INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Published Online: 24 December 2022 Vol 12, Issue 12, (2022) EISSN:2222-6990

# Factors That Influence Information Security Behaviour of Home User

Mohd Sharulnizam Kamarulzaman[1,2], Shamila Mohamed Shuhidan[1], Abdul Jalil Toha[3]

[1]Faculty of Information Management, Universiti Teknologi MARA, UiTM Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia, [2]Cybersecurity Malaysia, Level 4, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia, [3]Bahagian Pembangunan Kurikulum Kementerian Pendidikan Malaysia, Aras 4-8, Blok E9, Kompleks Kerajaan Parcel E, Pusat Pentadbiran Kerajaan Persekutuan, Presint 1, 62000 Putrajaya, Malaysia

## Abstract

Pandemic Covid-19 situation has enforced most companies imposes their staff to work from home basis as mode of operational. Due to that the number of home computer users is increasing faster than ever. This scenario indirectly highlighted home users' information security as an important field to be investigated. This is not only a matter of securing home users' personal and work information, but also because internet users who access from home provide an ideal breeding ground for security hackers targeting organisations and individuals. Therefore, this paper aims to investigate the factors that influence the information security behaviour of home user. As for this study, 201 respondents among employees in an ICT agency are being analyzed using quantitative approach through the online survey questionnaires. From the findings, it has been concluded that the perceived severity, perceived susceptibility, response efficacy, cues to action and perceived benefit has been identified as the factors that influenced the information security behaviour of home users. Perceived severity was found to be the factor that influenced how users react to implement or not the security safety measures while accessing information. Although respondents do not feel they are possible targets for security threats, they recognize that the result of a security breach would have a significant impact on them. It might be irrational to suppose, that any security experience, knowledge or history background by individuals is the way they act at home. It is therefore hoped to see policy makers or authorised bodies design and implement security awareness campaigns and programs so that users are effectively informed about threats and the skills they can use to mitigate security threats and thereby improve the security climate of users. Where the majority of IS research based on behavioral IS within an organizational framework, "security of home users" demands greater attention from researchers in order to provide an improve analysis and proper practice on home user’s security behavior.

**Keywords:** Information Security Behaviour, Home User, Security, Threats, Ethical

## Introduction

The rising number of Internet users throughout the globe, including in Malaysia, has resulted in a rise in the number of security events caused by users, and the cost of mitigating these occurrences has been substantial (Johnston & Warkentin, 2010). According to Digital 2021 data, there will be around 4.66 billion Internet users in the globe by January 2021, of which 2 billion will be computers including servers, desktops, and laptops. According to these global figures, there were 27.43 million Internet users in Malaysia in 2020, and their number increased by 738 thousand (+2.8%) in 2021. According to this data, household Internet connectivity in Malaysia increased by 91.7 percent in 2020 compared to 90.1% in 2019, as reported by the Department of Statistics Malaysia (DOSM). Since the reported rise in Internet users is directly connected to these studies of information security, attention should be drawn to these studies of home user information security behaviour in light of the Covid-19 Pandemic in particular. The majority of employees from across the globe have been directed to work from home, posing a threat to the company and the Internet as a whole. In contrast to employees in the workplace, home users often do not get information security training, nor are they supported in the case of a security breach or security threat. The enormous number of home users constituted a key weakness in the infrastructure for preserving information security (Anderson & Agarwal, 2010). It was acknowledged that public behaviour might imperil other Internet users and organisations in general, and that, in the worst-case scenario, dependence on organization or individual Internet transactions could increase if web infrastructure dependability and security are compromised (Anderson & Agarwal, 2010). While home users are very likely to supply important information to hackers and attackers, organisations should also be concerned about the security of home users' activities such as, email, online banking, instant messaging, stock trading and online shopping. This is due to the fact that infected home computers are an excellent breeding ground for hackers and disseminators of illegal or morally dubious content.

The end user is often seen as the weakest link and is frequently targeted by hackers. Adoption and potential impacts of computer safety measures are advancing more slowly than criminal activity, resulting in an increase in computer security incidents. Therefore, we may want to investigate if the problem's fundamental cause is technology or humans. Despite technological advancements, security risks continue to be a serious concern. It is recognised that the contribution of individuals is crucial for a lasting solution. Safety is seen as a concern for individuals, and individuals are viewed as the weakest security link. This study will add to the growth of existing research in the field of information security for home users. The purpose of this study is to determine the factors that influence the information security behaviour of home users and to investigate whether or not these factors have an effect on users.

The majority of research on information security are undertaken in organisational settings (Cilliers, 2019; Hooper & Blunt, 2019). Due to environmental variations, such as the importance of competences, training, awareness sessions, and the presence of rules and policies enforced by organisations, this study cannot be simply transferred to the domestic setting. However, the notions of information security pertaining to users are still applicable and may serve as a guide. Therefore, it is vital to study the home environment and how individuals might be urged to take extra precautions to protect their personal information's when working from home.

## Literature Review

The 2010 Fear Appeals Model (FAM) by Johnston and Warkentin, drawn on Rogers' Motivation for Protection (PMT) theory, serves as one of the study's theoretical foundations (Rogers, 1975; Rogers, 1985). For a very long time, fear appeals have been used to persuade individuals to perform the required action, notably in IT security (Johnston & Warkentin, 2010). The concept that reasoning and fear influence appeal is founded in FAM, according to which people may be persuaded to defend themselves from different physical, psychological, and social hazards (Williams, 2012). Rogers created the theory of protection motivation (PMT) in 1975 to comprehend fear appeals, how individuals respond to them, and their consequences for humans. PMT is derived from psychology and has been modified to forecast how end-users would react to certain situations or what they wish to accomplish (Williams, 2012). The premise of this theory is that individuals would attempt to protect themselves from damage or hazards. Motivation for protection was characterised by Rogers (1975) as a variable that not only sustains, but also supports and leads action. The PMT theory defines the elements of a fear appeal that elicit a response from an audience. Perceptions of threat severity, susceptibility, and response efficacy are positioned as primary antecedents of information security behaviour among home users. The perceived threat severity and perceived threat susceptibility relate to the belief that the audience of the fear appeal has on the significance of the danger and the risk. In contrast, response efficacy implies that a person is more likely to respond if he or she believes that protective measures may mitigate a danger. Response efficacy is also the biggest predictor of the willingness to engage in a protective activity. Anderson and Agarwal (2010) also discuss the information security behaviour of home users in their research.

In addition, the Health Belief Model (HBM) is adopted from medical literature for the purpose of studying the computer safety behaviours of users. In the literature on information security, Ng et al (2009) used HBM to investigate employee computer safety activities. The health belief model is complex, including several significant conceptual constructs for computer safety practise that are not captured in IS adoption or other healthcare theories. For the purpose of this study, two HBM-related components are studied. In HBM, action cues may be significant for computer security behaviour. Indicators of action might include the organization's safety awareness activities. While perceived benefit refers to an individual's confidence in the relative effectiveness of the security threat control activity. Here, the perceived benefits pertain to a user's trust in the efficacy of information security. A greater perception of rewards will enhance information security.

In Malaysia, there have been a few researches on the information security behaviours of employees, but these studies have not included an in-depth evaluation of the employees in their home environments. Therefore, the objective of this research is to determine the characteristics that impact a user's information security behaviour in their home environment.

## Research Methodology

This research was intended to determine the factors that influence information security behaviour of home users. A quantitative research approach therefore deals with quantification and regression variables to produce information. According to Creswell (2017), quantitative research is getting the perceptions, opinion and thought from a large population regarding particular issues of investigation. The data collection used in this research was online survey, through convenience random sampling among employees from one ICT agency in Selangor. About 201 respondents answered the online survey and Statistical Package of Social Scientist version 26 Software were used as a platform to analyse Frequency Analysis, Reliability Test Result, and Descriptive Analysis in the study.

## Findings

This section discusses the findings from this study by explaining the Frequency Analysis, Reliability Test Result, and Descriptive Analysis in the study to identify factors that influence the information security behaviour of home users.

### Frequency Analysis

Table 1 presents the demographic profile of the respondents. Out of the feedbacks from 201 respondents, 120 were female and 81 were male. The range of the age of the respondents is between 25 years old and above, majority, i.e. 56 of them were between 36 - 40 years old and the lowest, i.e. 15 of them were age 25 years old and below.

Table 1
*Demographic Profile*

| | | Frequency | Percentage (%) |
|---|---|---|---|
| Gender | Male | 81 | 40.3 |
| | Female | 120 | 59.7 |
| Age | 25 years old and Below | 15 | 7.5 |
| | 26 -30 years old | 31 | 15.4 |
| | 31 -35 years old | 52 | 25.9 |
| | 36 - 40 years old | 56 | 27.9 |
| | 41 years old and Above | 47 | 23.4 |
| Job Position | Top Level Management | 23 | 11.4 |
| | Middle / Executive Level | 78 | 38.8 |
| | Operational / Supporting | 31 | 15.4 |
| | Technical Level | 42 | 20.9 |
| | Others | 27 | 13.4 |
| Education Background | PhD | 11 | 5.5 |
| | Master | 38 | 18.9 |
| | Bachelor's Degree | 126 | 62.7 |
| | Diploma | 21 | 10.4 |
| | STPM/SPM or any Certificate | 5 | 2.5 |
| Working Experience | Below 1 year | 10 | 5.0 |
| | 1 – 4 years | 31 | 15.4 |
| | 5 – 8 years | 47 | 23.4 |
| | 9 – 12 years | 34 | 16.9 |
| | Above 12 years | 79 | 39.3 |
| Household Size | Small (1 – 2 persons) | 43 | 21.4 |
| | Medium (3 – 4 persons) | 109 | 54.2 |
| | Large (5 persons and above) | 49 | 24.4 |
| Technology Tools and Device | Laptop | 178 | 34.4 |
| | iPad | 76 | 14.7 |

| | | | |
|---|---|---|---|
| | Smartphone | 197 | 38.0 |
| | Personal Computer | 66 | 12.7 |
| | Others | 1 | 0.2 |
| Category of Activity | Office Work | 177 | 21.5 |
| | Financial and Banking | 167 | 20.3 |
| | Online Education | 130 | 15.8 |
| | Online Shopping | 157 | 19.1 |
| | Social Media | 177 | 21.5 |
| | Others | 16 | 1.9 |
| Hours Spent | 2 hours and below | 5 | 2.5 |
| | 3 – 5 hours | 61 | 30.4 |
| | 6 – 8 hours | 101 | 50.2 |
| | 9 hours and above | 34 | 16.9 |

Most of the respondents comes from Middle and Executive Level staffs with 78 respondents and lowest, i.e. 23, represent Top Level Management. Average education of the respondents is Bachelor’s Degree holder with most of them already have experience in work between 12 years and more. The survey shows that most of the respondents come from medium households’ size with 3 to 4 persons in a family. Smartphones and laptop are the most preferred tool or device used as a medium to retrieve information, i.e. 197 and 178 that mostly used for office work and social media usage, i.e. 177 respondents. The most time that they spent are between 6 to 8 hours per day to search of information using the said tool and device.

**Reliability Test**

The value of Cronbach's Alpha has been determined by researchers to test the reliability and consistency of the questions used by each variable. Consistency and reliability have improved where the Cronbach alpha value is nearer than 1.00 and the corresponding value of the Cronbach alpha must be greater than 0.6 if it is to be accepted (Woon et al., 2005). Therefore, the following table 2. summarized the test findings.

Table 2 *Cronbach Alpha Result*

| Variables | No. of Item Tested | Cronbach’s Alpha |
|---|---|---|
| Security Behaviour of Home Users | 8 | 0.864 |
| Perceived Severity | 6 | 0.803 |
| Perceived Susceptibility | 5 | 0.843 |
| Response Efficacy | 6 | 0.867 |
| Cues to Action | 6 | 0.883 |
| Perceived Benefit | 6 | 0.889 |

Based on the value of Cronbach's Alpha, the findings show that the instrument used is appropriate and does not show any discrepancy. The overall Cronbach’s Alpha result was above 0.7, as agreed by Sekaran & Bougie (2016) with minimum result of 0.60; otherwise it will not fit the analysis requirement. The highest score is 0.889 for Perceived Benefits with 6 items tested, the second highest score with 6 items tested is Cues to Action with 0.883, Response Efficacy with 5 items tested and the score is 0.867, Security Behaviour of Home

Users with 8 items and the score is 0.864, Perceived Susceptibility with 5 items tested and score result is 0.843 and the least score is 0.803 with 6 items tested under Perceived Severity.

### Descriptive Analysis

Descriptive analysis of each variable used in this study is show in Table 3. With the Likert scale used between one to five, i.e. one is strongly disagreed and five is strongly agree. The results show that the mean value of each variable in relation to factors that influence information security behaviour of home user, which is 4.21 which indicates that the responses agree about it.

Table 3 Descriptive analysis for each variable

| Item | Mean | Std. Deviation |
|---|---|---|
| Security Behavior of Home Users | 4.14 | 0.939 |
| Perceived Severity | 4.57 | 0.622 |
| Perceived Susceptibility | 3.65 | 1.084 |
| Response Efficacy | 4.39 | 0.694 |
| Cues to Action | 4.02 | 1.005 |
| Perceived Benefit | 4.47 | 0.702 |
| **Overall Average Variables** | **4.21** | **0.841** |

### Results

Result from the descriptive analysis shows in Table 3 that the perceived severity with 4.57 mean result was found to be the factor that influenced how home users react to implement or not the security features on their devices. This shows that loss of information due to hacking activities are very concerned issues for most of the respondents. Although respondents do not feel they are possible targets for security threats, they recognize that the result of a security breach would have a significant impact on them (e.g., hacking of personal information). This finding is consistence in other related studies that perceived severity has typically been shown to affect security motivations in the organizational domain (Vance et al., 2013). Adding to this, the results on the role of perceived severity of a user in personal handling of information's were quite mixed. Woon et al (2005) observed that users when they felt threaten and unsecure that they might be a victim of security breach, they are more likely to automatically enable their security features. In contrast, study by Zhang et al (2017) found that password protection activity was not anticipated substantially, and Tsai et al (2016) surprisingly found that magnitude was considered to have a negative effect on users' security intentions and behaviour.

The second finding on the descriptive analysis with an average dimension of 4.47 is perceived benefit. The value is valid to shows that this factor is suitable as determine factor to measure user's belief in practicing information security does gives them the benefit. This is supported by a study by (Ng et. al., 2009). Both constructs for this factor does shows high value mean. This shows that users already practice safety protection behaviour in normal routine such as checking any attachment or email received before opening them that can lead to spread of a virus. Having to do this routine will prevent them from getting attacked. The scores do shows evenly that users mostly agreed on the benefit of taking preventive security measures. The third factor that influence with a score of 4.39 is response efficacy. Response efficacy variable is to understand the user's belief as to whether the recommended step highlighted will help them to avoid any threats. The results show that user agree to enable and take security measures that can prevent security breaches on their personal information and identity and it does support the similar response by the same study from McGill & Thompson (2017) indicates that if a person feels that protecting measures can minimize a threat, he or she is more likely to act.

Out of five factors, perceived susceptibility gets the lowest score with 3.65 value. Perceived susceptibility is to examine the user's belief that they will someday receive threat on their information. The score does show a lowest result from most of the respondents. Perhaps due to the background and the nature of respondents working environment, from IT security agency, with an assumption that the user's degree of alertness and preparedness if the threat is occurred in near future is very high as mentioned by (McGill & Thompson, 2017).

On the basis of the results of the survey, a number of responses were compiled on the obstacles that respondents felt were necessary for them to practise information security safety in their homes. This may be shown using Table 2.0. The majority of respondents said that gaining access to the Internet network itself is the most difficult aspect of obtaining constantly updated security measures. The majority of updates take a reasonable amount of time to complete. Others said that when they are in their comfort zone at home, they tend to disregard and disobey any security regulations. This is a typical user behaviour, only manifesting itself when there is a serious danger. Sharing devices with other family members also contributes to a lack of security motivation, since passwords are the least desirable security measure to consider, as it will benefit all family members who use the shared devices without them. This is corroborated by a study by Gundu, (2019), which found that users express behavioural intentions rather than actual behaviours owing to a lack of motivation. In essence, intentions do not always perfectly translate into actions. Users seem to prefer the concept of these automatic security solutions owing to their usability and manageability. The poll also collected suggestions for such activities. Considering the findings of the surveys, such required and coercive actions are also important for home users if the overall security is to be improved. Although users at home often have the option of employing automated security measures, it is up to their discretion whether they want to do so or not.

## Conclusion

In conclusion, the security of home users should be an important area of study in the field of information security. This is not just an issue of safeguarding the personal and professional information of home users in their homes, but also because Internet users in their homes provide the ideal breeding ground for hackers who target companies and individuals, as well as those who propagate illegal or morally questionable material. Due to this, it is essential to investigate and evaluate the information security practises of home users. Whereas the bulk of IS research focuses on behavioural IS within an organisational framework, it is contested that "home user security" requires more attention from academics. Despite the fact that home user security behaviour and employee compliance with IS Security procedures and guidelines in an organisational context are identical, distinguishing characteristics must be considered in order to provide an improved analysis and best practises for home user security behaviour. Fear, attitudes, and descriptive norms, which may potentially have an influence on information security behaviour, may be examined in a future research as potential additions to the existing model.

Therefore, it is hoped that security awareness campaigns and programmes will be designed and implemented in the context of policymakers or authorised bodies so that users are effectively informed about threats and the skills they can use to mitigate security threats, thereby improving the security climate of users. It may be required to employ a customised method in order to deliver security messages to individuals with the correct content and at the right frequency. In addition to employing safety awareness programmes, authorities should consider a variety of techniques for communicating safety and security messages to all users, both within the organisation and at home, in order to influence users' attitudes toward IS security, to emphasise the significance of IS security, to explain policies and regulations, and to emphasise users' responsibilities for IS security. In content, awareness training often covers security events, potential threats, fundamental IS security concepts, how good safety habits are formed, and recommended assistance in the case of security difficulties. In their home environments, end users get less formal instruction on IS security awareness. Self-study and practical experience are the primary sources of IS security expertise. Obviously, some individuals may have received training at their place of employment, but there is little evidence to suggest that this training is transferred to the home for the purpose of enhancing safety. There is an additional social factor-based method for affecting the security awareness of home users. The study by Ng and Rahim (2005) reveals that the media, family, and co-workers all play an important part in developing a healthy information security behaviour.

## Acknowledgement

Thank you to the Faculty of Information Management, Universiti Teknologi Mara Puncak Perdana Branch, Shah Alam, Associate Professor Dr. Shamila Mohamed Shuhidan and En. Abdul Jalil Toha for the guidance and assistance throughout this research.

## Corresponding Author

Mohd Sharulnizam Kamarulzaman
Faculty of Information Management, Universiti Teknologi MARA, UiTM Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia
Email: sharul.aimer@gmail.com

## References

Anderson & Agarwal. (2010). Practicing safe computing: A multimethod empirical examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613. https://doi.org/10.2307/25750694

Cilliers, L. (2019). Wearable devices in Healthcare: Privacy and Information Security issues. *Health Information Management Journal, 49*(2-3), 150-156. doi:10.1177/1833358319851684

Creswell, J. W., & Sinley, R. C. (2017). Developing a culturally-specific mixed methods approach to Global Research. *KZfSS Kölner Zeitschrift Für Soziologie Und Sozialpsychologie, 69*(S2), 87-105. doi:10.1007/s11577-017-0453-2

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*, 94–102.

Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of it employees. *Behaviour & Information Technology, 39*(8), 862-874. doi:10.1080/0144929x.2019.1623322

Johnston & Warkentin. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549. https://doi.org/10.2307/25750691

McGill, T., & Thompson, N. (2017). Old risks, new challenges: Exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology, 36*(11), 1111-1124. doi:10.1080/0144929x.2017.1352028

Ng, B., Kankanhalli, A., & Xu, Y. (. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi:10.1016/j.dss.2008.11.010

Ng, B.-Y., & Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. In *In Proceedings of the Ninth Pacific Asia Conference on Information Systems* (pp. 7–10). Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1132&context=pacis2005

Sekaran, U., & Bougie, R. (2010). Research method for business: A skill building approach, 5th edition. In United States: John Wiley & Sons Inc.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150. doi:10.1016/j.cose.2016.02.009

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in Information Systems. *Journal of Management Information Systems, 29*(4), 263-290. doi:10.2753/mis0742-1222290410

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. *Association for Information Systems - 26th International Conference on Information Systems, ICIS 2005: Forever New Frontiers*, 367–380.

Williams, K. C. (2012). Fear appeal theory. *Research in Business and Economics Journal*, 5, 1- 21.

Zhang, S., Grenhart, W. C., McLaughlin, A. C., & Allaire, J. C. (2017). Predicting computer proficiency in older adults. *Computers in Human Behavior, 67*, 106-112. doi:10.1016/j.chb.2016.11.006