Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN
https://www.amerabra.org

E-B Environment - Behaviour Proceedings Journal

ICIS2022Penang
https://fim.uitm.edu.my/index.php/research/conference/342-icis-2022
5th International Conference on Information Science
Royale Chulan, Penang, Malaysia, 19-21 Sep 2022
Organised by Faculty of Information Management, UiTM, Malaysia

Systematic Literature Review: Information security behaviour on smartphone users

Ferdinand Jilan Dawie[1], Mohamad Noorman Masrek[2], Safawi Abdul Rahman

[1] Faculty of Information Management, Universiti Teknologi MARA, Selangor, Malaysia

Email of All Authors: Email of All Authors: jilanferdinand@gmail.com, mnoorman@uitm.edu.my, safawi@uitm.edu.my
Tel of 1st Author: 013-8051241/603-79622001

Abstract
Information such as bank access, password, and location data stored in the smartphone has become the primary target for cybercriminals. As the users are frequently stated as the weakest link in the information security chain, therefore, there is a need to investigate users' security behavior in the smartphone context. Using the systematic literature review approach, a total of 48 research articles were analyzed to summarizes the developments of Information Security literature on smartphone users. The findings suggest, Qualitative Approach are most adopted approach and Protection Motivation Theory is the most adopted theory in this field.

Keywords: Smartphone user; Information Security; Security Behaviour; Literature review.

DOI: https://doi.org/10.21834/ebpj.v7iSI10.4133

1.0 Introduction

The smartphone is undoubtedly the most convenient piece of technology ever made by humankind throughout history. The connectivity to the internet and the numerous dynamic applications on the smartphone are able to support users' daily needs, thus making humans becoming even more inseparable from the function of the smartphone in their daily life. Besides that, the smartphone is reported to be the most frequently used technology compared to the computer. This is because the computer owner may have a smartphone but not every smartphone owner owns a computer. In addition, the smartphone users are inclusive as their users can range from toddlers to elders.

Ever since the major pandemic outbreak started in early 2020, many organizations have directed their business operation virtually, especially banks, thus making the smartphone becoming a "walking sever" to store banking data and other sensitive information. With the integration of smartphone users' financial, business, and personal data, the smartphone has become the main target for many cyber criminals worldwide. In addition, one of the most targeted information security breaches on the smartphone in the year 2021 is the users' bank access information and financial information (Kaspersky., 2022). The risk of unauthorized access to this sensitive information on the smartphone can be achieved through malware, spyware, and information phishing (Verkijika, S. F., 2019; Butler, R., 2021; Kaspersky., 2022). Depending only on security technology alone is not enough to prevent this attack. Hence, it also requires the users to be well concerned about their data security.

Information is known as "processed data" or "data that has a meaning", such as name, id numbers, and address (Frické, M., 2009). The term "Information Security" is usually associated with confidentiality, integrity, and availability (CIA) of both electronic and physical information from unauthorized access (Qadir, S., & Quadri, S. M. K., 2016). Accordingly, Numerous researchers have defined Information

eISSN: 2398-4287 © 2022. The Authors. Published for AMER ABRA cE-Bs by E-International Publishing House, Ltd., UK. This is an open-access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer-review under responsibility of AMER (Association of Malaysian Environment-Behavior Researchers), ABRA (Association of Behavioral Researchers on Asians), and cE-Bs (Centre for Environment-Behavior Studies), Faculty of Architecture, Planning & Surveying, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/ebpj.v7iSI10.4133

Security Behaviour (ISB) based on their point of view. Therefore, in this literature, Information Security Behaviour is defined as an action or effort by an individual to ensure the confidentiality, integrity, and availability (CIA) and to protect or at least lessen the risk, threats and damage resulting from an information security breach while using any Information Technology (IT).

Morden society has almost successfully assimilated all of their basic need with the functions of the smartphone. The smartphone is a compact and portable electronic device that combines the functions of a mobile telephone and advanced computing system. Smartphones are usually installed with an operating system such as iOS and Android and are able to support numerous dynamic applications. Meanwhile, smartphone users are simply the people who are using or interacting with a smartphone. In the information security field, human factors (users) are identified as the weakest link in the security chain (Enge, E. 2021). Therefore, it is crucial to understand factors that influence users' security behaviour in order to find a solution and reduce the risk of the information security breach at both individuals' or/and organizations' levels.

This literature was conducted to review and summarise the current direction and findings in the field of Information Security on Smartphone Users. Accordingly, the following research questions were defined:

RQ 1: How much activity in the field of Information Security Behaviour on Smartphone Users has there since 2017?
RQ 2: What are the research topic being discuss in Information Security Behaviour studies in Smartphone context?
RQ 3: What are the most dominant research approach being used?
RQ 4: What are the most dominant theories are being used?
RQ 5: What are the potential future research topics for in the field?

2.0 Methodology

Information security is one of the most discussed domains in information systems research. Information security has two (2) major streams, which are organizational, and home users (individual). In addition, information security study has three (3) main topic, which is behavioural studies, policy studies, and technical studies. This paper aims to review research articles in the field of information security behaviour in relation to the smartphone context. Thus, the systematic literature review approach was chosen to achieve the goal of this study. This method is mainly used to review several scientific findings from previous studies, hence will provide a "bigger picture" of current findings in the subject of research. In addition, this approach is wholly straightforward and repeatable (Butler, R., 2021).

One of the main objectives of this literature is to review research articles related to the Information Security Behaviour of Smartphone Users. In addition, this literature also aims to summarise work done in information security in the scope of smartphones context published in the last six (6) years. Therefore, the search period is limited from January 2017 to the date of the search (June 2022).

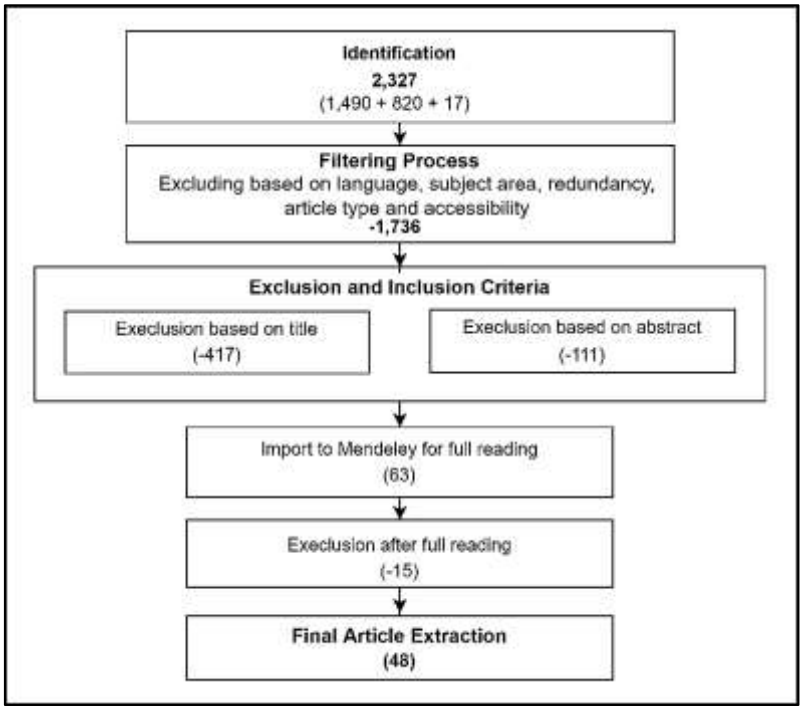

Fig 1: article screening and refinement process

The total search results are 2,327 papers which 1,490 articles are from Web of Science (WOS), 820 articles are from Scopus, and 17 articles are from Google Scholar. The excluding criteria during the screening phase are language berries, subject types, duplicate (article redundancy), and accessibility (paywall). Based on that, a total of 4 articles were removed based on language berries,1,644 articles based on the subject area, 62 articles redundancy, and a total of 14 articles are inaccessible due to a paywall. In addition, literature review articles

were also excluded in the screening phase, resulting in an additional 12 papers being removed. Therefore, a total of 1,734 results were removed based on the screening process. Next, a total of 417 articles were removed based on the title and a total of 111 articles were removed based on the abstract. Thus, a total of 63 reminding articles were imported to Mendeley Desktop for full reading, and a total of 48 articles were accepted and used as data in this study. The visualization of this process is presented in figure 1.

3.0 Findings

After the exclusion and inclusion phase, a total of 48 articles were selected. Then each of the articles was manually examined, and data was extracted to answer the research question.

RQ 1: How much activity in the field of Information Security Behaviour on Smartphone Users has there since 2017?

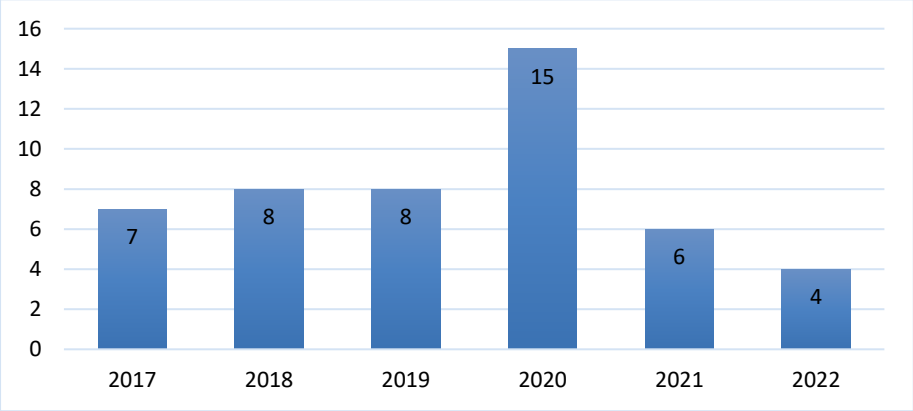

Fig 2: number of publications from 2017 -2022

According to the data, there has been appreciable publication activity in the field of information security related to smartphone users' behaviour since 2017, with an average of 8 articles per year. The first three examined years (2017-2019) showed a consistent publication activity, and a spike can be seen in the year 2020 with 15 publications. Later, the trend drastically decreased in the year 2021 and 2022. Based on this data, it can be stated that the research activity in information security related to smartphone users' behaviour is significantly active, and there are quite of numbers of researchers who are active in this field. Nevertheless, as smartphone technology becomes more advanced from time to time, it is believed that the publication in this field will continue to increase.

RQ 2: What are the research topic being discuss in Information Security Behaviour studies in Smartphone context?

The topic in the information Security field is versatile and so do the articles. One of the objectives of this study is to identify the research topic discussed in the article, whether the article is trying to explain the general idea of information security behaviour in the smartphone context or try to apply the approach to the participant in the research. In order to address the research questions, the researcher identifies the classification of the topic into four (4) categories, as shown in table 1 (Melinat, P., Kreuzkam, T., & Stamer, D., 2014). The four categories are:

Table 1. Research Topic

Topic	Description
Concept	Presenting the general idea of information security behaviour in smartphone context.
Solution	To implement a general concept or a framework to explain the issue in information security issue among smartphone users.
Evaluation	Evaluate the concept or framework and/or try to verify or falsify the concept or framework.
Experiment	Exemplify an approach and applies the approach to the participant of the research

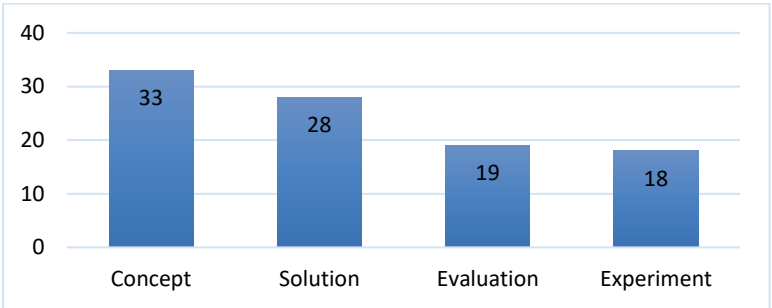

Fig 3: Research Topic

It is possible for one article to have multiple research topics, for example, introducing a solution (implementing a general concept or a framework to explain the issue) and later evaluating the framework. Therefore, to demonstrate the whole coverage of the selected papers, each article could be associated with two or more of the mentioned categories.

Based on the data, most of the studies focus on Concepts (33) and solutions (28). Besides that, a sizable amount of studies focus on the Evaluation (19) of concepts or solutions and exemplifying an approach to the participant in the research (Experiment – 18). Additionally, most of the studies in 2017 and 2018 focused on developing scales and implementing theories to explain the issue of information security among smartphone users. This is relatable as the issue of information security in the smartphone context was relatively at that time. Moreover, in recent years, more studies have been focusing on integrating theories and developing a solution for information security issues.

RQ 3: What are the most dominant research approach being used?

Research methods define the plans and the procedures for how the scientific research will be carried out. The selection of research methods is based on the nature of the research, research objective and/or problem, and the targeted respondent of the study.

There are three (3) main research approaches in scientific research, namely, Qualitative, Quantitative, and Mixed Methods (McCusker, K., & Gunaydin, S., 2015; Creswell, J. W., 2014). The difference between qualitative research and quantitative research is defined based on terms or words. For instance, Quantitative is based on the words "quantity", which usually involves numbers. Qualitative, on the other hand, often involves direct interaction with the subject of research (qualitative interview). Another way to distinguish the differences between these two methods is through the data collection procedure. The data collection procedure for Quantitative methods is through instruments (surveys). Meanwhile, the qualitative approach is collecting data through observing or/and interviewing the subject. The mixed Method, on the other hand, is the incorporation of both Qualitative and Quantitative elements in a single study.

For the generality of this study, this literature aimed to review the research approach chosen by the researcher in the selected articles.

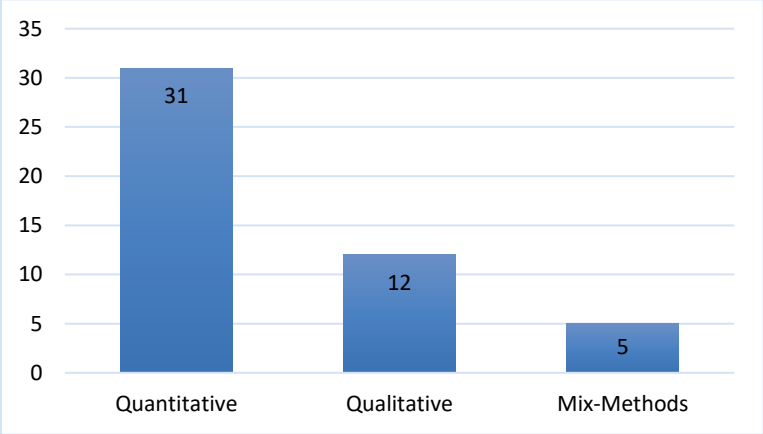

Fig 4: research method

Based on the result of the analysis, it is evident that the Quantitative Method is the most dominant approach in information security studies, with a total of 31 out of 48 articles. Besides that, Quantitative Methods (12) shows a sizeable amount of approaches chosen in this field. In addition, based on the literature review, most of the qualitative methods focus on developing a model or scale or applying a solution to study the users' behaviour. Mixed-method (5) is undoubtedly to be one of the most comprehensive approaches in any scientific field, which require many resources and is a relatively least popular approach to be used in this field.

RQ 4: What are the theories are being used?

The theory is described as a set of interrelated variables, definitions, and propositions that presents a systematic view of phenomena by specifying relations among variables with the purpose of explaining natural phenomena (Creswell, J. W., 2014; Kerlinger, F. N., 1979). In quantitative research, the researchers often test the theories as an explanation for answers to their research questions. The use of theory in qualitative research, on the other hand, is much more dynamic. Instead of testing the hypothesis (theory), in a qualitative approach, the entire research process may generate a new theory as the final outcome of the study, such as Grounded Theory. In mixed methods research, the researchers may both generate and test the theories (Creswell, J. W., 2014).

In scientific research, a theoretical framework provides explanations for the existing phenomenon in a particular field. Based on the literature review, there are fourteen (14) theories or research models that are adopted in the studies;

Technology Threat Avoidance Theory (TTAT), Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Confidentiality, Integrity, and Availability (CIA Traits), Behavioural Intention Model (BIM), Information Security Behaviour Profiling Framework (ISBPF), Unified Theory of Acceptance and Use of Technology (UTAUT), Self-Efficacy (SE), Health Actions Process Approach (HAPA), Fogg Behavioural Model (FBM), Behavioral Model of Cybersecurity (BMS), General Diterance Theory (GDT), Security Awareness Maturity Model (SAMM), and Kano Model (KM).

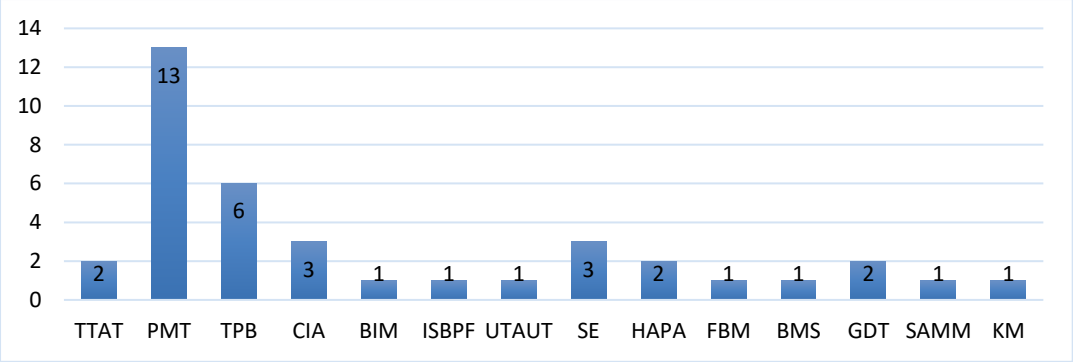

Fig 5: List of theory used

Based on the data presented in the graph, the most dominant theory used to investigate security behaviour in the smartphone context is PMT (13), followed by TPB with six (6) counts. CIA Traits and Self-Efficacy are both recorded three (3) times in the literature. Meanwhile, TTAT, GDT, and HAPA are mentioned twice. Besides that, most studies use integrations of multiple theories and/or adapt variables from many theories in one study.

As there are few to none papers that have discussed on most theories adopted in Information Security fields, therefore, the actual reason why PMT is the most adopted/adapted theory in this field remains unknown. Besides that, scales such as the Human Aspects of Information Security Questionnaire (HAIS-Q), Security Behaviour Intention Scale (SeBIS), and Information Security Behaviour Scale (ISB) are among the most common scale adopted in this field.

RQ 5: What are the potential future research topics for in the field?

Based on the reviewed articles and current information security issues, this literature has come with several possible directions of research in the information security field related to smartphone security in the smartphone context.

First thing first, is the behaviour perspective. Similar to the "mother and kids" concept, if a person is well attached to their smartphone, theoretically, the smartphone users should be more vigilant toward the security matter of their devices including the personal data stored in the device. Accordingly, to this day, users are highly dependent on the function of their smart devices. Therefore, the loss or damage to their smartphone should cause a big issue for them. Hence, smartphone security should be their main priority at all times. Information such as contact numbers, location data, financial records, passwords and other valuable information which are stored on the smartphone is the main reason why smartphone users become the primary target for financial fraud online (Kaspersky., 2022). Therefore, it should be the users' main priority to ensure their data are secured on their own devices. However, not many studies have been done to investigate the effect of individual attachment or reliability towards smartphones in relation to the users' security behaviour.

Based on the findings, the literature suggests that PMT are most dominant theory in the Information Security Field. There is some speculation that can be made based on these findings where PMT is believed to be more comprehensive as it includes almost all variables in one theory. This is because some theories can be too specific while PMT is more general. For example, TTAT it's focusing on threat appraisal, while GDT is focusing on sanctions. However, this claim cannot be confirmed as there is lack of evidence and supportive findings to support my such claim. In addition, the reason for the researcher to adopt certain theories is influenced by their research objectives. To the best of our knowledge, there is no study has been done extensively discussing why PMT are more preferred theories to be used in this field thus cracking another theoretical gap for future research topics to come out with a proper theoretical discussion of why PMT are most dominant theory in the Information Security Field.

Last but not least, from a technical perspective, there are numerous information security studies that have suggested the best solution for information security issues in the smartphone context. Such as information security awareness programmes, training, and security notification has proven to significantly increase security alertness among users, hence reducing the intention of the users to commit risky behaviour when using a computer or smartphone (Abraham, S., & Chengalur-Smith, I., 2019). However, those "solution" is mostly done in a controlled situation (experiment), and very few studies have been focusing on implementing those methods in a real-world setting. Thus, the effectiveness of those suggested "solutions" to real-life situations remains unknown.

4.0 Conclusion

This paper described a systematic literature review focusing on Information Security Behaviour in the Smartphone user's context. The procedure for article searching and the screening and refining process for this literature was described and illustrated accordingly. A total of 48 research articles were selected and analysed in this literature review to answer five (5) research questions as mentioned earlier.

According to the data collected, there are a sizable number of publications have been made related to security behaviour on smartphone users since 2017, with an average of 8 articles published per year. Similar to other information security studies, in this context, the researcher also focuses on concepts and solutions to understand the ever-changing phenomenon of security behaviour among smartphone users. In addition, out of the three main research approaches, qualitative is more preferable approach in this field. Due to the nature of this research, which is to review works done related to security behaviour, it is noticed that protection motivation theory is the

most common theory adopted in this field. Besides that, in this literature, this paper proposed three potential research directions based on behavioural, policy and technical aspects.

Lastly, due to the main challenges in this literature review (Paywall), only two (2) main scientific databases are used for article searching. Although, with the help of Google Scholar, it is impossible to include all data in a single study at once, therefore, it is undoubted that there are "missing" articles which are not included in this study. However, since the selected scientific databases contain a relatively large amount of published work within the research scope, hence, the potential for changes in the findings of this literature is predicted to be relatively small.

Reference

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner-controlled information security training. Computers & Security, 87, 101586.

Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017, July). Information security behavior: Recognizing the influencers. In 2017 Computing Conference (pp. 844-853). IEEE.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. Computers and Security, 88. https://doi.org/10.1016/j.cose.2019.101647

Butler, R. (2021). A systematic literature review of the factors affecting smartphone user threat avoidance behavior. November. https://doi.org/10.1108/ICS-01-2020-0016

Chow, G. W., & Jones, A. (2008). A framework for anomaly detection in OKL4-linux based smartphones. Proceedings of 6th Australian Information Security Management Conference, December 2006, 40–47. https://doi.org/10.4225/75/57b55ad8b876b

Creswell, J. W. (2014). Qualitative, quantitative and mixed methods approaches.

Enge, E. (2021, March 23). *Mobile vs. desktop usage in 2020* . perficient.com. Retrieved June 24, 2022, from https://www.perficient.com/insights/research-hub/mobile-vs-desktop-usage

Frické, M. (2009). The knowledge pyramid: a critique of the DIKW hierarchy. Journal of information science, 35(2), 131-142.

Hadlington, L., & Chivers, S. (2021). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. Policing (Oxford), 14(2), 479–492. https://doi.org/10.1093/police/pay027

Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information Security Culture: A Systematic Literature Revier. Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015, 205, 456–463.

Kaspersky. (2022). IT threat evolution in Q1 2022. Non-mobile statistics. Securelist.com. Retrieved June 24, 2022, from https://securelist.com/it-threat-evolution-in-q1-2022-non-mobilestatistics/106531/#:~:text=According%20to%20 Kaspersky%20Security%20Ne work,313%2C164%2C030%20unique%20URLs%20as%20malicious

Kerlinger, F. N. (1979). Behavioral research a conceptual approach.

Li, W., Wang, Y., Li, J., & Xiang, Y. (2020). Toward supervised shape-based behavioral authentication on smartphones. Journal of Information Security and Applications, 55(August), 102591. https://doi.org/10.1016/j.jisa.2020.102591

Lima, A., Sousa, B., Cruz, T., & Simões, P. (2017). Security for mobile device assets: A survey. Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017, May, 227–236.

Madyatmadja, E. D., Meyliana, & Prabowo, H. (2016). Participation to public e-service development: A systematic literature review. Journal of Telecommunication, Electronic and Computer Engineering, 8(3), 139–143.

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. Perfusion, 30(7), 537-542.

McGill, T., & Thompson, N. (2018). Gender differences in information security perceptions and behaviour. ACIS 2018 - 29th Australasian Conference on Information Systems, 1–11. https://doi.org/10.5130/acis2018.com

Melinat, P., Kreuzkam, T., & Stamer, D. (2014, September). Information overload: a systematic literature review. In International Conference on Business Informatics Research (pp. 72-86). Springer, Cham.

Mi, T., Gou, M., Zhou, G., Gan, Y., & Schwarzer, R. (2020). Effects of planning and action control on smartphone security behavior. Computers and Security, 97, 101954. https://doi.org/10.1016/j.cose.2020.101954

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature : A Meta-Analytic Structural Equation Modeling Approach. 23, 196–236. https://doi.org/10.17705/1jais.00723

Nowrin, S., & Bawden, D. (2018). Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh. Information and Learning Science, 119(7–8), 444–455. https://doi.org/10.1108/ILS-04-2018-0029

Qadir, S., & Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. Journal of Information Security, 7(3), 185-194.

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., & Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. Knowledge-Based Systems, 246, 108709. https://doi.org/10.1016/j.knosys.2022.108709

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. Computers and Security, 77, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. Computers in Human Behavior, 101(January), 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Xiao, Q. (2021). Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study. Telematics and Informatics, 58(May 2020), 101535. https://doi.org/10.1016/j.tele.2020.101535