The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/2056-4961.htm

Received 24 July 2020
Revised 9 February 2021
29 April 2021
Accepted 30 April 2021

Exploring potential gender differences in information security and privacy

Tanya McGill
Information Technology, Murdoch University, Perth, Australia, and
Nik Thompson
School of Management and Marketing, Curtin University, Perth, Australia

Abstract

Purpose – Information technology users often fail to adopt necessary security and privacy measures, leading to increased risk of cybercrimes. There has been limited research on how demographic differences influence information security behaviour and understanding this could be important in identifying users who may be more likely to have poor information security behaviour. This study aims to investigate whether there are any gender differences in security and privacy behaviours and perceptions, to identify potential differences that may have implications for protecting users' privacy and securing their devices, software and data.

Design/methodology/approach – This paper addresses this research gap by investigating security behaviours and perceptions in the following two studies: one focussing on information security and one on information privacy. Data was collected in both studies using anonymous online surveys.

Findings – This study finds significant differences between men and women in over 40% of the security and privacy behaviours considered, suggesting that overall levels of both are significantly lower for women than for men, with behaviours that require more technical skill being adopted less by female users. Furthermore, individual perceptions exhibited some gender differences.

Originality/value – This research suggests that potential gender differences in some security and privacy behaviours and perceptions should be taken into account when designing information security education, training and awareness initiatives for both organisations and the broader community. This study also provides a strong foundation to explore information security individual differences more deeply.

Keywords Gender, Information security, Security behaviour, Equity, Privacy behaviour, Individual differences

Paper type Research paper

Introduction

Recent findings from the Ponemon Institute paint a concerning picture of the rising cost of cybercrime. The average cost of a cyber-attack on a business rose 12% to US$13.0m in 2018 (Accenture Security and Ponemon Institute, 2019). Above the direct financial cost from damage to technology and software, significant costs arise from the associated information loss and business disruption. Information security and privacy protection are becoming essential for individuals, as well as for organisations as information technology (IT) pervades all aspects of life. Approximately 27% of data breaches in organisations are caused by end-users (Ponemon Institute, 2018) and home users often do not adopt basic security and privacy measures (Alshammari *et al.*, 2015) or grasp common security issues such as spam or phishing emails (Rajivan *et al.*, 2017). This has led to increases in cybercrimes such as identify theft (The Harris Poll, 2019). While technical solutions to security issues are important, improving human security behaviour is essential to effective

Information & Computer Security
Vol. 29 No. 5, 2021
pp. 850-865
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-07-2020-0125

protection, and security education, training and awareness initiatives can provide guidance on how to respond to these threats (Puhakainen and Siponen, 2010). There has not, however, been much research on how information security and privacy behaviour is influenced by demographic differences (Gratian *et al.*, 2018) and understanding this could be important in identifying users who may be more likely to have poor information security and privacy behaviour (McCormac *et al.*, 2017), and may need targeted support to improve it. With a greater understanding of individual differences, security education, training and awareness initiatives can be customised to increase their efficacy.

In this paper, we focus on one key individual difference – gender. There is previous research showing that gender may influence the perceptions, attitudes and behaviours of individuals on websites (Nosek *et al.*, 2002) and social networking sites (Lin and Wang, 2020), hence, its role in security and privacy behaviour warrants further investigation. This research aims to investigate whether there are any differences in security and privacy behaviours and perceptions between people who identify as women and people who identify as men and if there are, to identify those that may have implications for protecting personal computing users' privacy and securing their devices, software and data. It builds on an earlier exploratory study (McGill and Thompson, 2018) and involves two studies, one focussing on information security and one on information privacy and considers a broad range of personal information security and privacy behaviours. The security and privacy perceptions considered are those that have been identified as potential determinants of security behaviour in previous research (Anderson and Agarwal, 2010; Thompson *et al.*, 2017; Tsai *et al.*, 2016). We address the scarcity of research on potential gender differences in information security and privacy behaviour.

Background

Even well-meaning employees who intend to comply with organisational policies may fail to comply simply because they do not understand what is required of them (Puhakainen and Siponen, 2010); similarly, personal computing users often lack confidence in their ability to protect themselves (McGill and Thompson, 2017). Failure to recognise and accommodate individual differences and the impact they can have on the decisions of users may be a contributor to the impaired effectiveness of otherwise cutting-edge security solutions.

Although little research has examined gender differences in information security or privacy behaviour, some differences have been in IT use and perceptions associated with use have been reported. Two studies found that women are more anxious about using IT (Broos, 2005; He and Freeman, 2009). Another older study found that women perceive software to be more useful than men do, but find it less easy to use (Venkatesh and Morris, 2000). In the past, women have also had less IT experience, knowledge and computer self-efficacy (He and Freeman, 2009). Thompson and Brindley (2020) also found the women are more likely to disclose information on social media than men.

The gender differences in security and privacy behaviour that have been reported include women having higher levels of security and privacy concerns (Mohamed and Ahmad, 2012; Laric *et al.*, 2009; Hoy and Milne, 2010) and better information security awareness (Pattinson *et al.*, 2019). However, other studies have reported that women have a greater susceptibility to phishing attacks (Sheng *et al.*, 2010; Jagatic *et al.*, 2007), poorer password behaviour (Gratian *et al.*, 2018) and a lower likelihood of adopting privacy-protecting behaviours (Milne *et al.*, 2009). Findings such as these suggest that further research is needed to explore potential gender differences in security and privacy behaviours and perceptions to understand their implications.

Many perceptions that individuals hold have been proposed to influence security and/or privacy protection behaviour. These include perceived vulnerability, perceived severity, security self-efficacy, response costs, response efficacy (Mwagwabi *et al.*, 2018; Liang and Xue, 2010) and subjective and descriptive norm (Anderson and Agarwal, 2010), which have all been shown to all influence security intentions or behaviours. Similarly, perceptions such as concerns about the collection of personal information (Choi *et al.*, 2018; Thompson *et al.*, 2020), perceived privacy risk and subjective norm (Lin and Wang, 2020) have been shown to influence privacy protection intentions and behaviour.

Whether gender plays a role is, however, less clear. Several studies have considered whether it may have a direct influence on security and privacy intentions or behaviours (Gratian *et al.*, 2018; Mamonov and Benbunan-Fich, 2018; Shah and Agarwal, 2020), whereas others have modelled it as a potential influence on perceptions such as: perceived risk (Garbarino and Strahilevitz, 2004); information privacy concern (Mohamed and Ahmad, 2012); and perceived vulnerability, security self-efficacy and response efficacy (Chen and Zahedi, 2016). It has also been modelled as a moderating influence (Anwar *et al.*, 2017; Luciano *et al.*, 2010). As few studies have specifically focussed on whether gender plays a role in security behaviour and the applicability of some findings is limited by their age (Milne *et al.*, 2009) or the use of student samples (Gratian *et al.*, 2018), our research provides a new contribution by examining both behaviours and perceptions to explore potential gender differences in two studies of personal computing users.

Research questions and hypotheses

IT users are subject to regular security and privacy threats (e.g. phishing and attacks on software vulnerabilities) and are responsible for taking protective action using measures such as creating secure passwords, backing up and installing software updates. Though some of these activities are covered by workplace policies, the search for factors that influence compliance is ongoing. The research described in this paper compares the behaviours and perceptions of men and women to identify whether any differences may have implications for securing devices, software and data. To observe the role of individual differences, the naturalistic setting of general personal computing use was chosen, to yield the clearest insights into individuals' security behaviour and perceptions without the influence of organisational policy or social desirability bias. The perceptions that are investigated in this research are defined in Table 1.

These perceptions, as well as common security and privacy behaviours, were considered to answer the following two central research questions:

RQ1. Do levels of female and male information security and privacy behaviour differ?

RQ2. Do levels of female and male information security perceptions and IT experience differ?

The results of previous research on potential gender differences in security and privacy behaviour have been mixed. Gratian *et al.* (2018) did not find differences in terms of device securement. Pattinson *et al.* (2015) also found no significant gender differences in work-related computer-based security behaviour and Park and Jang (2014) found no differences in mobile privacy skills. However, Anwar *et al.* (2017) reported gender differences in overall information security behaviour with men reporting more security behaviour. In terms of specific security behaviours, Sheng *et al.* (2010) found female users were more likely to click on links in phishing emails and proceed to provide personal information. Also, in a study by Gratian *et al.* (2018) women had weaker password behaviours in terms of password

Perceptions and source of items	Definitions
Study 1	
Perceived severity Woon *et al.* (2005), Workman *et al.* (2008) and Ifinedo (2012)	The degree to which a user believes that the consequences of security threats would be severe
Perceived vulnerability Woon *et al.* (2005), Ifinedo (2012) and Siponen *et al.* (2014)	The degree to which a user believes that they are likely to experience security-related threats
Security self-efficacy Anderson and Agarwal (2010)	The degree to which a user believes in their own ability to take protective action against security threats
Response efficacy Woon *et al.* (2005)	The degree to which a user believes that available protective measures are effective
Response cost Workman *et al.* (2008), Woon *et al.* (2005)	The degree to which a user believes that there are costs associated with recommended protective behaviours
Subjective norm Adapted from Taylor and Todd (1995)	A user's beliefs as to whether others want them to perform security behaviours
Descriptive norm Anderson and Agarwal (2010)	A user's beliefs as to what most other people do in terms of protective security behaviours
Study 2	
Privacy concerns about the collection Smith *et al.* (1996)	The degree to which a user is concerned that data about their personalities, background or activities are being accumulated
Privacy concerns about secondary use Smith *et al.* (1996)	The degree to which a user is concerned that any collected information may be re-purposed or disclosed to other parties without authorisation
Privacy protection confidence (developed for this study)	A user's confidence in their ability to further protect their privacy

Table 1. Perceptions measured in Studies 1 and 2

strength, changing passwords regularly and use of different passwords for different accounts; in this study, they also had weaker updating behaviours such as not immediately installing updates. Based on this, we anticipate that there may be differences across individual security and privacy behaviours such as backing up of data and software and use of firewalls and privacy settings and hypothesise that:

H1a. Women will have lower overall levels of information security behaviour than men.

H1b. Women will have lower overall levels of information privacy behaviour than men.

Early research on gender differences in IT use found that many people saw computer use as a masculine activity (Williams *et al.*, 1993) and that in the past women have been more anxious about using computers (Broos, 2005). Women consumers have also been shown to perceive a higher risk in online purchasing (Garbarino and Strahilevitz, 2004). Unfortunately, a 2017 meta-analysis indicated that there has been little reduction in the previously observed differences in technology-related attitudes between genders (Cai *et al.*, 2017). However, this meta-analysis found that differences may be more pronounced in specific areas of attitude; for instance, women are more concerned about online privacy risks than men (Mohamed and Ahmad, 2012; Laric *et al.*, 2009; Hoy and Milne, 2010).

A range of security and privacy-related perceptions have been shown to influence the adoption of protective behaviours. These include factors identified in Protection Motivation Theory (Rogers, 1983) as potentially important in determining whether protective behaviour is undertaken: perceived severity and perceived vulnerability (Thompson *et al.*, 2017; Siponen *et al.*, 2014); self-efficacy and response efficacy (LaRose *et al.*, 2008; Tu *et al.*, 2015) and response cost (Liang and Xue, 2010; Mwagwabi *et al.*, 2018). In addition, factors such as subjective norm and descriptive norm have also been shown to influence information security behaviour in some studies (Anderson and Agarwal, 2010; Thompson *et al.*, 2017).

Given that some previous studies have reported gender differences in technology-related attitudes, it is likely that gender differences may exist in information security and privacy perceptions that have been shown to influence protective behaviour (Table 1 for the perceptions considered in this study), and a study by Anwar *et al.* (2017) provides some support for this, as it found differences in security self-efficacy with men having higher levels of security self-efficacy. We, therefore, hypothesize that:

> *H2*. Differences in information security and privacy perceptions will exist between women and men.

Early work in end-user computing suggested that men tended to have higher overall levels of computer skill (Harrison and Rainer, 1992). This difference was subsequently highlighted through meta-analysis, leading to a call for interventions to address this apparent gender gap (American Association of University Women, 1994). However, gender differences in self-reported technology skills still appear to persist (Anwar *et al.*, 2017). In exploring why the women participants in their study were more susceptible to phishing attacks, Sheng *et al.* (2010) reported that they had less security knowledge and training than the men and suggested this as a partial explanation for gender differences in susceptibility to phishing attacks. Therefore, we hypothesise that:

> *H3*. Women will have less IT skills and previous information security training than men.

Method

The target population for this research is people who use devices such as computers, tablets and smartphones for personal use. This paper analyses data collected in two studies, both conducted using anonymous online questionnaires. The studies were conducted in two culturally similar western countries (the US and Australia). The data from each study is analysed separately as each study has a different focus: the first on security behaviours and perceptions and the second on privacy behaviours and perceptions [further information about these studies is available in Thompson *et al.* (2017) and Kininmonth *et al.* (2018)]. Data were collected in a daily use context for these studies; this was for two reasons. Firstly, the prevalence of working from home and *bring your own device* has blurred the line between personal and business use contexts. Secondly, the varying levels of security automation in organisations may introduce an uncontrolled source of variance when surveying users about workplace behaviours. Thus, our findings represent the volitional and habitual behaviours enacted by users, which highlight the individual level differences under examination.

Study 1 – information security perceptions and behaviour

Participants and procedures. In Study 1, a third-party recruiting company was used to obtain participants who were 18 or over, had both a personal computer and a mobile device and came from a wide spectrum of backgrounds. The recruiting company used census balanced random sampling to identify potential participants from their panel members in the USA. Potential participants were contacted via email and invited to complete an anonymous online questionnaire that was hosted on SurveyMonkey.

Survey instrument. The questionnaire first asked about gender, previous information security training and self-reported level of skill with IT. The second section of the questionnaire collected information about security perceptions and behaviours, and to ensure coverage of a broad range of technologies participants were randomly allocated to answer questions about either their personal computer or their mobile device use.

The perceptions measured were perceived severity, perceived vulnerability, security self-efficacy, response efficacy, response cost, subjective norm and descriptive norm. To ensure validity and reliability of the items, we selected items that had been validated in previous security research wherever possible and they were modified for the personal computing domain as necessary (Table 1 for definitions of these perceptions and sources of the measurement items). The items were all measured on seven-point Likert scales from 1 "Strongly Disagree" to 7 "Strongly Agree". Following data collection, reliability testing was conducted and the Cronbach alphas of all constructs relating to perceptions were found to be above 0.9, demonstrating that the scales were reliable (Nunnally, 1978). We then calculated a summary measure of each construct, for each respondent, as the mean of the responses to the items.

Six items were used to measure security behaviour, each of which asked about the performance of a specific common security behaviour (Table 2 for a full list). These items were representative of recommended personal information security behaviours and responses to the items were coded as 1 for "Yes" or 0 for "No" or "Unsure". An overall measure of information security behaviour was also then calculated for each respondent as the sum of the responses to the six items.

Study 2 – privacy concerns and behaviour

Participants and procedures. In Study 2, participants were recruited using snowball sampling. The initial invitations were distributed through social networks, including LinkedIn and Facebook. Potential participants were invited to participate by completing an anonymous online questionnaire that was hosted on the Qualtrics platform. All were over 18 years of age and residents of Australia.

Survey instrument. The questionnaire first gathered general demographic information about participants, including age and gender. The second section of the survey asked questions about the participants' privacy concerns and any protective behaviours that they undertook to address such concerns.

Two aspects of privacy concerns were measured as follows: privacy concerns about collection and privacy concerns about secondary use. Privacy concerns about collection relate to the degree to which a user is concerned that data about their personalities, background or activities are being accumulated by government agencies. Privacy concerns about secondary use refer to the degree to which a user is concerned that any collected

Table 2. Individual security behaviours comparison

	Women (%)			Men (%)			
Security behaviour	Yes	No	Unsure	Yes	No	Unsure	Sig. diff
Have recent backups	43.3	42.8	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	✓

information may then be re-purposed or disclosed to other parties without authorisation. The items for these measures were drawn from Smith *et al.* (1996) and were measured on five-point Likert scales from 1 "Strongly Disagree" to 5 "Strongly Agree". Following data collection, reliability testing was conducted. The Cronbach alpha for privacy concerns about the collection was 0.81 and thus reliable (Nunnally, 1978). The Cronbach alpha for privacy concerns about secondary use was only 0.58, however, as the use of the items with Australian adults was exploratory (Hinton *et al.*, 2004) and because subsequent analysis showed that composite reliability was satisfactory at 0.75 (Hair *et al.*, 2014), the measure was retained as acceptable.

An additional privacy perception, privacy protection confidence, was also measured using one item that was developed for the study as follows: *If you wanted to protect your communication privacy further, how confident are you about your ability to do so*. It was measured on a four-point scale from 1 "No Confidence" to 4 "High Confidence".

Privacy protection behaviours enacted to preserve online privacy were measured using a list of 10 items based on Shelton *et al.* (2015) and respondents indicated whether or not they had adopted each measure (Table 5 for all privacy behaviour items). An overall measure of information privacy behaviour was calculated as the number of privacy behaviours that each participant had adopted.

Results

Study 1 – information security perceptions and behaviour

In Study 1, 624 responses (62.5% female and 37.5% male) were obtained. Levels of adoption of common individual security protections by these female and male participants were compared using χ^2 tests. Significant differences between women and men were found for three of the six individual security behaviours (Table 2). Women were found to be less likely to have recent backups of their device [43.3% versus 53.8%, χ^2 (2, N = 624) = 11.064; p = 0.004]. It was also interesting to find that in this study, they were more likely to be unsure whether they had recent backups (13.8% versus 6.4%). There were also gender differences in whether users had installed security software such as anti-malware [χ^2 (2, N = 624) = 7.805; p = 0.020], with women significantly less likely to have done so. However, no gender differences were found in terms of whether used security software was used [χ^2 (2, N = 624) = 3.749; p = 0.153].

No gender differences in whether users enabled automatic updating of software [χ^2 (2, N = 624) = 3.858; p = 0.145] were found nor in whether they used a password to secure their device [χ^2 (2, N = 624) = 1.346; p = 0.510]. There were, however, gender differences in whether users had a firewall enabled in their home network [χ^2 (2, N = 624) = 13.241; p = 0.001], with women significantly less likely to have done so (64.1% versus 13.7%) and also more likely to be unsure whether a firewall had been enabled (17.7% versus 9.0%).

To compare levels of overall security behaviour and perceptions, non-parametric Mann-Whitney U tests were used as the data did not meet the assumption of normality. As can be seen in Table 3, women had significantly lower levels of overall security behaviour than men (Mdn 4.00 vs 5.00; U = 38,480, Z = –3.33, p = 0.001). *H1a* was, therefore, supported.

Table 3 presents the mean levels of each of the perceptions that were considered in Study 1. Significant differences were found for two of these perceptions, perceived severity and descriptive norm. Women displayed significantly higher levels of perceived severity than men (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 men did. Despite this, they did not feel that they were more vulnerable to security threats than men did (Mdn 4.67 vs 4.83; U = 44,532, Z = –0.50, p = 0.614).

The other difference was in levels of descriptive norm. Women were more likely to believe that other people undertake security measures to protect their devices (Mdn 5.00 vs 4.75; U = 40125, Z = −2.54, p = 0.011). Women did not, however, differ from men in their perceptions of whether others want them to undertake security behaviour to protect themselves (subjective norm) (Mdn 4.67 vs 4.83; U = 44,675, Z = −0.45, p = 0.655). Also, no significant differences were found for any of 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 there are some differences in information security perceptions that are gender-specific, with female users believing that the outcomes of security threats will be more severe and that others are more likely to be taking security behaviours to protect themselves. It was, however, interesting that no significant difference in security self-efficacy was found, given that some previous research suggests that women may have less IT knowledge and security training (Sheng *et al.*, 2010) and lower levels of security self-efficacy (Anwar *et al.*, 2017). This was explored further in testing *H3*.

Table 4 provides a summary of the participants' self-rated skills with IT and their previous security training by gender. The majority of participants of both genders rated their skill with computers as good or excellent (60.5% of women, 71.0% of men), however, few had previously received any information security training (14.9% of women, 25.6% of men). χ^2 tests were used to test whether there were significant gender differences in these

	Women		Men			
	Mean	SD	Mean	SD	p	Sig. diff
Overall 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 perceptions comparison

	Women (%)	Men (%)
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. IT skill and training comparison

measures of IT experience and significant differences were found between women and men in self-rated skill with IT [χ^2 (4, N = 624) = 15.510; p = 0.004] and whether they had previously undertaken information security training [χ^2 (1, N = 624) = 11.061; p = 0.001]. That is, women considered themselves to have lower levels of skill with IT and were less likely to have received information security training in the past. Therefore, *H3* was supported.

Study 2 – privacy concerns and behaviour

In Study 2, 100 responses (45% female and 55% male) were obtained. As in Study 1, the adoption of privacy protections was compared using χ^2 tests. Significant differences were found for four of the privacy protection behaviours, and in each of these cases, men were more likely to have undertaken the protective action (Table 5). Men were significantly more likely to have used a search engine that does not track search history [36.4% versus 11.1%; χ^2 (1, N = 100) = 8.418; p = 0.004] and to have used a Virtual Private Network (VPN) [49.1% versus 17.8%; χ^2 (1, N = 100) = 10.667; p = 0.001]. Only 2.2% of women had used a privacy-enhancing browser plugin (e.g. DoNotTrackMe and privacy badger) compared with 29.1% of men [χ^2 (1, N = 100) = 12.663; $p < 0.001$]. Women had similarly low levels of use of anonymity software such as Tor with men significantly higher, but still exhibiting relatively low levels of use [16.4%; χ^2 (1, N = 100) = 5.499; p = 0.019].

No gender differences were found in whether participants protected their privacy by providing inaccurate or misleading information about themselves [χ^2 (1, N = 100) = 0.300; p = 0.584] or used a temporary username or email address [χ^2 (1, N = 100) = 2.309; p = 0.129] or changed their privacy setting on social media [χ^2 (1, N = 100) = 1.260; p = 0.262]. There were also no significant differences in whether women and men encrypted phone calls, text messages or email [χ^2 (1, N = 100) = 0.780; p = 0.377] or whether they used more complex passwords [χ^2 (1, N = 100) = 0.475; p = 0.491].

To compare levels of overall privacy behaviour and perceptions, non-parametric Mann-Whitney U tests were used as the data did not meet the assumption of normality. As can be seen in Table 6, significantly lower levels of overall privacy behaviour were reported by

Table 5.
Individual privacy behaviours comparison

	Women		Men		
Privacy behaviours	Yes (%)	No (%)	Yes (%)	No (%)	Sig. diff
Used a search engine that does not keep track of your search history	11.1	88.9	36.4	63.6	✓
Used a VPN	17.8	82.2	49.1	50.9	✓
Given inaccurate or misleading information about yourself	40.0	60.0	45.5	54.5	×
Used a temporary username or email address	28.9	71.1	43.6	56.4	×
Changed your privacy settings on social media such as Facebook or Twitter	82.2	17.8	72.7	27.3	×
Encrypted your phone calls, text messages or email	13.3	86.7	20.0	80.0	×
Used more complex passwords	64.4	35.6	70.9	29.1	×
Added a privacy-enhancing browser plugin like DoNotTrackMe or privacy badger	2.2	97.8	29.1	70.9	✓
Used anonymity software such as Tor	2.2	97.8	16.4	83.6	✓

women than men (Mdn 4.00 vs 5.00; U = 900, Z = −2.37, p = 0.018). *H1b* was, therefore, supported.

Table 6 provides the mean levels of the two types of privacy concerns and of participant privacy protection confidence. No significant differences were found for privacy concerns about data collection (Mdn 4.43 vs F 4.57; U = 1,133, Z = −0.72, p = 0.468) or privacy concerns about secondary use of this data (Mdn 5.00 vs 5.00; U = 1,165, Z = −0.56, p = 0.569). Men did, however, report significantly higher levels of privacy protection confidence (Mdn 3.00 vs 2.00; U = 1,715, Z = −3.65, $p < 0.001$). These results provide partial support for *H2*, suggesting that there are some gender-specific differences in information privacy perceptions. While levels of privacy concerns were high across both genders, women felt less confident in their ability to protect their privacy.

Discussion

We set out to investigate whether gender, a fundamental, yet under-researched, individual difference, plays a role in information security and privacy. We considered a range of actual behaviours and user perceptions that have been previously shown to influence these behaviours. As hypothesised, we found some gender differences in security and privacy behaviour, with men exhibiting stronger behaviour overall. This is consistent with previous research (Gratian *et al.*, 2018; Sheng *et al.*, 2010). Men did not, however, consistently protect themselves better across all the individual behaviours we considered.

Gender differences were found for half of the security behaviours having recent backups, installing security software and enabling a firewall. Gender differences were also found in the adoption of individual privacy behaviours, with significant differences in four of the 10 privacy behaviours. These include the use of non-tracking search engines, VPNs, privacy-enhancing browsers and software such as Tor. In all cases, men were more likely to enact these privacy protections. The behaviours where levels of use were not significantly different between genders were, except for use of encryption, those that require less technical skill. This is consistent with prior research showing perceptions about ease of use of personalised cybersecurity influence intention to adopt personalised web browser security measures more strongly for women than men (Addae *et al.*, 2019). This suggests that women may be less likely to adopt the measures which appear to be harder to use, and this could be explained by Sheng *et al.*'s (2010) claim that gender effects on security behaviour are mediated by technical knowledge and training, as our results also showed that the women in Study 1 reported lower levels of IT skill and information security training.

We found gender differences for some security and privacy perceptions but not others. Surprisingly, although on average women did not feel more vulnerable to security threats, they believed that the effects would be worse for them than men did despite believing themselves to be less skilled at IT. The higher levels of perceived severity that female

Table 6. Privacy perceptions and overall privacy behaviour comparison

	Women		Men			
	Mean	SD	Mean	SD	p	Sig.diff
Overall privacy behaviour	2.62	1.58	3.84	2.54	0.018	✓
Privacy concerns (collection)	4.41	0.57	4.35	0.56	0.468	×
Privacy concerns (secondary use)	4.71	0.41	4.80	0.33	0.569	×
Protection confidence	2.25	0.78	2.89	0.76	<0.001	✓

participants reported are consistent with the differences observed in Anwar *et al.* (2017) and with some previous studies where women were found to have higher levels of information privacy concerns (Mohamed and Ahmad, 2012; Laric *et al.*, 2009; Hoy and Milne, 2010), despite there being no significant difference in either kind of privacy concern in Study 2. The lack of gender difference in terms of perceived vulnerability is also consistent with the findings of Anwar *et al.* (2017). Research by Sasse *et al.* (2001) on security perceptions found that users tend to consider that their information is not of value to others, and therefore, view it as not important enough to be targeted. Therefore, while female users may perceive the outcomes of a security event as being worse than men do, they do not view themselves as more likely to be attacked, perhaps because of devaluing the worth of their information.

Given the lower levels of IT skill and security training that female users reported, it was surprising that no significant gender differences in perceptions of security self-efficacy were found in Study 1. Levels of IT and security skills should influence users' perceptions of their ability to protect themselves (Tu *et al.*, 2015), and consistent with this, in Study 2 men reported a significantly higher level of belief in their own ability to take measures to protect their privacy. The similarities in security self-efficacy between women and men in Study 1 may, however, be consistent with early research that showed differences in computer self-efficacy for complex tasks, but not simple ones (Busch, 1995) and requires further research, given that differences in protective behaviour were only observed for actions that may be seen by users as more difficult to implement.

In the past, women have been shown to be driven more by social norms than men in terms of their general attitudes towards computers (Venkatesh and Morris, 2000). In Study 1, descriptive norm and subjective norm as they apply to beliefs about information security were investigated and women were found to have higher levels of descriptive norm than men, but not subjective norm. This means that women were more likely to believe that other people take actions to actively protect their own information security, but their sense of whether other people who are important to them want them to take security measures did not differ from that of men. Descriptive norm is a more important predictor of whether users undertake protective security behaviour than subjective norm in the personal computing context (Thompson *et al.*, 2017), therefore, gender differences in descriptive norm are likely to contribute to the differences in security and privacy behaviour that were observed.

Both men and women reported similar mean levels of privacy concerns, both for collection and for secondary use of data. These levels were relatively high, suggesting that participants did hold concerns about privacy. Interestingly, though, these concerns may not directly translate to behaviour. Overall, privacy protection behaviour was significantly higher for men than women, despite similar levels of both kinds of concern. This suggests that other factors are influencing or moderating the relationship between expressed concern and the enactment of privacy protections.

Implications for practice

Our results have implications for how security education, training and awareness initiatives are designed and conducted and suggest that knowledge and training should be tailored. However, this tailoring must be more nuanced than rolling out gender-specific training programmes. Such an approach may be counter-productive and reinforce gender stereotypes amongst users.

Though women generally enacted fewer security and privacy-protective behaviours overall, it is interesting to consider which specific behaviours did not display gender differences. These tended to be ones that might be perceived to require a lower technical skill and are better known in general. While this is consistent with the lower levels of IT skill and training reported by women it is at odds with the finding that their security self-efficacy was not significantly different. The key difference here may not simply be the level of training, but what motivates an individual user to enact certain behaviours. In some cases, this may be the influence of peers.

Thus, an important implication for practice is that just increasing the *quantity* of individual training for women may not be the most effective strategy. This is consistent with recommendations made by Bullee *et al.* (2017) about identifying phishing emails. While such an approach should have some positive impact, it does not directly address the normative and social influences on protective behaviour. Establishing communities of practice may have a deeper impact, by reinforcing collective responsibility for security and encouraging knowledge sharing. Such communities must be inclusive and ensure adequate representation and participation from all groups to create a positive culture of security behaviour.

When attempting to encourage positive behaviour in this way it is important to adopt an effective strategy for influencing users. Research has shown that behaviour change is more likely when individuals hold a favourable view of others who adopt those behaviours (Todd *et al.*, 2016). Supporting users to develop broader and relatable perceptions of what a security and privacy-conscious individual is, should encourage improved security and privacy behaviour. This principle has been understood and applied in other domains (e.g. public health) not yet in the domain of IT training.

Limitations and future work

A limitation of this research is that it only involved participants from two Western cultures, Australia and the USA. Psychological gender (i.e. values such as masculinity or femininity) has been shown to play a more important role in website perceptions than biological gender (Cyr *et al.*, 2017), therefore, as different cultures show differences in masculinity/femininity (Hofstede, 1983) the potential role of psychological gender in influencing information security behaviour should be considered in future research in non-Western countries that builds on the work of Rocha Flores *et al.* (2014) in the organisational security context.

The differences that have been observed in this study should also be investigated in future research to understand why they arise. Personality may play a role in this as McCormac *et al.* (2017) found that gender differences in organisational information security awareness disappeared when the personality traits of conscientiousness and agreeableness were taken into account; however, Alohali *et al.* (2018) found that the role of personality traits in influencing security behaviour risk levels was associated with gender.

Conclusion

In this study, we analysed whether gender is associated with differences in security and privacy behaviours and perceptions in the personal computing context. We have addressed the scarcity of research on potential gender differences in information security and privacy by reporting on data from two studies and have considered a broad range of information security and privacy perceptions, as well as how gender differences may impact behaviour.

Our findings revealed significant differences between those who identify as women and those who identify as men in over 40% of the behaviours considered, suggesting that overall levels of security and privacy behaviour are significantly lower for women. We also found that women users were more likely to perceive a higher level of security threat severity than men but did not feel more vulnerable to these threats. Also, gender differences in subjective norms were observed with women being more likely to believe that other people protect themselves by adopting security measures; however, no gender differences were found in perceptions of whether other significant people may want them to adopt these measures.

We believe that these results may be particularly relevant to those that design security and privacy education, training and awareness initiatives for the broader community. The effectiveness of organisational security strategies, both technical and behavioural, may be also positively influenced by developing with individual differences in mind.

References

Accenture Security and Ponemon Institute (2019), "The cost of cybercrime", available at: www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed 11 June 2019).

Addae, J.H., Sun, X., Towey, D. and Radenkovic, M. (2019), "Exploring user behavioral data for adaptive cybersecurity", *User Modeling and User-Adapted Interaction*, Vol. 29 No. 3, pp. 701-750.

Alohali, M., Clarke, N., Li, F. and Furnell, S. (2018), "Identifying and predicting the factors affecting end-users' risk-taking behavior", *Information and Computer Security*, Vol. 26 No. 3, pp. 306-326.

Alshammari, N.O., Mylonas, A., Sedky, M., Champion, J. and Bauer, C. (2015), "Exploring the adoption of physical security controls in smartphones", *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer International Publishing.

American Association of University Women (1994), "Shortchanging girls, shortchanging America: executive summary: a nationwide poll that assesses self-esteem, educational experiences, interest in math and science, and career aspirations of girls and boys ages 9-15", available at: www.aauw.org/files/shortchanging-girls-shortchanging-america-executive-summmary.pdf (accessed 15 January 2020).

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. and Xu, L. (2017), "Gender difference and employees' cybersecurity behaviors", *Computers in Human Behavior*, Vol. 69, pp. 437-443.

Broos, A. (2005), "Gender and information and communication technologies (ICT) anxiety: male self-assurance and female hesitation", *CyberPsychology and Behavior*, Vol. 8 No. 1, pp. 21-31.

Bullee, J.W., Montoya, L., Junger, M. and Hartel, P. (2017), "Spear phishing in organisations explained", *Information and Computer Security*, Vol. 25 No. 5, pp. 593-613.

Busch, T. (1995), "Gender differences in self-efficacy and attitudes toward computers", *Journal of Educational Computing Research*, Vol. 12 No. 2, pp. 147-158.

Cai, Z., Fan, X. and Du, J. (2017), "Gender and attitudes toward technology use: a meta-analysis", *Computers and Education*, Vol. 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*, Vol. 40 No. 1, pp. 205-222.

Choi, H., Park, J. and Jung, Y. (2018), "The role of privacy fatigue in online privacy behavior", *Computers in Human Behavior*, Vol. 81, pp. 42-51.

Cyr, D., Gefen, D. and Walczuch, R. (2017), "Exploring the relative impact of biological sex and masculinity–femininity values on information technology use", *Behaviour and Information Technology*, Vol. 36 No. 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*, Vol. 57 No. 7, pp. 768-775.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018), "Correlating human traits and cyber security behavior intentions", *Computers and Security*, Vol. 73, pp. 345-358.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2014), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage, Thousand Oaks, CA.

Harrison, A.W. and Rainer, R.K. (1992), "The influence of individual differences on skill in end-user computing", *Journal of Management Information Systems*, Vol. 9 No. 1, pp. 93-111.

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", *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

Hinton, P.R., Browlow, C., Mcmurray, I. and Cozens, B. (2004), *SPSS Explained*, Routledge, New York, NY.

Hofstede, G. (1983), "National cultures in four dimensions: a research-based theory of cultural differences among nations", *International Studies of Management and Organization*, Vol. 13 No. 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*, Vol. 10 No. 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 and Security*, Vol. 31 No. 1, pp. 83-95.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007), "Social phishing", *Communications of the ACM*, Vol. 50 No. 10, pp. 94-100.

Kininmonth, J., Thompson, N., Mcgill, T. and Bunn, A. (2018), "Privacy concerns and acceptance of government surveillance in Australia", *Proceedings of the 29th Australasian Conference on Information Systems (ACIS 2018)*.

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*, Vol. 12 No. 1, pp. 93-111.

Larose, R., Rifon, N.J. and Enbody, R. (2008), "Promoting personal responsibility for internet safety", *Communications of the ACM*, Vol. 51 No. 3, pp. 71-76.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: a threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7, pp. 394-413.

Lin, X. and Wang, X. (2020), "Examining gender differences in people's information-sharing decisions on social networking sites", *International Journal of Information Management*, Vol. 50, pp. 45-56.

Luciano, E.M., Mahmood, M.A. and Maçada, A.C.G. (2010), "The influence of human factors on vulnerability to information security breaches", *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017), "Individual differences and information security awareness", *Computers in Human Behavior*, Vol. 69, pp. 151-156.

McGill, T. and Thompson, N. (2017), "Old risks, new challenges: exploring differences in security between home computer and mobile device use", *Behaviour and Information Technology*, Vol. 36 No. 11, pp. 1111-1124.

McGill, T. and Thompson, N. (2018), "Gender differences in information security perceptions and behaviour", *Proceedings of the 29th Australasian Conference on Information Systems (ACIS 2018)*.

Mamonov, S. and Benbunan-Fich, R. (2018), "The impact of information security threat awareness on privacy-protective behaviors", *Computers in Human Behavior*, Vol. 83, pp. 32-44.

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*, Vol. 43 No. 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*, Vol. 28 No. 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*, Vol. 41 No. 1, pp. 147-182.

Nosek, B.A., Banaji, M.R. and Greenwald, A.G. (2002), "Harvesting implicit group attitudes and beliefs from a demonstration web site", *Group Dynamics: Theory, Research, and Practice*, Vol. 6 No. 1, pp. 101-115.

Nunnally, J.C. (1978), *Psychometric Theory*, McGraw-Hill, New York, NY.

Park, Y.J. and Jang, S.M. (2014), "Understanding privacy knowledge and skill in mobile communication", *Computers in Human Behavior*, Vol. 38, pp. 296-303.

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D. and Mccormac, A. (2019), "Matching training to individual learning styles improves information security awareness", *Information and Computer Security*, Vol. 28 No. 1, pp. 1-14.

Pattinson, M., Butavicius, M., Parsons, K., Mccormac, A. and Calic, D. (2015), "Factors that influence information security behavior: an australian web-based study", *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, Cham.

Ponemon Institute (2018), "2018 Cost of data breach study: global overview", available at: https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/ (accessed July 2020).

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Rajivan, P., Moriano, P., Kelley, T. and Camp, L.J. (2017), "Factors in an end user security expertise instrument", *Information and Computer Security*, Vol. 25 No. 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 and Security*, Vol. 43, pp. 90-110.

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*, Vol. 19 No. 3, pp. 122-131.

Shah, P. and Agarwal, A. (2020), "Cybersecurity behaviour of smartphone users in India: an empirical analysis", *Information and Computer Security*, Vol. 28 No. 2, pp. 293-318.

Shelton, M., Rainie, L., Madden, M., Anderson, M., Duggan, M., Perrin, A. and Page, D. (2015), "Americans' privacy strategies Post-Snowden", available at: www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ (accessed 15 Mar 2019).

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", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

Siponen, M., Mahmood, A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51 No. 2, pp. 217-224.

Smith, H., Milberg, S. and Burke, S. (1996), "Information privacy: measuring individual's concerns about organizational practices", *MIS Quarterly*, Vol. 20 No. 2, pp. 167-196.

Taylor, S. and Todd, P.A. (1995), "Understanding information technology usage: a test of competing models", *Information Systems Research*, Vol. 6 No. 2, pp. 144-176.

The Harris Poll (2019), "Cyber safety insights report United States (US) results", available at: www.symantec.com/content/dam/symantec/docs/about/2018-norton-lifelock-cyber-safety-insights-report-us-results-en.pdf (accessed 15 July 2019).

Thompson, N. and Brindley, J. (2020), "Who are you talking about? Contrasting determinants of online disclosure about self or others", *Information Technology and People*.

Thompson, N., McGill, T.J. and Wang, X. (2017), "Security begins at home": determinants of home computer and mobile device security behavior", *Computers and Security*, Vol. 70, pp. 376-391.

Thompson, N., McGill, T., Bunn, A. and Alexander, R. (2020), "Cultural factors and the role of privacy concerns in acceptance of government surveillance", *Journal of the Association for Information Science and Technology*, Vol. 71 No. 9, pp. 1129-1142.

Todd, J., Kothe, E., Mullan, B. and Monds, L. (2016), "Reasoned versus reactive prediction of behaviour: a meta-analysis of the prototype willingness model", *Health Psychology Review*, Vol. 10 No. 1, pp. 1-24.

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 and Security*, Vol. 59, pp. 138-150.

Tu, Z., Turel, O., Yuan, Y. and Archer, N. (2015), "Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination", *Information and Management*, Vol. 52 No. 4, pp. 506-517.

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*, Vol. 24 No. 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*, Vol. 29 Nos 7/8, pp. 515-525.

Woon, I., Tan, G. and Low, R. (2005), "A protection motivation theory approach to home wireless security", *Proceedings of the Twenty-Sixth International Conference on Information Systems*. Las Vegas.

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*, Vol. 24 No. 6, pp. 2799-2816.

Corresponding author
Tanya McGill can be contacted at: t.mcgill@murdoch.edu.au