International Journal of Safety and Security Engineering
Vol. 14, No. 3, June, 2024, pp. 795-806
Journal homepage: http://iieta.org/journals/ijsse

Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users

Candiwan Candiwan*, Luthfi Machdar Rianda

School of Economic and Business, Telkom University, Bandung 40287, Indonesia

Corresponding Author Email: candiwan@telkomuniversity.ac.id

https://doi.org/10.18280/ijsse.140312

Received: 4 April 2024
Revised: 20 May 2024
Accepted: 4 June 2024
Available online: 24 June 2024

Keywords:
email management, information security behavior, infrastructure management, mobile banking, password management, privacy concerns, security perception

ABSTRACT

In today's digital era, the concept of transactions at your fingertips has revolutionized how we conduct financial transactions, allowing us to conduct them anywhere and anytime. Unfortunately, this is followed by inappropriate information security-related behaviors, such as using the same password for multiple accounts and assuming transactions with public WiFi are fully secure, etc. Inappropriate behaviors related to information security increase the risk of cybercrime. Therefore, this study aims to explore the factors that are relevant to fostering positive information security behaviors among mobile banking users in Indonesia. The constructs in this study consist of password management, infrastructure management, email management, security perception, and privacy concerns. Data collected from 197 respondents was derived from distributing online questionnaires and analyzed using Partial Least Squares-Structural Equation Modeling (PLS-SEM) techniques and descriptive analysis. This study reveals that security perceptions contribute the most to fostering positive information security behavior, followed by infrastructure management, privacy concerns, email management, and password management. Based on the descriptive analysis from the security perception section, mobile banking users should be more aware that using public WiFi for financial transactions is risky. On the other hand, in Indonesia, mobile banking users have shown a good indication of concern for the security of their devices, which needs to be maintained. This research can be a reference for service providers to educate their users and create regulations such as mandatory password changes. These can minimize the risk of cybercrime among mobile banking users.

1. INTRODUCTION

Technological development has become a sure thing to happen in the modern era. By the end of 2022, the number of smartphones in use will reach 68 percent of the total population in the world and is predicted to experience growth in the following years [1]. The ever-increasing use and advancement of mobile communication technology led to a corresponding surge in speed and dependence on wireless communication [2]. Technological advances have made digital transactions possible and commonplace; the global economy is now operating differently due to digitization and internet use [3]. Coin-and paper-based money is rapidly being replaced by practical and economical digital payment methods [4]. The Bank was one of the first to transform and adapt human services to mobile-based platforms to address this digitization trend [2]. One of the results of banks' adaptation to this digitization trend is mobile banking products. The presence of mobile banking makes transactions at your fingertips prevalent among the public.

Since cashless culture or, in this case, financial transactions using fingertips through mobile banking applications became commonplace, the number of digital banking transactions has continued to increase. In January 2024, digital banking transactions grew 17.19% year on year (yoy) to Rp 5,335.33 trillion [5]. The increase in the intensity of digital transactions in financial services certainly presents an increased crime risk in these services [6]. Thus, the significant increase in the use of digital transactions not only opens up opportunities for easy access to financial services but also creates an opening for an increase in criminal activity in the cyber domain. One of the detrimental effects of advances in smartphone technology that still affects users is the possibility of data theft [7]. In general, cybercriminals directly attack end-users. Phishing is a cybercrime that uses texts, phone calls, and emails to obtain personal identities, banking information, credit card details, and passwords, by sending legitimate-looking emails or creating pop-up windows that appear to come from a trusted source to trick victims into providing their personal information to fake websites, and sometimes transferring malware to access victims' personal data [8]. Cybercriminals want to obtain credential information from users; this information is used to access the user's account so that the perpetrator can freely act as if they are the account owner. Many people still use the same password for multiple accounts [9]. The use of the same password for various accounts increases security risks. If one account is successfully hacked, other accounts using the same password are also potentially

threatened; this practice makes it easier for cybercriminals to access various personal information and other vital data [9]. In addition, many people still do not know that conducting digital financial transactions using public WiFi is risky [10]. The use of public WiFi for important matters such as financial transactions is very risky for tapping [11]. Most public WiFi uses persistent third-party monitoring cookies, which allow surveillance of users' online activity even after they are no longer using that WiFi [12]. From this, other parties can obtain important information, such as usernames and passwords, that users utilize to log in to a website.

Inappropriate user behavior, such as insecure password management, negligence in managing the device's infrastructure (e.g., not updating or even not using antivirus software on the device), careless email handling, and lack of security perception and privacy concern, providing opportunities for cybercriminals to exploit personal information from users [9, 10, 13, 14]. Failure of users to implement comprehensive information security practices not only facilitates illegal access to their personal and financial data but also increases the likelihood of cybercrime incidents. Information is precious and must be protected [15]. Mobile banking service providers have expanded their efforts to create a secure system to maintain their reputation. However, if users do not apply appropriate information security behaviors, cybercrime cases in mobile banking users will continue to appear. This can be said because information security risks arise when the data is uploaded to the internet [16].

Based on the explanation above, it can be concluded that progress and increased use in the technology field will be followed by an increase in the risk of cybercrime. It is not enough just for service providers to make efforts to anticipate cybercrimes; users should be proactive in adopting preventive measures to avoid becoming victims of cybercrime.

We found different results from previous research, where infrastructure management was found to be irrelevant as a factor that can foster positive information security behavior in business employees [17]; but, in another study where computing students were the object of research, it was found that infrastructure management played an important role in fostering positive information security behavior [10]. In addition, previous studies did not include aspects of privacy concerns as variables, whereas the research conducted by Hidayanto et al. [18] clearly states that aspects of privacy concerns affect positive information security behavior directly.

This study aims to prove the legitimacy of aspects such as password management, infrastructure management, email management, security perception, and privacy concerns, which in previous studies have been shown to play a role in fostering positive information security behavior. Besides that, it also examines the information security behavior of mobile banking application users in Indonesia based on descriptive analysis.

The information in this research is expected to encourage people to improve these factors so everyone has positive information security behaviors. This aims to make the concept of "transactions at your fingertips" safe for the public to implement.

2. LITERATURE REVIEW/RELATED WORKS

Cyberattacks are more likely to occur when there are more activities that rely on the internet [9]. The banking industry is one of the industries closely related to cybercrime; users have an essential role in preventing this from happening [9]. Appropriate user behavior regarding information security is critical to avoiding cybercrime [19].

The constructs in this study were adapted from the research conducted by Saeed [10], including password management, infrastructure management, and email management as perceived behavioral control, while security perception as behavioral attitude; behavior toward information security is derived from the theory of planned behavior, which emphasizes conditions in which users perceive an action as beneficial, possess the necessary skills, and receive appropriate support from their peers.

The research of Kautsarina et al. [18] aims to identify which aspects are directly related to positive information security behavior and which serve as mediators. The findings indicate that government efforts, privacy concerns, and perceived behavioral control directly influence positive information security behavior, while other aspects function as mediators.

Based on this framework, we decided to test the legitimacy of the aspects of password management, infrastructure management, email management, security perception, and privacy concerns in fostering positive information security behavior. Government efforts were not included because this study focuses solely on aspects involving users. This approach is supported by the research of Candiwan et al. [9], which asserts that user behavior and awareness of information security are crucial in minimizing the risk of cybercrime threats.

From several literatures, we found that the aspect of password management [17, 20, 21], infrastructure management [10], email management [10, 17], perception of security [14, 22], and privacy concerns [18], as an essential component in encouraging positive information security behavior. In this study, the aspects of Password Management, Infrastructure Management, and Email Management are interpreted as Perceived Behavioral Control, while Security Perception and Privacy Concerns are interpreted as Behavioral Attitude. The details of these aspects will be explained in the following section.

2.1 Password management

Password management refers to the process that involves creating, storing, and securely retrieving passwords [20]. Most people are familiar with both good and bad password management practices, but they still often violate password management practices because they feel the negative consequences are not immediately apparent [23]. Many people still use the same username and password for several accounts [9]. Imagine if the criminal managed to get the username and password of the user, enabling the perpetrator to access several accounts owned by the user. Positive user behavior is critical to mitigating more significant risks and losses in managing information security [9]. Prior research involving business employees as respondents has established that effective password management is crucial in fostering positive behavior toward information security [17]. This approach focuses on the importance of good password management practices as a preventive measure against potential cyberattacks. However, the results of different studies show contrasting views on the effectiveness of password management. In research involving students in computing, password management was not considered a relevant factor in fostering positive information security behaviors [10]. Based on the explanation above, the first hypothesis of this study is: "Effective password

management practices can foster positive information security behavior for mobile banking application users in Indonesia."

2.2 Infrastructure management

A secure infrastructure reduces the likelihood of a system having vulnerabilities [17]. Infrastructure management in this study leads to the governance of security systems on devices to reduce the possibility of vulnerabilities. Things to note related to system security in a device include antivirus [24], firewall [25, 26], and anti-spyware [27, 28]. All three software can reduce the vulnerability of the device used. On the other hand, Al Saleh et al. [29] believe that although antivirus software provides basic security to users, the way antivirus works is inherently disruptive and can impact the device's performance. However, if you do not update or even do not use antivirus software on the device, it can increase its vulnerability [30]. A study targeting computer students showed that infrastructure management is considered relevant and contributes to fostering positive information security behaviors [10]. In contrast, infrastructure management is not considered as influential in fostering positive information security behaviors among business employees [17]. This is because, in many business organizations, responsibility for infrastructure maintenance falls to the IT department, so business employees are less likely to see infrastructure management as an essential aspect of their information security practices [17]. Individual users, unlike the general public, who use mobile banking applications, do not require specialized parties, such as IT departments, to secure their device infrastructure. Therefore, the purpose of this study is to investigate this issue among mobile banking users. Consequently, the second hypothesis of this study is: "Implementing appropriate measures to secure device infrastructure can foster positive information security behavior for mobile banking application users in Indonesia."

2.3 Email management

One of the most popular communication media is email [17]. That doesn't mean email is a secure medium of communication. Research conducted by Kruger et al. [31] discusses the dangers of identity theft and virus attacks associated with email communication and the fact that most people read emails with potentially harmful content without considering the repercussions.

Phishing is a form of crime in the cyber world. One of the entrances for cybercriminals to commit phishing is through email, which sends messages that seem to come from trusted sources; victims are deceived and enter the spam web so that the personal information they have can be obtained by the perpetrator [8]. Previous research with business employee respondents identified effective email management practices as a key contributor to encouraging positive information security behaviors [17]. Findings from another study involving computing students [10] further support this assertion. However, this study aims to further substantiate the role of effective email management in promoting positive information security behavior, with a particular focus on mobile banking users from diverse backgrounds as respondents. The aim is to ensure that the study's findings can serve as a universal benchmark. Therefore, the third hypothesis in this study is: "Implementing secure email management practices can foster positive information security behavior for mobile banking application users in Indonesia".

2.4 Perception of security

The perception of information security is how a person assesses information security threats and decides how to respond behaviorally [22]. Perceptions of security can influence users to make transactions on digital services [13]. The logical reason is that people tend to make transactions on a digital service when they are sure the transaction is safe and the service provider can guarantee it. The perception of security as a factor influencing information security behavior has been studied with mixed results. Research conducted by Saeed [10] found that among computing students, perceptions of security did not significantly influence positive information security behaviors. The research suggests that students' technical proficiency may reduce the role of security perception because they may feel more aware of security threats. Another study, which involved business employees as respondents, also identified the aspect of security perception to be irrelevant [17]. In contrast, the study by Chan et al. [14] identifies perceptions of security as contributing factors to appropriate information security behavior. Research by Huang et al. [14] aligns with these findings, suggesting that security perceptions significantly influence positive information security behaviors. Therefore, the fourth hypothesis in this study is that "positive perceptions of device security lead to positive information security behavior for users of mobile banking applications in Indonesia."

2.5 Privacy concerns

Privacy concerns are how individuals consider the privacy sacrifices they make when using a particular app or website [32]. In the context of mobile banking users, when informed about privacy policies, they may feel anxious about the confidentiality of their data. Uncertainty about the retention period of personal data and its usefulness by service providers can also lead to privacy concerns [33]. Kautsarina et al. [18] found that the privacy concern aspect directly influences an individual's information security behavior. In other words, someone's concern about their privacy can foster positive information security behavior. As a result, the fifth hypothesis in this study is that "privacy concerns influence positive behavior towards information security in mobile banking application users in Indonesia."

Previous literature examining different objects has shown differences in the key factors that drive positive information security behavior. In investigating a person's behavior, the theory of planned behavior is better to use than other theories because it has the ability to identify the type of beliefs a person has about controlling what will happen as a result of their behavior [34]. In addition, other literature [35] said that the Theory of Planned Behavior can accurately predict compliance with information security.

This study tries to bring aspects of password management, infrastructure management, email management, perception of security, and also privacy concerns to be tested again by mobile banking users, which is a combination of people with diverse backgrounds; the results of this study aim to provide information related to critical factors in fostering positive information security behavior which is more general to be applied to all circles.

3. MATERIAL AND METHODOLOGY

This research investigates the information security behavior of mobile banking users in Indonesia. In previous literature [10], research has been conducted to understand information security behavior based on four aspects review: email management, infrastructure management, password management, and perception of security. However, in other studies [18], It has been found that apart from these four aspects, one more aspect can directly lead someone to implement positive information security behavior, namely the privacy concerns aspect. Therefore, the framework of this study is illustrated in Figure 1.

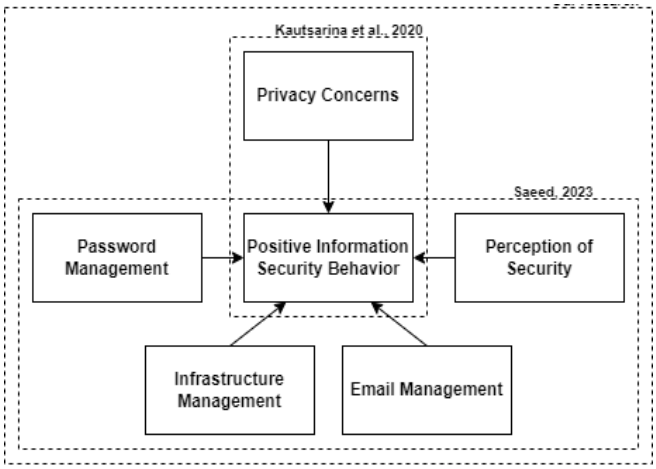

Figure 1. Framework model

Based on the framework model depicted in Figure 1, and the previous section (theoretical support) provided a detailed explanation using five factors that influence positive information security behavior. Therefore, we present the following outline of the study's hypotheses:

- HI: Effective password management practices can foster positive information security behavior for mobile banking application users in Indonesia.
- H2: Implementing appropriate measures to secure device infrastructure can foster positive information security behavior for mobile banking application users in Indonesia.
- H3: Implementing secure email management practices can foster positive information security behavior for mobile banking application users in Indonesia.
- H4: A positive perception of device security leads to positive information security behavior for mobile banking app users in Indonesia.
- H5: Privacy concerns affect positive behavior towards information security in mobile banking application users in Indonesia.

Data collection was carried out through surveys, with research instruments in the form of questionnaires consisting of various statements adopted from previous literature [10, 17, 18]. Before widespread distribution, this research questionnaire underwent validity and reliability testing with SPSS software. Involving 30 respondents, the test confirmed the statements in the questionnaire as valid and reliable, indicating its capability to accurately measure the targeted variables and produce consistent data with repeated use. The respondents' responses were measured using a scale of 1 to 5, where one indicated strongly disagree, and five indicated strongly agree.

The minimum sample number is determined based on the inverse square root method formula with a minimum coefficient path value of 0.2 and a significance level of 5%, resulting in a minimum sample requirement of 154,505, rounded to 155. The inverse square root method is a better alternative to the ten times rule technique for determining sample size because it produces the minimum sample size needed while considering both the statistical power and significance level [36].

The respondents collected were 197 people, all of whom were users of mobile banking applications in Indonesia. Respondents in this study consisted of 104 females and 93 males. In this study, the sampling technique used was convenience sampling, followed by data processing using the Partial Least Squares-Structural Equation Modeling (PLS-SEM) technique. The bootstrapping method is implemented with 5000 iterations to strengthen the analysis. The hypothesis test process interprets P and T values to confirm the results' accuracy.

4. RESULTS AND DISCUSSION

4.1 Responses analysis

This study garnered participation from 197 respondents, who had to fill out five survey sections. These sections assessed various aspects such as password management, infrastructure management, email management, perception of security, and privacy concerns. The responses provided by the participants across these five domains are presented in Tables 1 through 5.

Table 1 presents data on password management practices gleaned from questionnaire responses. The information reveals that most respondents gave positive answers when asked about good password management habits, such as keeping their passwords private and updating them when the program asks. On the other hand, compared to other proper password management practices, fewer respondents responded positively to practices such as not using the same password for multiple accounts and using software to manage passwords/usernames. Research by Candiwan et al. [9] found the same thing that many users continue to use one password for multiple accounts. Although we conducted this study in 2024, this practice continues, reflecting widespread unawareness of its security risks. Indeed, using the same password for multiple accounts simplifies the process, as it only requires remembering one password, but it is extremely dangerous because when a cybercriminal manages to get hold of one password, other accounts are likely to be affected. Password manager software is a solution for users who are reluctant to memorize many passwords. With this software, unique and different passwords for each account can be stored and accessed easily via biometric verification or PIN at login.

Responses related to device infrastructure management are presented in Table 2. The responses show that 57% of respondents have antivirus software installed on their devices, and only about 52% keep their antivirus software up-to-date. As for the use of firewalls and anti-spyware software, more than 50% of the respondents ignored them; most of the respondents showed a neutral attitude towards firewalls and anti-spyware tools, indicating ignorance of their urgency. Some people may think that the smartphones they use are already secure in terms of infrastructure; users often overlook

this aspect of device infrastructure security. The main function of a firewall is as a first line of defense that protects the device from network threats, and it can prevent unauthorized access to the user's device [25, 26]. While anti-spyware tools serve to detect and remove unwanted spyware programs [27, 28]. The use of firewalls and anti-spyware tools on smartphones can prevent various cybercrime methods. One threat that can be warded off is a Trojan that has the potential to steal personal information, including users' financial data. On the other hand, proper device infrastructure management practices, such as always locking the phone when not in use and using passwords or biometric security to unlock the phone, show that more than 80% of respondents do so. Based on this explanation, there is a need for wider education on comprehensive security infrastructure management for personal devices to ensure a fully protected user experience.

Table 1. Password management-related responses

Statements on Questionnaires Related to Password Management	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I use a wireless network at home, I secure the wireless network connection. (PM1)	[10, 17]	1.5%	8.1%	22.3%	41.6%	26.4%
I do not use the same password for multiple accounts. (PM2)		9.1%	15.7%	16.8%	29.9%	28.4%
I change passwords when the application requires changes. (PM3)		1.5%	7.6%	13.2%	41.6%	36.0%
When I change my password, I do not use the old password as the basis. (PM4)		4.6%	10.7%	15.2%	42.1%	27.4%
I store my username/password in an electronic file or write it down. (PM5)		7.1%	8.1%	17.8%	38.1%	28.9%
I use software to manage my passwords. (PM6)		7.1%	14.7%	22.8%	35.5%	19.8%
I do not share my password with others. (PM7)		6.1%	6.1%	8.1%	31.0%	48.7%

Table 2. Infrastructure management-related responses

Statements on Questionnaires Related to Infrastructure Management	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Administratorgree
My phone comes with an antivirus program. (IM1)	[10, 17]	5.6%	11.7%	24.9%	39.1%	18.8%
The antivirus program on my phone is always updated. (IM2)		6.6%	11.7%	25.9%	31.0%	24.9%
I have a firewall installed on my cell phone. (IM3)		5.6%	15.7%	33.0%	35.0%	10.7%
I use an anti-spyware tool on my phone. (IM4)		9.1%	24.9%	32.5%	27.4%	6.1%
I always lock my phone when I leave it. (IM5)		1.5%	5.1%	10.7%	24.9%	57.9%
I use password / biometric security to unlock my phone. (IM6)		2.0%	4.1%	11.2%	23.9%	58.9%
My mobile phone's operating system or mobile banking application is always updated. (IM7)		3.0%	6.1%	11.7%	32.5%	46.7%

Table 3. Email management-related responses

Statements on Questionnaires Related to Email Management	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I do not open an email if I do not know the sender. (EM1)	[10, 17]	3.6%	13.2%	24.4%	34.5%	24.4%
I do not open attachments in incoming emails if I do not know the sender. (EM2)		3.0%	8.1%	25.9%	35.5%	27.4%
I use encryption when sending emails. (EM3)		6.6%	13.2%	38.6%	32.5%	9.1%
I pay attention to the security settings on my web-based email application. (EM4)		2.5%	7.6%	17.8%	41.1%	31.0%

Table 3 investigates email management behaviors, focusing on attitudes toward not opening emails and attachments from unknown sources, the use of email encryption, and the management of security settings in web-based email applications. The responses show that 72% of the respondents pay attention to security settings on web-based email applications, 59% do not open emails from unknown senders, and 63% do not open attachments from unknown senders. From this explanation, it can be concluded that most respondents have carried out proper email management practices. Unfortunately, there are still many neutral responses on the part of using encryption when-sending email messages. This identifies that many people still do not recognize and know the function of this encryption feature. The findings in this study are similar to those found in a previous study [37], which showed that more than 60% of respondents did not know about this feature; however, the majority of respondents in that study were worried that their data could be stolen. The conditions that occur with these concerns are certainly very contradictory. If people are worried about their personal data being stolen, it should be necessary to use this encryption feature. This can be said because the encryption feature disguises the message so that only the sender and the intended recipient can access the message [37]. Therefore, education to the public, especially in this case, namely mobile banking users, needs to be carried out so that information about the importance of all indicators in password management can be applied.

Table 4 shows responses regarding several statements that describe respondents' perceptions of information security. The majority of respondents gave response agree and strongly agree responses to all statements. More than 79% of respondents agreed that cybercrime is inevitable but can be prevented by implementing positive information security

behaviors. In addition, more than 66% of respondents believe that they can protect their smartphones from cybercrime threats, and 67% believe that data stored on their smartphones, whether important or not, can still be misused. This means that while they have the confidence to protect their devices from cybercrime threats, they are still cautious as they believe that there is still a chance of becoming a victim of cybercrime. In addition, only a few respondents are not concerned about the security of their devices. This shows that most mobile banking users, especially in Indonesia, care about the security of their devices that can protect them from cybercrime threats. However, quite a number of respondents gave neutral responses regarding the perception of not using public WiFi networks to conduct financial transactions. The use of public WiFi is very risky because important information belonging to users can be obtained by cybercriminals using the same network [12]. In addition, it is difficult to guarantee that the available public WiFi is safe from the threat of cybercrime. For example, there was an experiment that provided public WiFi with free access but aimed to obtain personal information from users; users must provide the requested information and agree to the terms and conditions if they want to use the WiFi. Once users do that, network providers can easily obtain personal information from them, including financial data such as usernames and passwords [11]. Although this is just an experiment, it proves that people are still tempted by free public WiFi services even though they have to give personal information to other parties who may have bad intentions. It's best to avoid doing essential activities by using public WiFi. If you have to use public WiFi, use public WiFi that does not ask for information with the possibility of misuse. In addition, it is recommended to use a trusted Virtual Private Network (VPN) when using public WiFi, because using a trusted VPN can increase security in using public WiFi [11, 12].

Table 5 discusses respondents' concerns regarding their privacy data. The data shows that strong responses highlighted deep concerns regarding how personal information is managed by service providers, with considerable consensus on the need for better data protection efforts. Responses showed that the majority of respondents gave positive responses to all statements in this section. This illustrates that most respondents are both concerned and worried about their personal data being misused. Although 78% of respondents objected to providing their privacy data, the provision of privacy data such as name, date of birth, ID number, etc., is inevitable because it is the regulation of the service provider to request this from service users. In addition, the data shows that 81% of respondents agreed that service providers should work harder to manage their privacy data securely. The responses from respondents in this section show that they are worried about their privacy data. The existence of concerns related to privacy data will cause users to be cautious when providing their personal information [38]. This concern can be one of the attitudes that prevents their private data from being misused. People who do not have this concern will easily provide their information to other parties who may have bad intentions. Therefore, the attitude shown by the majority of respondents who are mobile banking users in Indonesia is good, and this attitude of concern should remain because basically no one can guarantee that our privacy data cannot be misused.

Table 4. Perception of security-related responses

Statements on Questionnaires Related to Perception of Security	Reference	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I can protect my device (phone) from hackers/phishers. (PoS1)	[10, 17]	3.0%	6.1%	24.4%	46.2%	20.3%
There is a difference if I pay special attention to device security, such as downloading a secure browser. (PoS2)		2.5%	5.6%	24.9%	41.1%	25.9%
The information I store on my device, whether important or not, can still be misused by others. (PoS3)		2.5%	8.6%	21.3%	40.6%	26.9%
If people have malicious intent, they will be able to hack into my device and the network I use. But it can all be prevented by positive behavior in maintaining my information security. (PoS4)		2.5%	5.6%	12.2%	49.7%	29.9%
Attention to device (smartphone) security is necessary but should not be excessive. (PoS5)		3.0%	6.1%	22.3%	45.2%	23.4%
I do not like using public WiFi for financial transactions. (PoS6)		4.6%	14.7%	28.4%	33.5%	18.8%
Device (smartphone) security is something I am concerned about. (PoS7)		2.0%	6.1%	14.2%	42.1%	35.5%

Table 5. Privacy concern-related responses

Statements on Questionnaires Related to Privacy Concerns	References	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I get annoyed when service providers ask for personal information. (PC1)	[18]	1.0%	5.6%	20.8%	38.1%	34.5%
I consider the privacy aspect before providing my personal data. (PC2)		2.0%	4.1%	10.7%	41.1%	42.1%
I object to providing personal data. (PC3)		1.0%	6.6%	13.7%	39.6%	39.1%
The provider collects too much of my personal information. (PC4)		2.5%	7.6%	25.4%	41.1%	23.4%
The provider should work harder to secure users' personal information. (PC5)		1.5%	5.1%	11.7%	35.0%	46.7%

From the responses provided by the respondents, we categorized each variable and whether its practices were classified as Very Bad, Bad, Normal, Good, or Very Good. This categorization is based on the average of the responses obtained for each variable with the following conditions: Very Bad (1.00-1.80), Bad (1.81-2.60), Normal (2.61-3.40), Good (3.41-4.20), and Very Good (4.21-5.00) [39].

In Table 6, it can be seen that all variables fall into the good category. This indicates that, on average, mobile banking users in Indonesia are already practicing and thinking appropriately about information security. However, this number should be even higher because, given that the target of cybercrime is the individual, proper practices and thinking about information security should be present in everyone.

Table 6. Average of responses per variable

Variables	PM	IM	EM	PoS	PC
Mean score	3.78	3.74	3.63	3.81	4.04
Category	Good	Good	Good	Good	Good

Based on Table 6, the responses given to the five aspects of this research questionnaire show that privacy concerns get the highest mean score. This indicates that mobile banking users, especially in Indonesia, are concerned about their privacy data, encouraging them to be more careful when providing privacy data to other parties. In addition, these results show that these concerns have led to important demands from users for greater transparency and accountability in data collection practices, emphasizing the need for increased protection and ethical standards in managing personal information by service providers.

Furthermore, the second highest aspect is the perception of security. In other words, most mobile banking application users in Indonesia understand the importance of securing their information. It can be concluded that they believe their actions related to information security can determine the likelihood of them becoming victims of cybercrime. Unfortunately, many respondents still gave a negative response regarding the statement of not using public WiFi to conduct digital financial transactions. This indicates that mobile banking users, especially in Indonesia, are still not aware of the risks of this practice.

On the other hand, the aspect that received the lowest means score was email management. This suggests that the risk of mobile banking users in Indonesia becoming victims of cybercrime using email as a medium is relatively high. In particular, practices such as not opening attachments in emails from unknown senders and using encryption when sending emails need to be considered for implementation. Strengthening these practices can significantly reduce the risk of email-based security breaches.

As for the infrastructure management aspect, the data shows a relatively high neutral response regarding using firewalls and anti-spyware tools. This could be caused by mobile banking app users, especially in Indonesia, think that the built-in protection on their smartphones is enough, so they do not need additional firewall software and anti-spyware tools to protect their smartphones, or they may not even know that these two things are essential for their devices. Using additional software such as antivirus, firewall, and anti-spyware tools can make it less likely for users to fall victim to cybercrime. Therefore, practices regarding effective device infrastructure management must be considered for implementation.

As for password management, many users still use the same password for multiple accounts. This is dangerous because when one account is successfully hacked, the possibility of other accounts being affected is high. In addition, quite several mobile banking app users, especially in Indonesia, gave a neutral response regarding the practice of managing passwords using software tools. These tools can allow users to use different passwords for multiple accounts without having to memorize all the passwords. Users only need to store their passwords in the tool. Therefore, this means that action is required to raise their awareness of the importance of effective password management practices so that mobile banking app users can implement them.

If we're looking at the average value of each indicator, the data shows that all indicators in this study, except indicators IM 3, IM 4, and EM 3, fall into the good and very good categories. Judging from the average value obtained, indicators IM 3, IM 4, and EM 3 fall into the normal category. This indicates mobile banking users, especially in Indonesia, still do not realize the importance of using firewall (IM 3) and anti-spyware (IM 4) software, as well as using encryption when sending emails (EM3). Regarding the use of firewalls and anti-spyware, a possible reason is that people think that the smartphones they use are secure enough that they do not need these two things anymore, or even they think that these two things do not need to be installed on their devices. In contrast, the indicator with the highest mean score is IM 6, which indicates that most mobile banking users, especially in Indonesia, know the importance of using passwords or biometric security to access their devices.

4.2 Validity and reliability testing

Before evaluating the structural model, the measurement model (outer model) was assessed in this study to test the validity and reliability of the construct. Figure 2 shows the output of outer loading values. The value of outer loadings must be > 0.7 to be valid [40]. Other literature [36] said that the reflective indicator is maintained as an indicator with an outer loading value of ≥ 0.7. Therefore, reflective indicators with an outer loading value of < 0.7, such as IM 3, IM 4, PM 2, PM 3, PM 5, PM 6, PM 7, PoS 3, PoS 6, and PC 4, are not included for further evaluation.

Table 7. Fornell-Larcker criterion test results

	EM	IM	PC	PISB	PM	PoS
EM	0.744					
IM	0.638	0.78				
PC	0.609	0.686	0.838			
PISB	0.661	0.702	0.661	0.792		
PM	0.533	0.59	0.519	0.605	0.851	
PoS	0.743	0.755	0.703	0.754	0.637	0.783

After evaluating the output value of outer loadings, the discriminant validity was determined using the Fornell–Larcker criterion, where the output results can be seen in Table 7. The criterion to be valid in the Fornell-Larcker Criterion evaluation is that the value of a variable must be greater than its correlation with other variables [40]. From Table 7, it can be seen that all variables contained in this model fall into the valid category. This can be said because each value of the output for each variable is higher than that of other variables. After that, construct validity and reliability were evaluated by reviewing the output of Cronbach's alpha, composite

reliability, and average variance extracted (AVE) values. The value of the AVE must be > 0.5 for a construct in a variable to be valid; the value of Cronbach's alpha and composite reliability must be ≥ 0.6 to be reliable [40]. From Table 8, it can be concluded that the construct of this model is valid and reliable.

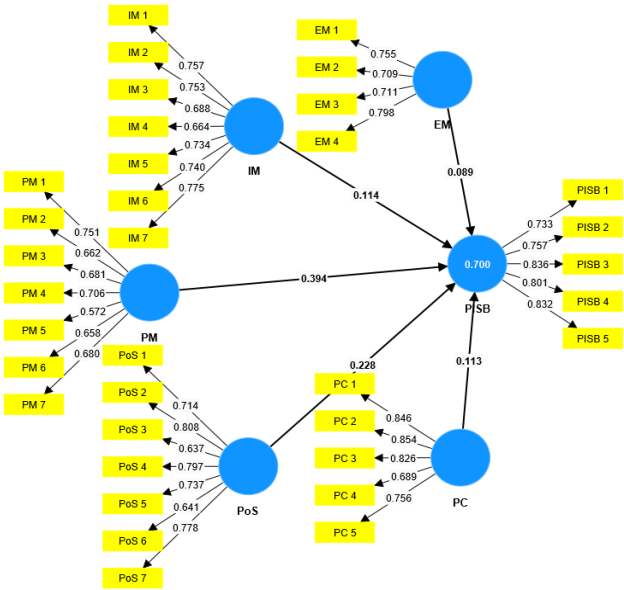

Figure 2. Output results of outer loading values

Table 8. Reliability and construct validity test results

	Cronbach 's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	(AVE)
PM	0.62	0.631	0.839	0.723
IM	0.838	0.843	0.885	0.608
EM	0.733	0.749	0.832	0.554
PoS	0.842	0.842	0.888	0.614
PC	0.858	0.86	0.904	0.702
PISB	0.851	0.856	0.894	0.628

4.3 Structural model (inner model)

Next, the structural model is evaluated to analyze the relationship between variables [41]. In this study, the value of the coefficient of determination or R2 of 0.646 was obtained, which shows a 64.6% variation in positive information security behavior that can be explained through password management, infrastructure management, email management, perception of security, and privacy concerns. This shows that these variables contribute significantly to information security behavior. However, another 35.4% of factors can still describe positive information behavior outside this study.

The results of the path coefficient are shown in Table 9. This path coefficient value is obtained from analysis using the SEM-PLS technique. This value reveals a significant influence of the Perception of Security (PoS), Infrastructure Management (IM), Privacy Concerns (PC), Email Management (EM), and Password Management (PM) variables on Positive Information Security Behavior (PISB). From the results obtained, it can be seen that PoS has the most significant effect with a path coefficient of 0.305 and a statistical T-value of 3.178, also showing statistically strong significance with a p-value of 0.001. This indicates that perceived security contributes significantly to positive information security behavior compared to other variables in this model. Furthermore, IM makes the second largest contribution with a path coefficient of 0.189 and a T-statistic of 2.976, also showing a very important significance with a p-value of 0.001. This confirms that infrastructure management plays an important role in supporting positive information security behavior. Furthermore, in third place, the PC aspect with a path coefficient of 0.156, T statistics of 2.073, and a p-value of 0.019 also provides evidence of a significant influence on PISB. Lastly, EM and PM aspects were found to have a significant influence on PISB with path coefficients of 0.143 and 0.142, respectively, and T-statistics of 2.211 and 2.143, respectively, with a p-value smaller than 0.05, indicating statistical significance in the model.

Table 9. Output result of path coefficients

	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values
EM-> PISB	0.143	0.145	0.064	2.211	0.014
IM-> PISB	0.189	0.189	0.064	2.976	0.001
PC-> PISB	0.156	0.155	0.075	2.073	0.019
PM-> PISB	0.142	0.141	0.066	2.143	0.016
PoS-> PISB	0.305	0.306	0.096	3.178	0.001

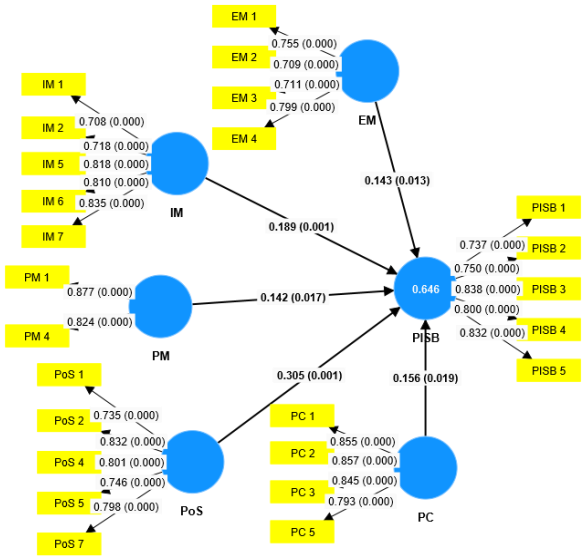

Figure 3. Final PLS model

Before entering the hypothesis discussion, we display the final model in this study, as shown in Figure 3. This model contains indicators with an outer loading value ≥ 0.7, the P value, and the path coefficient between variables.

4.4 Hypothesis discussion

4.4.1 Effective password management practices can foster positive information security behavior

Analysis of responses from respondents showed that password management influences a person's positive behavior regarding information security. In other words, password management is one of the essential things in protecting someone from cybercrime. This finding is in line with results from previous studies [17], which found that password

management is one of the critical factors determining one's information security behavior.

These findings provide information that effective password management measures are something that mobile banking application users must take. Notably, it was found that user actions, such as securing home wireless networks and avoiding using old passwords as the basis for new passwords, can foster positive information security behavior. Apart from this, service providers need to remind or educate users so that password management is one of the things they pay attention to.

4.4.2 Implementing appropriate measures to secure device infrastructure can foster positive information security behavior

The use of devices in the form of smartphones is undeniably related to their involvement in transactions through mobile banking applications. The findings of this study show that aspects of infrastructure management are a crucial factor in growing a person's positive information security. In particular, it was found in this study that user actions such as installing and updating antivirus on their devices, locking the device when not in use, installing a password or biometric security to unlock the device, and constantly updating the software on the device, can foster a person's positive information security behavior. In other words, the Infrastructure Management aspect is one of the critical factors in determining a person's information security behavior, which is in line with previous research [10].

The findings above provide background on many cybercriminals who rely on viruses or malware to take personal data from users. The positive practice of infrastructure management of the devices used can prevent this. Therefore, proper practices of device infrastructure management can prevent users from becoming victims of cybercrime because it can lead someone to have positive information security behavior.

4.4.3 Implementing secure email management practices can foster positive information security behavior

If we refer back to the background section, many cybercrime cases involve phishing methods, such as sending fake links to users' emails. In this study, aspects of email management positively influence effective information security behavior. Specifically, this study found that user actions such as not opening messages from unknown senders, not accessing attachments in emails from unknown senders, using encryption in email communication, and reviewing the security settings of web-based email applications can foster a person's positive information security behavior. That means email management is also one of the critical factors in determining a person's information security behavior. In other words, users who adopt effective email management practices will lower their chances of becoming victims of cybercrime. These findings are supported by previous research [10, 17], Where email management is one of the critical factors in determining one's information security behavior.

A person's habit of ignoring security aspects in email management practices leads them closer to becoming victims of cybercrime [10]. Therefore, email management becomes essential for users to pay attention to. In addition, service providers must also play a role in educating users or presenting policies that can make this aspect necessary to pay attention to.

4.4.4 Positive perceptions of device security lead to positive information security behavior

This study found that aspects of perception of security influence a person's information security behavior. The statements in this research questionnaire, especially in the perception of security section, indicate that they have a good perception of information security. Specifically, the study found perceptions of people as thinking they could protect devices from hacking/phishing, believing that paying particular attention to security aspects will make a difference in securing devices, assuming that hacking can be prevented with adequate information security behavior, thinking that attention to device security is necessary; and worrying about device security can foster a person's positive information security behavior. In other words, a good perception of security will lead them to positive behaviors in information security. However, previous literature found this aspect irrelevant [10, 17]. However, a person's perception of security determines their behavior regarding information security [42]. In addition, this finding is further reinforced by previous research [22], where the study conveyed that the perception of security is essential in encouraging positive behavior toward information security.

Perception of security can be a barrier to someone's not taking vulnerable actions. The existence of the perception of security makes users perform actions they already consider safe [22]. For example, when someone has a good perception of security and wants to download from the internet, they will first question the security of the download. However, if they still have doubts about its security, that makes them delay or even not download it. In other words, their likelihood of becoming a victim of cybercrime is reduced.

4.4.5 Privacy concerns affect positive behavior toward information security

Privacy concerns positively influence effective information security behavior. The results of the hypothesis test in this study have proved this. In particular, this study found user attitudes such as the fear of giving personal information to others, awareness of the importance of privacy, and a tendency to think before providing personal data; provide personal data if it believes that it will be used securely and responsibly; and feel information security must be improved, can encourage positive information security behavior of a person. This finding is reinforced by previous research [18], Where it was found in the study that privacy concern has a direct impact on a person's information security behavior.

Concerns about the privacy of users' data make them more cautious in taking action. This reduces the risk of becoming a victim of cybercrime. In reality, users are asked to provide their personal data. When an official mobile banking application service provider requests personal data from users or prospective users, the possibility of misuse is relatively small. However, if personal data is requested by someone claiming to be from a service provider or official party and the user is successfully deceived, it will undoubtedly cause problems. This certainly makes the possibility of personal data from users more vulnerable to misuse. Therefore, concerns about users' privacy make them more careful when giving their personal data, minimizing the possibility of becoming victims.

These results support the hypothesis that infrastructure management, password management, security perception, email management, and privacy concerns foster positive information security behaviors. The statistical significance of

the path coefficient and the statistical T value confirm the reliability of these findings. In addition, an important finding in this study is that perception of Security is the most influential aspect in fostering positive information security behavior. This research provides insight into the fact that efforts to improve information security depend not only on one or two factors but also on a combination of various interrelated aspects of information security.

5. CONCLUSION

Mobile banking users in Indonesia are highly concerned about their data privacy. We must maintain this concern as no one can guarantee the misuse of our privacy data, leading mobile banking users to be more cautious when providing their personal information. In addition, our findings show that user concerns have resulted in significant demands for increased accountability and transparency in data collection techniques. This highlights the need for service providers to manage personal information by improving protection and ethical standards.

The results regarding mobile banking users' security perception in Indonesia are favorable. However, one indicator that requires improvement is the avoidance of using public WiFi for financial transactions. Public WiFi often comes with easy and free access, but these benefits are not worth the risk of security threats to users' data or crucial information.

Another finding from this research is that there is still a lack of user education regarding software or features that can strengthen information security. This is evident in the number of neutral responses regarding the use of firewalls and anti-spyware tools. While this may sound like a hassle, using such software or security features is worth considering given the magnitude of the loss that users can feel.

Many users persist in using the same password for multiple accounts, posing a risk as successful hacking of one account can compromise other accounts. Furthermore, many mobile banking app users in Indonesia are not concerned with secure password management practices using software tools. With these tools, users can use different passwords for multiple accounts without having to memorize them. All users need to do is store their passwords in the tool. This suggests that mobile banking app users should practice proper password management techniques, and steps should be taken to increase their awareness of its importance.

On the other hand, the most concerning finding from the responses given was the aspect of email management. This aspect received the lowest average score in this study. This suggests that mobile banking users in Indonesia are at high risk of becoming victims of cybercrime via email. We should adopt practices such as sending encrypted emails and refraining from opening attachments from unknown senders. Strengthening these procedures can significantly reduce the risk of email victimization. Email, as one of the most widely used communication mediums, is a lucrative option for cybercriminals.

This study reveals that aspects of password management, infrastructure management, email management, security perceptions, and privacy concerns can significantly foster a person's positive information security behavior. Security perception is the most influential factor in fostering positive information security behavior. However, this study found that paying attention to only one aspect to encourage positive information security behavior is insufficient. Still, it must involve a combination of several other aspects, such as infrastructure management, privacy concerns, email management, and password management. Based on the coefficient of determination in this study, several factors can still describe positive information security behavior. Therefore, the suggestion for further research is to add other variables besides those in this study.

The structured approach to this research facilitated a comprehensive analysis of user behavior toward cybersecurity, providing a nuanced understanding of the current landscape and pinpointing areas for potential improvement. This research strongly suggests that users should consider and implement these aspects properly to reduce the likelihood of becoming victims of cybercrime. Additionally, this study offers an effective strategy to enhance an individual's positive information security behavior through the proper application of aspects such as password management, infrastructure management, email management, security perceptions, and privacy concerns. The information presented by this study can help service providers improve the security of their digital transactions from the user's point of view by providing reminders, education, and information to implement the aspects of this study properly. The ultimate goal is to ensure the long-term implementation of the concept of transactions at your fingertips remains safe.

ACKNOWLEDGMENT

We appreciate the assistance provided by Telkom University, particularly in providing several reference materials.

REFERENCES

[1] Laricchia, F. (2024) Smartphones-statistics & facts. statista. https://www.statista.com/topics/840/smartphones/#topicOverview.

[2] Che, M., Say, S.Y.A., Yu, H., Zhou, Q., Shu, J., Sun, W., Lou, X., Xu, H. (2023). Investigating customers' continuous trust towards mobile banking apps. Humanities and Social Sciences Communications, 10(1): 1-10. https://doi.org/10.1057/s41599-023-02483-3

[3] Khando, K., Islam, M.S., Gao, S. (2022). The emerging technologies of digital payments and associated challenges: A systematic literature review. Future Internet, 15(1): 21. https://doi.org/10.3390/fi15010021

[4] Premchand, A., Choudhry, A. (2015) Future of Payments-ePayments. https://api.semanticscholar.org/CorpusID:17369649.

[5] Bank Indonesia. BI-RATE held at 6,00%: Synergy Maintaining Stability and Reviving Growth. https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_263324.aspx, accessed on Mar. 1, 2024.

[6] Riadi, I., Aprilliansyah, D. (2023). Analysis of Anubis trojan attack on android banking application using mobile security labware. International Journal of Safety & Security Engineering, 13(1): 31-38. https://doi.org/10.18280/ijsse.130104

[7] Sudirman, B.P., Sari, P.K. (2023). Differences in information security behavior of smartphone users in

Indonesia using Pearson's Chi-square and Post Hoc Test. International Journal on Advanced Science, Engineering & Information Technology, 13(2): 703-717. https://doi.org/10.18517/ijaseit.13.2.17975

[8] Kothamasu, G.A., Venkata, S.K.A., Pemmasani, Y., Mathi, S. (2023). An investigation on vulnerability analysis of phishing attacks and countermeasures. International Journal of Safety & Security Engineering, 13(2): 333-340. https://doi.org/10.18280/ijsse.130215

[9] Candiwan, C., Azmi, M., Alamsyah, A. (2022). Analysis of behavioral and information security awareness among users of zoom application in COVID-19 era. International Journal of Safety and Security Engineering, 12(2): 229-237. https://doi.org/10.18280/ijsse.120212

[10] Saeed, S. (2023). Education, online presence and cybersecurity implications: Administrator study of information security practices of computing students in Saudi Arabia. Sustainability, 15(12): 9426. https://doi.org/10.3390/su15129426

[11] McShane, I., Gregory, M., & Wilson, C. (2016). Practicing safe public wi-fi: Assessing and managing data-security risks. Available at SSRN 2895216.

[12] Ali, S., Osman, T., Mannan, M., Youssef, A. (2019). On privacy risks of public WiFi captive portals. In Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, pp. 80-98. https://doi.org/10.1007/978-3-030-31500-9_6

[13] Saeed, S. (2023). A Customer-Centric view of E-commerce security and privacy. Applied Sciences (Switzerland), 13(2): 1020. https://doi.org/10.3390/app13021020

[14] Chan, M., Woon, I., Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3): 18-41. https://doi.org/10.1080/15536548.2005.10855772

[15] Candiwan, Sari, P.K., Nurshabrina, N. (2016). Assessment of information security management on Indonesian higher education institutions. In Advanced Computer and Communication Engineering Technology: Proceedings of ICOCOE 2015, pp. 375-385 https://doi.org/10.1007/978-3-319-24584-3_31

[16] Sari, P.K., Prasetio, A. (2017). Comparison analysis of information security awareness among social media users in Indonesia.Advanced Science Letters, 23(5): 4306-4309. https://doi.org/10.1166/asl.2017.8284

[17] Saeed, S. (2023). Digital workplaces and information security behavior of business employees: An empirical study of Saudi Arabia. Sustainability, 15(7): 6019. https://doi.org/10.3390/su15076019

[18] Hidayanto, A.N., Anggorojati, B., Abidin, Z., Phusavat, K. (2020). Data modeling positive security behavior implementation among smart device users in Indonesia: A partial least squares structural equation modeling approach (PLS-SEM). Data in Brief, 30: 105588. https://doi.org/10.1016/j.dib.2020.105588

[19] Kruger, H.A., Kearney, W.D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4): 289-296. https://doi.org/https://doi.org/10.1016/j.cose.2006.02.008

[20] Tarwireyi, P., Flowerday, S., Bayaga, A. (2011). Information security competence test with regards to password management. In 2011 Information Security for South Africa, pp. 1-7. https://doi.org/10.1109/ISSA.2011.6027524

[21] Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. Computer Science Review, 33: 69-90. https://doi.org/https://doi.org/10.1016/j.cosrev.2019.03.002

[22] Huang, D.L., Rau, P.L.P., Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29(3): 221-232. https://doi.org/10.1080/01449290701679361

[23] Tam, L., Glassman, M., Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. Behaviour & Information Technology, 29(3): 233-244. https://doi.org/10.1080/01449290903121386

[24] Sanok Jr, D.J. (2005, September). An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, pp. 142-144. https://doi.org/10.1145/1107622.1107655

[25] Hayajneh, T., Mohd, B.J., Itradat, A., Quttoum, A.N. (2013). Performance and information security evaluation with firewalls. International Journal of Security and Its Applications, 7(6): 355-372. https://doi.org/10.14257/ijsia.2013.7.6.36

[26] LIUa, M., SUb, C., XIEa, W. (2024). Design and implementation of network emergency interception platform based on firewall. Advances in Transdisciplinary Engineering, 218-226. https://doi.org/10.3233/ATDE240079

[27] Gurung, A., Luo, X., Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. Information Management & Computer Security, 17(3): 276-289. https://doi.org/10.1108/09685220910978112

[28] Sheta, M.A., Zaki, M., El Hadad, K.A.E.S. (2016, July). Anti-spyware security design patterns. In 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, China, pp. 465-470. https://doi.org/10.1109/IMCCC.2016.202

[29] Al-Saleh, M.I., Espinoza, A.M., Crandall, J.R. (2013). Antivirus performance characterisation: System-wide view. IET Information Security, 7(2): 126-133. https://doi.org/https://doi.org/10.1049/iet-ifs.2012.0192

[30] Tiwari, R.K., Karlapalem, K. (2005). Cost tradeoffs for information security assurance. In WEIS. https://api.semanticscholar.org/CorpusID:14117843.

[31] Kruger, H., Drevin, L., Steyn, T. (2007). Email security awareness—A practical assessment of employee behaviour. In Fifth World Conference on Information Security Education: Proceedings of the IFIP TC11 WG 11.8, WISE 5, United States Military Academy, West Point, New York, USA, pp. 33-40. https://doi.org/10.1007/978-0-387-73269-5_5

[32] Hong, W., Thong, J.Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. Management Information Systems Quarterly. https://doi.org/10.25300/MISQ/2013/37.1.12

[33] Joinson, A.N. (2008). Looking at, looking up or keeping

up with people? Motives and use of Facebook. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pp. 1027-1036, https://doi.org/10.1145/1357054.1357213

[34] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2): 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

[35] Sommestad, T., Karlzén, H., Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information & Computer Security, 23(2): 200-217. https://doi.org/10.1108/ICS-04-2014-0025

[36] Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M. (2022). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (3rd ed.). SAGE.

[37] Reuter, A., Boudaoud, K., Winckler, M., Abdelmaksoud, A., Lemrazzeq, W. (2020). Secure email-a usability study. In Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, vol. 12063. https://doi.org/10.1007/978-3-030-54455-3_3

[38] Quan-Haase, A., Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. Journal of the Association for Information Science and Technology, 71(9): 1089-1102. https://doi.org/10.1002/asi.24364

[39] Pimentel, J.L. (2010). A note on the usage of Likert Scaling for research data analysis. USM R&D Journal, 18(2): 109-112. https://www.researchgate.net/publication/331231816_A_note_on_the_usage_of_Likert_Scaling_for_research_data_analysis.

[40] Abdillah, W., Hartono, J. (2015). Partial least square (PLS) Alternatif Structural Equation Modeling (SEM) Dalam Penelitian Bisnis. Yogyakarta: Penerbit Andi.

[41] Sarwono, J., Narimawati, U. (2015). Membuat Skripsi, Tesis dan Disertasi dengan Partial Least Square SEM (PLS-SEM). Yogyakarta: Andi.

[42] Zhang, J., Luximon, Y. (2021). A quantitative diary study of perceptions of security in mobile payment transactions. Behaviour & Information Technology, 40(15): 1579-1602. https://doi.org/10.1080/0144929X.2020.1771418