ^2 (2, N=624) = 3.749; p = 0.153).

	Females			Males			Sign.
	Yes (%)	No (%)	Unsure (%)	Yes (%)	No (%)	Unsure (%)	Diff?
Have recent backups	43.3	64.2	13.8	53.8	39.7	6.4	✓
Installed security software	49.7	40.5	9.7	59.8	35.0	5.1	✓
Use security software	63.3	26.9	9.7	68.4	26.1	5.6	×
Enabled automatic updating of software	58.7	29.2	12.1	65.8	26.1	8.1	×
Device secured with password	69.0	25.6	5.4	71.4	25.2	3.4	×
Have a firewall enabled on home network	64.1	18.2	17.7	77.4	13.7	9.0	✓

Table 2. Individual security behaviours comparison

Females and males were not significantly different in terms of whether they enabled automatic updating of software (χ^2 (2, N=624) = 3.858; p = 0.145), nor in whether they secured their device with a password (χ^2 (2, N=624) = 1.346; p = 0.510). There were, however, significant differences between females and males in whether they had a firewall enabled in their home network (χ^2 (2, N=624) = 13.241; p = 0.001), with females less likely to have done so (64.1% versus 13.7%); females were also more likely not to know whether one had been enabled (17.7% versus 9.0%).

To compare levels of overall security behaviour, a non-parametric Mann-Whitney U test was used as the data did not meet the assumption of normality. As can been seen in Table 3, females had significantly lower levels of overall security behaviour than males (Mdn 4.00 vs 5.00; U=38,480, Z=-3.33, p=0.001). H1 was therefore supported.

	Females		Males		p	Sig.
	Mean	SD	Mean	SD		Diff?
Security behaviour	3.48	1.91	3.97	1.91	0.001	✓
Perceived severity	6.08	1.18	5.72	1.28	<0.001	✓
Perceived vulnerability	4.68	1.41	4.75	1.21	0.614	×
Security self-efficacy	5.12	1.31	5.30	1.08	0.160	×
Response efficacy	5.07	1.31	5.02	1.11	0.387	×
Response cost	3.30	1.49	3.36	1.47	0.507	×
Subjective norm	3.86	1.60	3.88	1.56	0.655	×
Descriptive norm	4.97	1.38	4.69	1.34	0.011	✓

Table 3. Overall security behaviour and security perceptions comparison

Table 3 also provides a gender comparison of the mean levels of each of the security perceptions relating to personal computing that were considered in this study. Differences in these perceptions were analysed using non-parametric Mann-Whitney U tests as the data did not meet the assumption of normality. Significant gender differences were found for two of the perceptions that were considered. Females were found to have significantly higher levels of perceived severity than males (Mdn 6.50 vs 6.00; U=36,642, Z=-4.21, p<0.001); that is, they believed that the impact of a security event would be worse for them than males did. They did not however feel more vulnerable to security threats (Mdn 4.67 vs 4.83; U=44,532, Z=-0.50, p=0.614).

The other significant gender difference related to descriptive norm. Females were more likely than males to believe that other people implement security measures to protect their devices (Mdn 5.00 vs 4.75; U=40125, Z=-2.54, p=0.011). They did not, however, differ in their perceptions as to whether other people want them to undertake security behaviour to protect themselves (Mdn 4.67 vs 4.83; U=44,675, Z=-0.45, p=0.655). No significant gender differences were found for the coping appraisal perceptions: security self-efficacy (Mdn 5.00 vs 5.33; U=42,574, Z=1.40, p=0.160), response efficacy (Mdn 5.00 vs 5.00; U=43,756, Z=-0.86, p=0.387) and response cost (Mdn 3.50 vs 3.57; U=44,186, Z=-0.66, p=0.507).

These results provide partial support for H2, suggesting that there are some gender specific differences in information security perceptions, with female users believing that the impacts of security events will be more severe, and that others are more likely to be taking action to protect themselves. It was surprising that no significant difference in security self-efficacy was found, given previous research that suggests that females have less technical information technology knowledge and training (Sheng et al. 2010) and that female students have lower levels of computer self-efficacy (He and Freeman 2009). This was explored further in testing H3.

Table 4 summarises participants' self-rated skill with information technology and their previous security training. Differences between genders were analysed using chi-square tests. The majority of participants rated their skill with computers as good or excellent (64.7%), however only 18.9% had previously received any information security training. There were significant differences between females and males in both self-rated skill with information technology (χ^2 (4, N=624) = 15.510; p = 0.004), and whether they had previously received information security training (χ^2 (1, N=624) = 11.061; p = 0.001). That is, females were less likely to have received information security training in the past and considered themselves to have lower levels of skill with information technology. Therefore H3 was supported.

	Females	Males
Self-rated skill with information technology		
Poor	0.5%	0.9%
Below average	3.8%	1.9%
Average	35.1%	26.5%
Good	45.6%	44.9%
Excellent	14.9%	26.1%
Previous information security training		
Yes	14.9%	25.6%
No	85.1%	74.4%

Table 4. Skill with information technology and previous information security training comparison

6 Discussion

This study investigated gender differences in a range of personal information security behaviours as well as potential contributors to security behaviour. As hypothesised, gender differences in security behaviour were found, with males exhibiting stronger behaviour overall. This is consistent with previous research (Gratian et al. 2018; Sheng et al. 2010). Males did not, however, consistently protect themselves better across all of the individual security behaviours considered. The three behaviours where no gender difference was found were: enabling automatic updating of software, securing devices with passwords, and using security software (once installed). These behaviours require less technical skill than those where differences were found: installing security software, enabling firewalls and keeping regular backups, supporting Sheng et al.'s (2010) suggestion that gender effects on security behaviour are mediated by technical knowledge and training, as our results also show that females report lower levels of information technology skill and information security training.

Gender differences were found for some security perceptions but not others. It is interesting that female users believed that the effects of a security threat would be worse for them than males users did, but did not feel more vulnerable, despite believing themselves to have less information technology skill. The higher levels of perceived severity are consistent with females having higher levels of information privacy concerns (Hoy and Milne 2010; Laric et al. 2009; Mohamed and Ahmad 2012), but the lack of

difference in terms of perceived vulnerability is not. However, in research on security perceptions Sasse et al. (2001) found that users tend not to consider their information to be of value to others and therefore view it as not important enough to be targeted. Therefore, while female users appear to perceive the outcomes of a security event as being worse they do not view themselves as more likely to be attacked, perhaps devaluing the worth of their information.

It was surprising to find that there were no significant differences in perceptions of security self-efficacy between female and male users despite the lower levels of information technology skill and security training that female users reported. This finding is inconsistent with early research that showed differences in computer self-efficacy for complex tasks, but not simple ones (Busch 1995) and requires further research.

In terms of general computer attitudes, females have been shown to be driven more by social norms than males (Venkatesh and Morris 2000). Both descriptive norm and subjective norm were considered in the current study and females were found to have higher levels of descriptive norm, but not subjective norm. That is, females were more likely to believe that other people actively protect their own information security, but their perceptions as to whether other people want them to take security measures did not differ from those of males. Descriptive norm has been shown to be a more important predictor of security behaviour than subjective norm in the personal information technology context (Thompson et al. 2017), therefore gender differences in this are likely to contribute to the differences in security behaviour that were observed.

The differences in levels of factors that may influence security behaviour and perceptions identified in this study have implications for how security education, training, and awareness initiatives are designed and conducted, and suggest that knowledge and training differences should be targeted. However, the fact that female levels of the coping appraisal factors of security self-efficacy, response efficacy and response cost were not significantly lower than those of males suggests that there is not a need for gender specific campaigns targeting these factors. The gender differences in security behaviour do not appear to arise from them.

A limitation of this study is that it only involved US participants. Cyr et al. (2017) found that psychological gender (i.e. values such as masculinity or femininity) plays a more important role in website perceptions than biological gender, therefore as different cultures show differences in masculinity/femininity (Hofstede 1983) the potential role of this dimension of national culture in information security behaviour should be considered in future research that builds on the work of Rocha Flores et al. (2014) in the organisational security context.

Future research should also further explore the differences that have been observed in this study, and why they arise. One avenue to consider is that of personality. In a study on organisational information security behaviour, McCormac et al. (2017) found that gender differences in information security awareness disappeared when the personality traits of conscientiousness and agreeableness were taken into account.

7 Conclusion

In this work, we analysed the influence of gender on security behaviours and perceptions in a home computing environment. We have addressed the scarcity of research on gender differences in information security by reporting the first large scale study home users, considering both a range of personal information security behaviours as well as how gender differences may impact determinants of security behaviour. We collected data from a broad range of respondents, and were not limited to a particular subset (e.g. students). Our findings reveal significant differences between males and females for three of the six individual security behaviours, and that overall levels of security behaviour were significantly lower for females than for males. In terms of security perceptions, we found that females were also more likely to perceive a higher level of severity of security threats than males, but perceived their vulnerability to be lower – possibly contributing to the lower overall security behaviour observed. Finally, gender differences were found in social norms with females being more likely to believe that other people implement security measures, although they did not differ in perceptions of whether other people may want them to undertake security measures.

These findings contribute to the behavioural information security field by considering a key individual difference – gender – in the context of security behaviours and perceptions. The results may be of particular relevance when designing security education, training, and awareness initiatives for the broader community as these are often based on models such as PMT (Rogers 1975; Rogers 1983). We

believe that the efficacy of technical and behavioural security countermeasures may be positively influenced by developing them with these individual differences in mind.

8 References

Alshammari, N.O., Mylonas, A., Sedky, M., Champion, J., and Bauer, C. 2015. "Exploring the Adoption of Physical Security Controls in Smartphones," in: *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*. Switzerland: Springer International Publishing, pp. 287-298.

Anderson, C.L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioural Intentions," *MIS Quarterly* (34:3), pp 613-643.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., and Polak, P. 2015. "What do Systems Users have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp 837-864.

Broos, A. 2005. "Gender and Information and Communication Technologies (ICT) Anxiety: Male Self-Assurance and Female Hesitation," *CyberPsychology & Behavior* (8:1), pp 21-31.

Busch, T. 1995. "Gender Differences in Self-Efficacy and Attitudes toward Computers," *Journal of Educational Computing Research* (12:2), pp 147-158.

Cai, Z., Fan, X., and Du, J. 2017. "Gender and Attitudes toward Technology Use: A Meta-Analysis," *Computers & Education* (105), pp 1-13.

Chen, Y., and Zahedi, F.M. 2016. "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China.," *MIS Quarterly* (40:1), pp 205-222.

Chua, S.L., Chen, D.-T., and Wong, A.F.L. 1999. "Computer Anxiety and Its Correlates: A Meta-Analysis," *Computers in Human Behavior* (15:5), pp 609-623.

Cyr, D., Gefen, D., and Walczuch, R. 2017. "Exploring the Relative Impact of Biological Sex and Masculinity–Femininity Values on Information Technology Use," *Behaviour & Information Technology* (36:2), pp 178-193.

Garbarino, E., and Strahilevitz, M. 2004. "Gender Differences in the Perceived Risk of Buying Online and the Effects of Receiving a Site Recommendation," *Journal of Business Research* (57:7), pp 768-775.

Gefen, D., and Straub, D.W. 1997. "Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model," *MIS Quarterly* (21:4), pp 389–400.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., and Ginther, A. 2018. "Correlating Human Traits and Cyber Security Behavior Intentions," *Computers & Security* (73), pp 345-358.

He, J., and Freeman, L. 2009. "Are Men More Technology-Oriented Than Women? The Role of Gender on the Development of General Computer Self-Efficacy of College Students," in: *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

Herath, T., and Rao, H.R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp 154-165.

Hofstede, G. 1983. "National Cultures in Four Dimensions: A Research-Based Theory of Cultural Differences among Nations," *International Studies of Management & Organization* (13:1-2), pp 46-74.

Hoy, M.G., and Milne, G. 2010. "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users," *Journal of Interactive Advertising* (10:2), pp 28-45.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp 83-95.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. 2007. "Social Phishing," *Communications of the ACM* (50:10), pp 94-100.

Laric, M.V., Pitta, D.A., and Katsanis, L.P. 2009. "Consumer Concerns for Healthcare Information Privacy: A Comparison of US and Canadian Perspectives," *Research in Healthcare Financial Management* (12:1), pp 93–111.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp 394-413.

Luciano, E.M., Mahmood, M.A., and Maçada, A.C.G. 2010. "The Influence of Human Factors on Vulnerability to Information Security Breaches.," in: *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

Mamonov, S., and Benbunan-Fich, R. 2018. "The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors," *Computers in Human Behavior* (83), pp 32-44.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. 2017. "Individual Differences and Information Security Awareness," *Computers in Human Behavior* (69), pp 151-156.

Milne, G.R., Labrecque, L.I., and Cromer, C. 2009. "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices," *Journal of Consumer Affairs* (43:3), pp 449–473.

Mohamed, N., and Ahmad, I.H. 2012. "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia," *Computers in Human Behavior* (28:6), pp 2366-2375.

Mwagwabi, F., McGill, T., and Dixon, M. 2018. "Short-Term and Long-Term Effects of Fear Appeals in Improving Compliance with Password Guidelines," *Communications of the Association for Information Systems* (41:1), pp Article 7 (147-182).

Nunnally, J.C. 1978. *Psychometric Theory*, (2nd ed.). New York: McGraw-Hill.

Ong, C.-S., and Lai, J.-Y. 2006. "Gender Differences in Perceptions and Relationships among Dominants of E-Learning Acceptance," *Computers in Human Behavior* (22:5), pp 816-829.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., and Calic, D. 2015. "Factors that Influence Information Security Behavior: An Australian Web-Based Study," in: *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*. Cham: Springer, pp. 231-241.

Ponemon Institute. 2013. "Cost of Data Breach Study: Global Analysis." https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf Retrieved 12 October, 2018.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp 757-778.

Rajivan, P., Moriano, P., Kelley, T., and Camp, L.J. 2017. "Factors in an End User Security Expertise Instrument," *Information & Computer Security* (25:2), pp 190-205.

Rocha Flores, W., Antonsen, E., and Ekstedt, M. 2014. "Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture," *Computers & Security* (43), pp 90-110.

Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp 93-114.

Rogers, R.W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in: *Social Psychophysiology,* J.T. Cacioppo and R.E. Petty (eds.). New York: Guilford Press, pp. 153-176.

Sasse, M., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link'—a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp 122-131.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. 2010. "Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. ," in: *Proceedings of the Sigchi Conference on Human Factors in Computing Systems*. ACM, pp. 372-382.

Siponen, M., Mahmood, A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp 217-224.

Sommestad, T., Karlzén, H., and Hallberg, J. 2015. "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," *International Journal of Information Security and Privacy* (9:1), pp 26-46.

Taylor, S., and Todd, P.A. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2), pp 144-176.

Thompson, N., McGill, T.J., and Wang, X. 2017. "'Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behavior," *Computers & Security* (70), pp 376-391.

Tsai, H.-y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., and Cotten, S.R. 2016. "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective," *Computers & Security* (59), pp 138-150.

Venkatesh, V., and Morris, M.G. 2000. "Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior," *MIS Quarterly* (24:1), pp 115-139.

Williams, S.W., Ogletree, S.M., Woodburn, W., and Raffeld, P. 1993. "Gender Roles, Computer Attitudes, and Dyadic Computer Interaction Performance in College Students," *Sex Roles* (29:7-8), pp 515-525.

Woon, I., Tan, G., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in: *Proceedings of the Twenty-Sixth International Conference on Information Systems*. Las Vegas: pp. 367-380.

Workman, M., Bommer, W.H., and Straub, D. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp 2799-2816.

Appendix

Construct	Items
Perceived severity (Ifinedo 2012; Woon et al. 2005; Workman et al. 2008)	A security breach on my *device* would be a serious problem for me
	Loss of information resulting from hacking would be a serious problem for me
	Having my confidential information on my *device* accessed by someone without my consent or knowledge would be a serious problem for me.
	Having someone successfully attack and damage my *device* would be very problematic for me
	I view information security attacks on me as harmful
	I believe that protecting the information on my *device* is important
Perceived vulnerability (Ifinedo 2012; Siponen et al. 2014; Woon et al. 2005)	I could be subject to a serious information security threat
	I am facing more and more information security threats
	I feel that my *device* could be vulnerable to a security threat
	It is likely that my *device* will be compromised in the future
	My information and data is vulnerable to security breaches:
	I could fall victim to a malicious attack if I fail to follow good security practices
Response cost (Woon et al. 2005; Workman et al. 2008)	Taking security measures inconveniences me
	There are too many overheads associated with taking security measures to protect my *device*
	Taking security measures would require considerable investment of effort
	Implementing security measures on my *device* would be time consuming
	The cost of implementing recommended security measures exceeds the benefits
	The impact of security measures on my productivity exceeds the benefits

Response efficacy (Woon et al. 2005)	Enabling security measures on my *device* will prevent security breaches Implementing security measures on my *device* is an effective way to prevent hackers Enabling security measures on my *device* will prevent hackers from stealing my identity The preventative measures available to stop people from getting confidential personal or financial information on my *device* are effective
Self-efficacy (Anderson and Agarwal 2010)	I feel comfortable taking measures to secure my *device* Taking the necessary security measures is entirely under my control I have the resources and the knowledge to take the necessary security measures Taking the necessary security measures is easy I can protect my *device* by myself I can enable security measures on my *device*
Subjective norm (Adapted from Taylor and Todd 1995)	Friends who influence my behavior think that I should take measures to secure my *device* Significant others who are important to me think that I should take measures to secure my primary *device* My peers think that I should take security measures on my primary *device*
Descriptive norm (Anderson and Agarwal 2010)	I believe other people implement security measures on their *devices* I believe the majority of people implement security measures on their *devices* to help protect the Internet I am convinced other people take security measures on their *devices* It is likely that the majority of home computer users take security measures to protect themselves from an attack by hackers

Copyright

Copyright: © 2018 McGill and Thompson. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 3.0 Australia License, which permits non-commercial use, distribution, and reproduction in any medium, provided the original author and ACIS are credited.