International Journal on
Advanced Science
Engineering
Information Technology

Vol.13 (2023) No. 2
ISSN: 2088-5334

Differences in Information Security Behavior of Smartphone Users in Indonesia Using Pearson's Chi-square and Post Hoc Test

Candiwan [a,*], Bella Pertiwi Sudirman [a], Puspita Kencana Sari [a]

[a] *School of Economics and Business, Telkom University, Bandung, 40257, Indonesia*
*Corresponding author: *candiwan@telkomuniversity.ac.id*

***Abstract*—The risk of data theft is still a negative impact of smartphone technology development that harms its users. One cause of data theft is information security behavior. Therefore, this study was conducted to determine information security behavior and its differences among smartphone users in Indonesia based on the demographic variables (i.e., gender, generation, educational background, and operating system) and four approaches, namely Avoiding Harmful Behavior, Settings, and Add-on Utilities, Preventive Behavior, and Disaster/Data Recovery. The data obtained from 400 respondents were processed using Pearson's chi-square and post hoc tests. The results showed that there are significant differences between the demographic variables and approaches. It was revealed that men behave better than women in terms of adopting settings and add-on utilities, preventive behavior, and disaster/data recovery. On the other hand, men tend to have riskier behavior than women in avoiding harmful behavior. Based on generation, it was found that Generation Z exhibits more secure behavior than Generation Y in terms of settings and add-on utilities regarding remote device locking. Meanwhile, Generation Z has better behavior than Generations X and Y in preventive behavior as they uninstall/remove unused applications. Furthermore, undergraduate users behave better than high schoolers in avoiding harmful behaviors such as sharing PIN/passwords. Lastly, iOS users were found to have better data recovery behavior than Android users in automatically backing up data in the cloud. These results can be considered when designing security education, training, and awareness programs to improve information security.**

***Keywords*—Security behavior; information security; smartphone users; user behavior; Indonesia.**

Manuscript received 23 Jun. 2022; revised 3 Sep. 2022; accepted 6 Oct. 2022. Date of publication 30 Apr. 2023.

I. Introduction

As technology advances, which continues to be witnessed worldwide [1], information technology is integral to today's life [2]. The development of information and communication technology and its associated revolution has led to the development of many mobile phone applications [3]. Mobile phones have evolved from simple means of communication to popular portable intelligent devices [4]. With the rapid development of mobile devices, smartphones have become commonplace in people's daily lives [5]. Since smartphones are connected to the Internet, they offer various uses, such as playing games, listening to music, and socializing [6]. Open connectivity is very convenient but also brings many risks that cannot be overlooked [7]. The continued integration of technology to connect and exchange data with other devices and systems over the Internet poses increasing risks to information security (IS) [8]. Therefore, smartphone security must be the primary concern of the users so that personal data is protected [9].

Organizations around the world today rely heavily on the digital world, and information systems and information security are becoming the backbone of their day-to-day operations [10]. Nevertheless, information security is a growing problem affecting businesses in nearly every industry, with data breaches affecting millions of customers and costing organizations millions of dollars [11]. Individuals and organizations risk having their information and systems compromised by malicious hackers, disgruntled employees, natural disasters, or hardware failures [12]. According to data from the National Cyber and Crypto Agency (BSSN), cyber-attack attempts in Indonesia from January to August 2020 were recorded at nearly 190 million, which means an increase of more than four times from the same period in the previous year with a range of 39 million [13]. Many cases occur in information security organizations ranging from viruses, social engineering, DoS attacks, and hackers to data theft. Security breaches have continued to increase, both in terms of the number of incidents and financial losses [14]. Secure user behavior is the key to preventing and mitigating mobile threats [15]. Poor behavior and personal awareness when using inappropriate technology pose a high risk associated with cybercrime [16]. Therefore, the user should consider mobile application security to prevent the exposure of confidential information. Smartphone users should protect their devices by setting lock screen protection, using third-party security applications, and choosing appropriate security settings because the default settings are often insufficient [17]. Information security breaches such as malware often activate unexpectedly [18]. Security breaches, such as planting a virus/malware, will have unpleasant consequences such as loss of productivity, theft of information assets, system downtime, damage to IT infrastructure, damage to the organization's reputation, lawsuits, fines, and regulatory action [19].

One popular method of distributing malware is via email attachments. To avoid such threats, users should avoid clicking on links in emails or downloading attachments from unknown or untrusted sources [20], and if people do not change their passwords, they can pose a serious security threat to users and organizations [21]. How individual users use certain applications is very important for information security when using a smartphone [22]. Shah and Agarwal [20] explained that appropriate actions on the part of users would help prevent cybersecurity incidents. They also explained that scanning smartphones regularly with anti-virus/anti-malware applications can reduce the possibility of malware infection. This preventive practice and behavior can help users protect their smartphone information's confidentiality, integrity, and availability. In addition, they explained that cybersecurity behaviors and practices refer to protective behaviors and the use of additional utilities that improve smartphone security features and security posture. Smartphones are easily stolen, lost, or infiltrated [22]. As a precaution, backup on a smartphone protects user data from the risk of data corruption or loss by saving personal information, media data, application data, and other settings [23]. Although many smartphone users are aware of the importance of information security, many are careless about their smartphones' security behavior [24]. Therefore, this study aims to find differences in smartphone users' information security behaviors in Indonesia according to four perspectives and demographic variables [20], [22].

II. Materials and Method

A. Data Description

The data used in this study are the results of questionnaires distributed to smartphone users. This study uses a quantitative descriptive method because it explains the security behavior of smartphone users. The timing of this study was cross-sectional. Based on the research strategy, data were obtained through an online survey using questionnaires distributed to 400 respondents. Data was distributed and collected through social media such as Instagram, WhatsApp, and Line. The units analyzed are individuals, namely smartphone users in Indonesia. Figure 1 is a Research Approach Based on Previous Research.

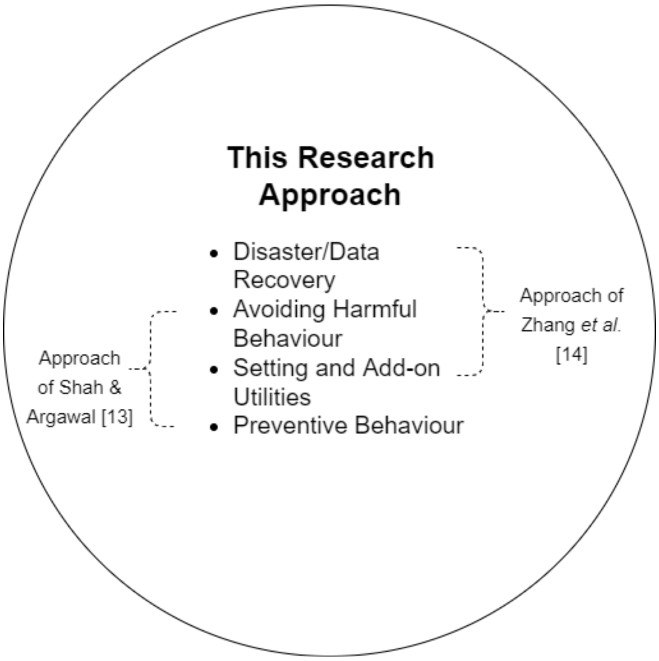
This Research Approach
Disaster/Data Recovery
Avoiding Harmful Behaviour
Setting and Add-on Utilities
Preventive Behaviour
Approach of Shah & Argawal [13]
Approach of Zhang et al. [14]

Fig. 1 Research Approach Based on Previous Research

This study uses two other studies as reference journals, namely the research of Shah and Agarwal [20] and Zhang *et al.* [22]. Shah and Agarwal [20] asserted that information security behavior consists of three approaches: settings and add-on utilities, avoiding harmful and preventive behaviors. Meanwhile, according to Zhang *et al.* [22], information security behavior is categorized as disaster/data recovery. In addition, this study was also enriched with questionnaires from other relevant studies, and experts checked the questionnaires. The validity and reliability of this study have been tested on 30 respondents. Therefore, the statement of each variable deserves to be used as a measuring tool in this study.

B. Related Work

Management information systems have several fields of study, including information systems and information security management systems [25]. Information systems can be broadly described as human-machine systems integrated into providing information to support management functions and determine alternative actions within organizational systems. Information system components are software, hardware, data, human, networks, input, output, storage, and control [26]. An information security management system is a set of policies and procedures that aim to protect information assets and provide a systematic approach to risk management [27]. The management information system is very important for information security. One of the important points in information security is behavior in the use of information systems. Behavior relates to human actions individually and in groups, and their effects on activities.

Shah and Agarwal [20] stated that information security behavior consists of 3 approaches: settings and add-on utilities, avoiding harmful behaviors and practices, and preventive behaviors and practices. In addition to these three approaches, according to Zhang *et al.* [22], information security behavior is categorized as disaster/data recovery. Shah and Agarwal's research [20] also explains that a person must have motivation and abilities above the threshold and be encouraged to perform target behaviors. Awareness of cybersecurity threats and safe behavior is the first line of defense that any individual can use. In this study, the authors use Brainware or humans as one of the components of the information system to measure the demographics of users' behavior. Demographics are measured based on aspects of gender, generation, educational background, and mobile operating system.

Shah and Agarwal [20] revealed that the respondents did not show good cybersecurity behavior overall. There were significant differences between cybersecurity behavior and practices, and independent variables such as gender, age, mobile operating system (OS), and mother tongue. Respondents were found to have a high level of motivation to protect their devices and data, but they only had a moderate level of threat awareness and ability to protect their devices and data.

Zhang *et al.* [22] also showed serious concerns about information security in the use of smartphones in China, including ignorance of security information. The study also revealed significant differences among various user groups regarding information security in smartphone use.

Nowrin and Bawden’s research [28] revealed a gap among smartphone users based on gender and educational background in the level of security behavior of smartphone users. Research conducted by Chen *et al.* [29] stated that non-science students exhibited higher levels of questionable information security behavior than science majors. Nevertheless, in research conducted by Alanazi *et al.* [30], moderators and unconventional factors such as religion and morality influence information security compliance behavior. However, demographic characteristics (age, marital status, work history, etc.) do not appear to have an effect. In addition, research conducted by Rachminingrum and Sari [31] on Android Mobile Apps users in Indonesia revealed several relationships between the security behavior sub-variables and the demographic sub-variables.

In a previous study by Letica, the more time young people spend online, the greater the privacy and information security risks they face [32]. However, Alsaleh *et al.* [33] stated that more youthful people behave more safely when using their smartphones. Regarding gender differences in cybersecurity in the organizational environment, Xu and Guo [34] explained that individual demographic factors (age and gender) do not influence security behavior. Despite gender differences, both males and females are unaware of the risks associated with smartphone use [35].

Arend *et al.*[36] stated that intent and actual behavior in cybersecurity behavior are significantly correlated with self-reported individual differences in passive risk behavior but not in proactive risk behavior. In research conducted by Shah and Agarwal [37], they also asked respondents to self-report. They found that the chances of safe behavior and practices by respondents with high motivation and high ability are 4.64 times higher than respondents with low motivation and low ability. According to research by Ali *et al.* [38], employees are more likely to comply with information security policies (ISP) if they are motivated to protect assets or exhibit behaviors motivated by protection. Research conducted by Hadlington *et al.* [39] stated that Individuals exhibiting more externality indicated weaker information security practices accepted in the workplace. Chu *et al.* [40] also noted that employees' unsafe internet usage, poor security practices, and poor access controls significantly negatively impact their willingness to report incidents.

Research conducted by Velki and Romstein [41] explained that people who know are more aware of potential security risks and, simultaneously, are more susceptible to risky behavior when using the information security behavior and awareness research system. Besides, Adebiyi *et al.* [42] mentioned that knowledge with awareness and understanding is acquired through experience, familiarity, or learning. Sang and Liao [43] also mentioned that a user's ability to distinguish information depends on the user's conscious actions and level of knowledge.

Ma [8] found that assessing coping mechanisms (response costs and self-efficacy) has important implications for protective behavioral intentions. Barth [44] explained that tech-savvy and financially independent users were at risk of potential privacy breaches despite being aware of the potential risks. In consideration, the data protection aspect did not play a significant role. Features, app design, and cost are more important than privacy concerns. Bax *et al.* [45] also stated that the cost of implementing protection against email phishing threats increases. The more protection behavior degrades, and maladaptive behavior increases.

Chowdhury *et al.* [46] stated that most cybersecurity incidents occur because users fail to behave safely. Girsang *et al.* [47] explained that cybercrimes such as phishing and cracking could lead to consumer complaints and reports suffering losses due to a lack of information and privacy security. He also explained that consumer satisfaction is influenced by information security and privacy. Chung *et al.* [48] stated that understanding information security perceptions and customer alienation through AI technology positively impacts consumer privacy concerns. Besides that, Hatamian *et al.* [49] noted that the amount and quality of privacy-related information published in user reviews and their relationship to actual app behavior suggest that user reviews are an important and valuable source of information about mobile app privacy behavior.

Zwilling et al. [50] stated that internet users have adequate cyber threat awareness but only apply minimal protective measures, which are usually relatively general and straightforward. However, the research conducted by Shadbad and Biros [51] stated that IT imposes a high level of awareness on many technostress creators, encouraging users to justify information security policy (ISP) violations and engage in non-compliant behavior. Asfoor et al. [52] stated that the human factor is the main factor in overcoming information security problems, and therefore, information security training is needed because it positively affects the level of security awareness [53].

Participation in government social media accounts can help provide knowledge and tips to the public about the latest information security threats, so it can positively influence their information security behavior through perceived severity, perceived vulnerability, self-efficacy, and response efficiency [54]. Research conducted by Kautsarina *et al.* [55] also stated that the result directly influences government engagement, privacy, perceived behavioral control, and the implementation of proactive security behaviors. Other variables have a positive and significant impact on the performance of positive security behaviors, indicating their role as mediators. Nevertheless, Schyff and Flowerday [56] found information security awareness as an indirect intermediary between openness and intent to check privacy settings. It suggests that as users become more open, they become more aware of privacy-related threats (through privacy news and events) and more willing to review their privacy settings. Breitinger *et al.* [17] stated that most users have good lock screen settings to protect their phones from physical access. However, other security best practices are ignored. For example, they are turning off unused features.

Overall, there are significant differences between several previous and current studies. The differences are in the objects and methods used. Most of the research conducted in this field has shown mixed results. However, research on the behavior of smartphone users in Indonesia is still limited. One of them is the research of Rachminingrum and Sari [31], which examined users of the Android Mobile application. Therefore, this study aims to determine the information security behavior of smartphone users in Indonesia. The findings are expected to be used in designing special training programs to improve information security for smartphone users in Indonesia.

C. *Research Method*

This study was conducted with four approaches: setting and add-on utility, avoiding harmful behavior, preventive behavior, and disaster/data recovery. Besides, respondents were asked to self-assess their interest in protecting smartphone devices and data related to motivation, ability, and threat awareness variables. The framework model in this study is shown in Figure 2.

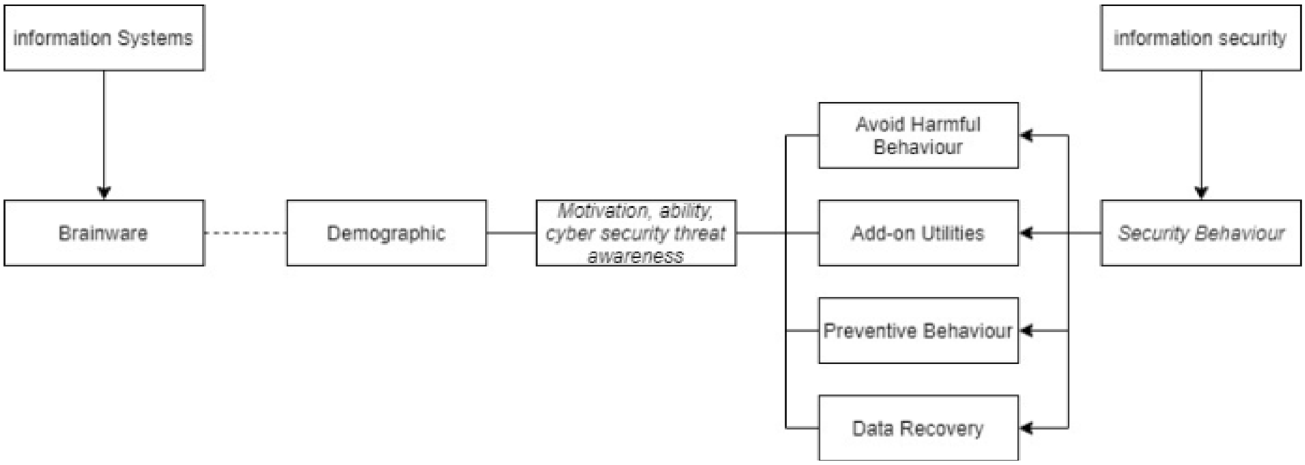

Fig. 2 Framework model of Security Behaviour

In this study, the author uses one of the components of the information system, namely brainwave or humans, to measure user behavior in terms of the user's demographics. Demographics are measured based on aspects of generation, gender, educational background, and mobile operating system. The analytical techniques used in this study include Pearson's chi-square test and post hoc test with the proportion column and Bonferroni correction. This study used Pearson's chi-square test with SPSS software to find the relationship between demographic variables and the security behavior of smartphone users. The variables considered in this study were gender, generation, educational background, and smartphone users' operating system (OS). The hypotheses of this research are formulated as follows

- H0: There is no significant difference between the two variables
- Ha: There is a significant difference between the two variables

The following decisions were made based on the significance value (Asymp. Sig.):

- If the value of Asymp. Sig. (*p*) <0.05, it means that H0 is rejected and Ha is accepted
- If the value of Asymp. Sig. (*p*) > 0.05, it means that H0 is accepted, and Ha is rejected

This research was conducted using a post hoc test with the proportion column and Bonferroni correction processed by SPSS software. According to Norman and Streiner [57], post hoc is used for further data exploration after finding significant effects. The Bonferroni correction was proposed to avoid problems when the number of tests increased, and errors in concluding a significant difference might occur, but when tested further, there was no such significant difference [58]. The tests were adjusted for all pairwise comparisons in one row of each subtable using Bonferroni correction [59] to examine whether the proportion of respondents in one column significantly differs from the one in another. If there is a significant difference in the variables previously tested using Pearson's chi-square test, then further testing is carried out to identify the items from the variables that provide the significant difference. However, if no differences are found among the tested variables, a post hoc test is not required [60]. Figure 3 is a diagram of the data processing in this study.

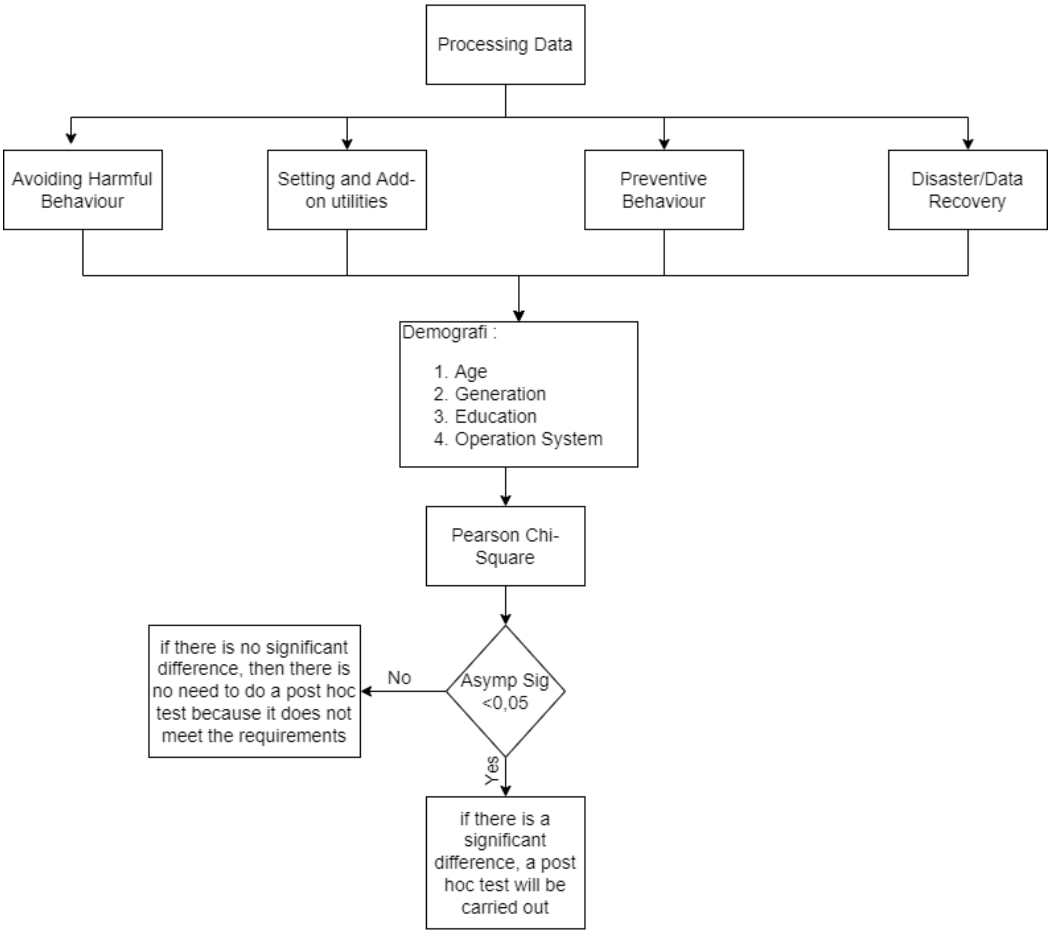
Processing Data
Avoiding Harmful Behaviour
Setting and Add-on utilities
Preventive Behaviour
Disaster/Data Recovery
Demografi :
1. Age
2. Generation
3. Education
4. Operation System
Pearson Chi-Square
Asymp Sig <0,05
No
if there is no significant difference, then there is no need to do a post hoc test because it does not meet the requirements
Yes
if there is a significant difference, a post hoc test will be carried out

Fig. 3 Processing Data

The following hypotheses were obtained based on previous studies and the theoretical basis of this research. Gender-based hypotheses: In research entitled Cybersecurity behavior of smartphone users in India: an empirical analysis [20], men demonstrated risky behavior by downloading applications from untrusted third parties, connecting to insecure free Wi-Fi networks, updating applications, and rooting or jailbreaking. However, male respondents were better at reading user agreements and checking app permissions. Research on university students found that male smartphone users were more aware of using backup data.

- H1. Men are more likely to adopt settings and add-on utilities than women.
- H2. Men are worse than women at avoiding harmful behavior in smartphone use.
- H3. Men have better preventive behavior than women in smartphone use.
- H4. Men have better data recovery behavior than women in smartphone use.

Generation-based hypotheses: The generation in this study represents a certain age group. Previous studies [20], [31] revealed that smartphone users of different ages significantly differ in security behavior.

- H5. There are differences between generations in avoiding harmful behavior.
- H6. There are differences between generations in adopting add-on settings and utilities.
- H7. There are differences between generations in carrying out preventive behavior.
- H8. There are differences between generations in dealing with disaster/data recovery.

Operation system-based hypotheses: Previous research [20] revealed that Android users behave more safely than iOS users. iOS respondents were more aware of the device-tracking services than the Android respondents. Android users demonstrated safe practices by scanning smartphones using anti-virus/anti-malware, signing out of the apps, and checking permissions for apps.

- H9. Android users tend to avoid harmful behavior in smartphone use better than iOS users.
- H10. Android users tend to be more secure in adopting settings and add-on utilities in smartphone use than iOS users.
- H11. Android users tend to have better preventive behavior in using smartphones than iOS users.
- H12. Android users tend to exhibit safer behavior dealing with disaster/data recovery in using smartphones than iOS users.

Educational background-based hypotheses: a previous study [31] divided educational background into seven groups and revealed that respondents with the last educational background of junior high school or equivalent had the highest average level of security behavior.

- H13. There are differences in the security behavior of smartphone users based on their educational background in avoiding harmful behavior.

- H14. There are differences in the security behavior of smartphone users based on their educational background in adopting settings and add-on utilities.
- H15. There are differences in the security behavior of smartphone users based on their educational background in carrying out preventive behavior.
- H16. There are differences in the security behavior of smartphone users based on their educational background in dealing with disasters/data recovery.

Motivation, ability, and threat awareness-based hypotheses: Previous research [20] revealed that there is a gap between the level of motivation and the adoption of security controls. Therefore, motivation, ability, and threat awareness show a mismatch with the application of user security behavior.

- H17. Motivation, ability, and threat awareness of smartphone users are not in accordance with the implementation of the security behavior of smartphone users.

III. Result and Discussion

This study obtained data from 400 respondents based on gender, generation, educational background, and operating system as shown in Table 1.

TABLE I
FREQUENCY OF DEMOGRAPHIC VARIABLES

Item	Response	Frequency
Gender	Male	152
	Female	248
Generation	Generation Z	325
	Generation Y	47
	Generation X	27
	Baby Boomer	1
Education Background	Primary school	2
	Junior high school	3
	Senior high school	249
	Diploma	28
	Undergraduate	111
	Graduate	6
	Post-graduate	1
Operation System	Android	269
	iOS	131

In this study, security behavior was tested using four approaches, namely Setting and Add-on Utilities (AU), Avoiding Harmful Behavior (AHB), Preventive Behavior (PB), and Disaster/Data Recovery (DR). The findings of this study can be seen in Table 2.

TABLE II
THE PEARSON CHI-SQUARE VALUE

Security Behavior	Item	Demographic			
		Gender	Generation	Education	Operation System
AU1	Did you activate the authentication mechanism?	0.038	NS	NS	NS
AU2	Have you turned on automatic updates?	NS	NS	NS	NS
AU3	Do you activate the screen lock?	NS	NS	NS	NS
AU4	Have you enabled any data encryption on your smartphone?	NS	NS	NS	NS
AU5	Do you disable GPS when not needed?	NS	NS	NS	NS
AU6	Do you turn off Bluetooth if not needed?	NS	NS	NS	0.000
AU7	Do you destroy the memory card safely when it is not used?	NS	0.000	0.007	0.000
AU8	Have you enabled remote tracking of the device?	0.002	NS	NS	0.000
AU9	Have you turned on data wipe remotely?	0.025	NS	NS	0.000
AU10	Have you enabled remote locking of the device?	NS	0.045	NS	NS
AHB1	Do you share your PIN/password information?	0.009	0.007	0.003	0.010
AHB2	Have you clicked on a link in an email from an unknown source?	NS	NS	NS	NS
AHB3	Did you click on the link in SMS or WhatsApp from unknown sources?	NS	NS	NS	NS
AHB4	Have you clicked on a link on a social network from an unknown source?	NS	NS	NS	NS
AHB5	Did you click on the email link while using the application?	NS	NS	NS	NS
AHB6	Do you click on the SMS or WhatsApp link while using the application?	NS	NS	NS	NS
AHB7	Do you click on social network links while using the application?	NS	NS	NS	NS
AHB8	Are you downloading applications from untrusted third-party websites?	NS	NS	NS	NS
AHB9	Are you connecting to an unsecured free Wi-Fi network?	NS	NS	NS	NS
AHB10	Did you download attachments from unknown emails?	NS	NS	NS	NS
AHB11	Do you upload location-based information on social networking sites?	NS	NS	NS	NS
AHB12	Are you Jailbreaking or Rooting?	0.001	NS	NS	NS
AHB13	Did you click on the email link while playing games?	NS	0.005	NS	NS

AHB14	Do you click on SMS or WhatsApp links while playing games?	0.018	NS	NS	0.010
AHB15	Do you click on social network links while playing games?	0.012	NS	NS	NS
PB1	Do you change your PIN/password frequently?	NS	0.003	NS	NS
PB2	Are you using anti-virus / anti-malware?	NS	NS	NS	NS
PB3	Do you regularly update the applications?	0.003	NS	NS	0.003
PB4	Do you uninstall/delete unused applications?	NS	0.001	NS	NS
PB5	Have you logged out your account from services like email and Facebook?	NS	NS	NS	0.045
PB6	Have you set a different password for the application?	NS	0.045	NS	NS
PB7	Did you check the permissions when installing the application?	0.010	NS	NS	NS
PB8	Did you read the end-user agreement?	NS	NS	NS	NS
PB9	Did you pay attention to the IMEI number?	0.021	NS	NS	NS
DR1	Do you backup data manually to USB / hard disk or other media?	NS	NS	NS	NS
DR2	Do you backup data automatically in the cloud?	NS	0.001	NS	0.000
DR3	Do you backup data when the smartphone is about to be reset or reinstalled?	NS	NS	NS	0.000
DR4	Do you erase data when the smartphone is about to be discarded?	NS	NS	NS	0.000
DR5	Do you insure your smartphone?	NS	0.004	NS	0.003

In the table above, NS stands for Not Significant with criteria Asymp. Sig. > 0.05, and if Asymp. Sig. <0.05, then there is a significant difference. In the table above, there are ten questions about setting and add-on utilities, 15 questions about avoiding harmful behavior, nine questions about preventive behavior, and five questions about disaster/data recovery with respect to gender, generation, education, and operation system. The following is an explanation of the results obtained :

A. Chi-Square Result

Based on the results of the chi-square test in Table 2, it can be concluded that there are ten significant items among the variables based on **gender** and **security behavior**:

- Three items are significant in setting and add-on utilities, including activating the authentication mechanism, enabling remote tracking of the device, and enabling remote wipe of data. The most significant is enabling remote device tracking, and the least is activating the authentication mechanism.
- Four items are significant for avoiding harmful behavior, including sharing PIN/password information, Jailbreaking or Rooting, clicking on SMS or WhatsApp links while playing games, and clicking on social network links while playing games. The most significant is Jailbreaking or Rooting, and the least is clicking on social network links while playing games.
- Three items are significant in preventive behavior, including updating applications regularly, checking the permissions when installing the application, and paying attention to the International Mobile Equipment Identity (IMEI) number. The most significant is updating applications regularly, and the least is paying attention to the International Mobile Equipment Identity (IMEI) number.
- No significant differences were found in dealing with disaster/data recovery.

There are nine significant items between the variables based on **generation** and **security behavior**:

- Two items are significant in setting and add-on utilities. The most significant is safely destroying memory cards when not in use, and the least is enabling the device lock remotely.
- Two items are significant in avoiding harmful behavior, and the most significant is clicking on email links while playing games, and The least is sharing PIN/password information.
- Three items are significant in preventive behavior, including changing PIN/password frequently, uninstalling/deleting unused applications, and setting a different password for the application. The most significant is changing PIN/password frequently, and the least is setting a different password for the application.
- Two items are significant in dealing with disaster/data recovery. The most significant is backing up data automatically in the cloud; the least is insuring the smartphone.

There are two significant items between the **educational background variable** and **security behavior**:

- One significant item in setting and add-on utilities is safely destroying the memory card when not in use.
- One significant item in avoiding harmful behavior is sharing PIN/password information.
- There is no significant difference in preventive behavior and disaster/data recovery.

There are 12 significant items between **operating system variables** and **security behavior** :

- Four significant items in setting and add-on utilities include turning off Bluetooth when not needed, destroying memory cards safely when not in use, enabling remote tracking of the device, and turning on data wipe remotely.
- Two significant items in avoiding harmful behavior include sharing PIN/password information and clicking on SMS or WhatsApp links while playing games.

- Two items are significant in preventive behavior. The most significant is updating applications regularly and the least is logging out of accounts from services like email and Facebook.
- Four significant items in disaster/data recovery include backing up data automatically in the cloud, backing up data when the smartphone is about to be reset or reinstalled, erasing data when the smartphone is about to be discarded, and insuring the smartphone. The less significant is insuring the smartphone.

B. Post Hoc Result

After the chi-square test, the significantly different items as shown in Table 2 were tested using the post hoc test. The post hoc test results for each significantly different item are indicated by letters in dark-colored cells in Table 3. Baby boomers, Primary school, and Post-graduates are not used in this test because the column proportions are equal to zero or one. The dark cells with post hoc analysis results in table III indicate a significant difference between items of settings and add-on utilities based on demographic variables.

TABLE III
POST HOC TEST RESULTS BETWEEN DEMOGRAPHICS, AND SETTINGS AND ADD-ON UTILITIES

Item	**Answer choices**	**Gender**		**Generation**			**Education**					**Operation System**	
		Man (A)	**Women (B)**	**Z(C)**	**Y(D)**	**X(E)**	**Junior high school (G)**	**Senior high school (H)**	**Diploma (I)**	**Undergraduate (J)**	**Graduate (K)**	**Android (L)**	**iOS (M)**
Enabling authentication mechanism	Yes	B										NOT SIGNIFICANT	
	No		A										
	DNK												
Enabling remote tracking of the device	Yes	B											L
	No			NOT SIGNIFICANT			NOT SIGNIFICANT					M	
	DNK		A										
Turning on data wiping remotely	Yes	B											L
	No											M	
	DNK												
Destroying the memory card safely when it is not used	Yes					C							
	No			E								M	
	DNK							J					L
Enabling remote locking of the device	Yes	NOT SIGNIFICANT											
	No				C							NOT SIGNIFICANT	
	DNK						NOT SIGNIFICANT						
Turning off Bluetooth if not needed	Yes											M	
	No												L
	DNK												

In Table 3, there are three answer choices, namely yes, no, and do not know (DNK). Based on ***gender,*** there are three significant differences. Men show safer behavior than women in terms of activating authentication mechanisms, enabling remote tracking, and activating data wiping remotely. Based on ***generation,*** there are two significant items. Generation X has safer behavior in destroying memory cards when not in use compared to Generation Z. Meanwhile, Generation Z is better at remotely locking devices than Generation Y. Based on ***education background,*** there is only 1 significant item. In terms of safely destroying memory cards when not in use, more users with high school background chose the answer of "don't know" than those with undergraduate background. It means, many users with high school background are still not familiar with this.

There are four significant items related to the ***operating system.*** Overall, iOS users seem to behave better than Android users in terms of safely destroying memory cards when not in use, enabling remote tracking of the device and enabling remote wipe of data. On the other hand, Android users seem to have better behavior in turning off Bluetooth when not needed compared to iOS users.

Post hoc analysis revealed that there were significant differences between the variables based on demographics and ***avoiding harmful behavior.*** The findings of this study can be seen in Table 4.

TABLE IV
POST HOC TEST RESULTS BETWEEN DEMOGRAPHICS AND AVOIDING HARMFUL BEHAVIOR

Item	**Answer choices**	**Gender**		**Generation**			**Education**					**Operation System**	
		Man (A)	**Women (B)**	**Z (C)**	**Y (D)**	**X (E)**	**Junior high school (G)**	**Senior high school (H)**	**Diploma (I)**	**Undergraduate (J)**	**Graduate (K)**	**Android (L)**	**iOS (M)**
Sharing PIN/password information	Never	B			C	C				H		M	
	Rarely												
	Occasionally		A	D									
	Frequently												L
	Very frequently										H		

Jailbreaking or Rooting	Never		A								
	Rarely										
	Occasionally										
	Frequently	B									
	Very frequently										
Clicking on SMS or WhatsApp link while playing a game	Never		A								
	Rarely										
	Occasionally										
	Frequently	B									
	Very frequently										
Clicking on social network links while playing a game	Never					CD				NOT SIGNIFICANT	
	Rarely										
	Occasionally										
	Frequently	B					NOT SIGNIFICANT				
	Very frequently	B									
clicking on the email link while playing a game	Never										
	Rarely										
	Occasionally										
	Frequently										
	Very frequently										
clicking on links on Social Networks from unknown sources	Never	NOT SIGNIFICANT								M	
	Rarely										L
	Occasionally										
	Frequently										
	Very frequently										

In Table 4, based on ***gender,*** there are four significant items. Women appear to have worse behavior than men when it comes to sharing PIN/password information. On the other hand, it is shown that men are worse and riskier than women in avoiding harmful behaviors such as jailbreaking or rooting, clicking on SMS or WhatsApp links while playing games, and clicking on social networking links while playing games. Based on ***generation,*** There are two significant items. Overall, Generation Y and Generation X appear to have more secure behaviors than Generation Z, such as when it comes to sharing PIN/password information and clicking email links while playing games. Based on ***educational background***, there is only one significant item, namely sharing PIN/password information. Respondents with a bachelor's education background have better behavior than high school students in terms of sharing PIN/password information, while those with a graduate background show worse behavior than high school respondents. Then based on the ***operation system,*** there are two significant items concerning operating systems. Android users have a more secure behavior than iOS users in sharing PIN/password information and clicking links on social networks from unknown sources.

Post hoc analysis revealed that there were significant differences between the variables based on demographics and ***preventive behavior.*** The findings of this study can be seen in Table 5.

TABLE V
POST HOC TEST RESULTS BETWEEN DEMOGRAPHICS AND PREVENTIVE BEHAVIOR

Item	**Answer choices**	**Gender**		**Generation**			**Operation System**	
		Man (A)	**Women (B)**	**Z (C)**	**Y (D)**	**X (E)**	**Android (F)**	**iOS (G)**
Updating the application on a regular basis	Never						G	
	Rarely		A					
	Occasionally							
	Frequently							
	Very frequently	B						
Checking permissions when installing the app	Never							
	Rarely		A					
	Occasionally			NOT SIGNIFICANT				
	Frequently							
	Very frequently							
Paying attention to the IMEI number	Never						NOT SIGNIFICANT	
	Rarely							
	Occasionally							
	Frequently	B						
	Very frequently							
	Never	NOT SIGNIFICANT			C	C		

Frequently changing PIN/password	Rarely							
	Occasionally							
	Frequently							
	Very frequently							
Uninstalling/deleting unused applications	Never				C			
	Rarely					C		
	Occasionally							
	Frequently							
	Very frequently			D				
Setting a different password for the app	Never					C		
	Rarely							
	Occasionally							
	Frequently							
	Very frequently							
Logging out account from services like email and Facebook	Never							
	Rarely							
	Occasionally			NOT SIGNIFICANT				
	Frequently							F
	Very frequently							

It can be seen in Table 5 that there are three significant items based on ***gender***. Overall, men performed better preventive behavior than women, such as updating apps regularly, checking permissions when installing apps, and paying attention to IMEI numbers. Meanwhile, no significance was found ***in the last 3 items of table 5*** after the post hoc test was carried out. Then, there are three significant items based on ***generation***. Generation Z shows better behavior than generations X and Y in terms of changing PIN/password frequently and uninstalling/deleting unused applications. Meanwhile, Generation X is wasteful by setting different passwords for their apps. Finally, based on the operating system, there are two important items. Android users exhibit worse behavior than iOS users when it comes to updating apps regularly. But when it comes to logging out of services like email and Facebook, iOS users exhibit better behavior than Android users.

Post hoc analysis revealed that there were significant differences between items of ***disaster/data recovery*** and the variables based on demographics**.** The findings of this study can be seen in Table 6.

TABLE VI
POST HOC TEST RESULTS BETWEEN DEMOGRAPHICS AND DISASTER/DATA RECOVERY

Item	**Answer choices**	**Generation**			**Operation System**	
		Z (A)	**Y (B)**	**X (C)**	**Android (D)**	**iOS (E)**
Backing up data automatically in the cloud	Never		A	A	E	
	Rarely				E	
	Occasionally					
	Frequently					D
	Very frequently	B				D
Insuring the Smartphone	Never		A	A	E	
	Rarely					
	Occasionally					
	Frequently					
	Very frequently					D
Backing up data when the smartphone is about to be reset or reinstalled	Never				E	
	Rarely				E	
	Occasionally					
	Frequently					
	Very frequently					D
Performing data deletion when the smartphone is about to be discarded	Never	NOT SIGNIFICANT			E	
	Rarely					
	Occasionally					
	Frequently					
	Very frequently					D

It can be seen in Table 6 that there are two significant items related to ***generation***: Generation Z has good behavior in automatically backing up data in the cloud and insuring smartphones. In addition, there are four significant items based on the ***operating system***, namely iOS users have better behavior than Android users in terms of automatically backing up data in the cloud, insuring smartphones, backing up data when the smartphone is about to be reset or reinstalled, and deleting data when the smartphone is about to be discarded.

In this study, descriptive analysis was used for hypotheses 1 to 4 and 9 to 12 because the hypotheses relate to safer or riskier security behaviors. Post hoc analysis was used for hypotheses 5 to 8 and 13 to 16 because the hypotheses were about significant or insignificant differences between security behaviors and demographics [20].

Hypothesis 1 states that men are more likely to adopt settings and add-on utilities than women. In this study it was revealed that the answer "Yes" was chosen by 58.95% men and 53.67% women. This means that men are better than women in adopting settings and add-on utilities. Similar findings were seen in a study by Nowrin and Bawden [28], men are relatively more aware than women in terms of adopting add-on utility features such as configuring automatic locking. Therefore, hypothesis 1 is accepted. This finding is in accordance with a previous study conducted by Shah and Agarwal [20] on smartphone users in India, which revealed that male respondents were better than women in implementing security controls.

Hypothesis 2 states that men are worse than women at avoiding harmful behavior in smartphone use. Overall, the average number of women who answered "never" in avoiding harmful behavior was 45,91%, while for men it was 43,51%. This means that men tend to show bad behavior and are at risk of avoiding harmful behavior compared to women. Therefore, hypothesis 2 is accepted. This finding is in accordance with a previous study conducted by Shah and Agarwal [20] on smartphone users in India, which revealed that men exhibit risky behavior in downloading applications from untrusted third parties, connecting to insecure free Wi-Fi networks, updating applications, and rooting or jailbreaking.

Hypothesis 3 states that men have better preventive behavior than women in smartphone use. Overall, the percentage number of women and men who answered "Frequently" and "Very Frequently" was 33,12% and 37,36%, respectively. This means that men are better at preventing smartphones from threats than women. Therefore, hypothesis 3 is accepted. This finding is in accordance with a previous study conducted by Shah and Agarwal [20] on smartphone users in India, which revealed that male respondents were better at reading user agreements and checking app permissions.

Hypothesis 4 states that men have better data recovery behavior than women in smartphone use. Overall, the percentage number of men and women who answered "Frequently" and "Very Frequently" was 40,12% and 38,40%, respectively. This means that men behave better than women in disaster/data recovery. Therefore, hypothesis 4 is accepted. This finding is similar to a previous study examining smartphone users in Bangladesh, which revealed that male smartphone users were more aware of the use of backup data [28].

Post hoc analysis revealed that there were two significant items between setting and add-on utilities, and generation. In safely destroying memory cards when not in use, Generation X shows more secure behavior than Generation Z. Meanwhile, Generation Z is better at enabling remote device locking than Generation Y. In avoiding harmful behavior, there are two significant items. Overall, generations Y and X demonstrated more secure behaviors than Generation Z, such as in sharing PIN/password information and clicking email links while playing games. In preventive behavior, there are three significant items. Generation Z exhibits good behavior in frequently changing PIN/password, uninstalling/removing unused apps and setting different passwords for apps. In Disaster / Data Recovery, there are two significant items. Generation Z shows good behavior in automatically backing up data in the cloud and insuring Smartphones. Similar findings were seen in a study by Alsaleh, *et al.* [33], in which younger people are more secure when using a smartphone such as when it comes to backing up data. Therefore, **H5, H6, H7, and H8** are accepted. The generation in this study is a generalization of the development of age groups. This finding is consistent with a previous study conducted by Shah and Agarwal [20] on smartphone users in India, which revealed that there were significant differences in security behavior with respect to the age of the users. In addition, this study is also similar to the one conducted by Rachminingrum and Sari [31], which revealed that there were significant differences in security behavior with respect to the ages of users.

Hypothesis 9 states that Android users tend to be better at avoiding harmful behavior in smartphone use than iOS users. Overall, the average number of Android and iOS users who answered "Never" was 47,05% and 40,75%, respectively. It means that Android users behave more safely than iOS in avoiding harmful behavior. This finding is in accordance with a previous study conducted by Shah and Agarwal [20] on smartphone users in India, which revealed that Android users behave more safely than iOS users.

Hypothesis 10 states that Android users tend to have more secure behavior in adopting settings and add-on utilities in smartphone use than iOS users. Overall, the average number of Android and iOS users who answered "Yes" was 54,02% and 59,09%, respectively. It means that iOS users behave more safely than Android users in adopting settings and add-on utilities. Therefore, hypothesis 10 is rejected. This finding is different from the findings made by Shah and Agarwal [20]. It is because the research conducted by Shah and Agarwal [20] has a relatively small sample. In addition, cultural differences between India and Indonesia could also be the cause.

Hypothesis 11 states that Android users tend to have better preventive behavior in using smartphones than iOS users. Overall, the average number of Android and iOS users who answered "Frequently" and "Very Frequently" was 33,58% and 37,09%%, respectively. This means that iOS users behave more safely than Android in preventive behavior. Therefore, hypothesis 11 is rejected. This finding is different from that of Shah and Agarwal [20]. This is because the research conducted by Shah and Agarwal [20] has a relatively small sample. In addition, cultural differences between India and Indonesia could also be the cause.

Hypothesis 12 states that Android users tend to have better behavior than iOS users in dealing with disasters/data recovery when using smartphones. Overall, the percentage of Android and iOS users who answered "Frequently" and "Very Frequently" was 33% and 44%, respectively. It means that iOS users behave more safely than Android users in handling disaster/data recovery. Therefore, hypothesis 12 is rejected. This is a new indicator, a combination of journals conducted by Shah and Agarwal [20] and Rachminingrum and Sari [31], in which Shah and Agarwal [20] analyzed based on the user's operating system, while Rachminingrum and Sari [31] conducted research using disaster/data recovery approach.

Post hoc analysis revealed that there was 1 significant item between setting and add-on utilities, and educational background. In destroying memory cards safely when not in use, users with senior high school background chose "Do Not Know" more than users with the undergraduate background. It means that there are still many users with a senior high school background who do not know this item. There is one significance in avoiding harmful behavior. In sharing PIN/password information, respondents with an undergraduate education background showed better behavior than high school graduates, while graduates showed poor behavior compared to respondents with high school education background. Similar findings were seen in a study by Velki and Romstein [41]. The last educational background of users shows their harmful behavior in using smartphones. There were no significant items in preventive behavior and disaster/data recovery.

Therefore, **hypotheses 13 and 14** were accepted. This finding is in line with the findings of a previous study by Rachminingrum and Sari [31] on Android Mobile Apps users in Indonesia, which revealed that users' last educational background had relationships and differences with harmful behavior and add-on utilities. **Hypothesis 15** is rejected because there is no significant difference in the security behavior of smartphone users based on educational background related to preventive behavior. Hypothesis 15 is a new indicator, a combination of research by Shah and Agarwal [20] and Rachminingrum and Sari [31], in which Shah and Agarwal [20] used a preventive behavioral approach, and Rachminingrum and Sari [31] analyzed based on educational background.

Hypothesis 16 was rejected because there is no significant difference in the security behaviour of Smartphone users based on their educational background related to disaster/data recovery. Meanwhile, research by Rachminingrum and Sari [31] has a significant difference because there are fewer questionnaire items than those in this study. Items on data recovery are only used to back up information on the smartphone and delete smartphone data and information when it reaches the end of its useful life.

TABLE VII
VALUE OF MOTIVATION, ABILITY, AND THREAT AWARENESS OF SMARTPHONE USERS

	Item	Very Low	Low	Medium	High	Very High
Motivation	My interest in avoiding harmful behavior when using smartphone	3%	5%	30%	47%	3%
	My interest in setting up and using add-on features to increase smartphone security	4%	6%	25%	32%	33%
	My interest in taking precautions that can help protect smartphone data	3%	4%	17%	***30%***	***46%***
	My interest in recovering data after a disaster (both natural disasters and damage caused by human negligence)	3%	6%	19%	33%	39%
Ability	My ability to avoid harmful behavior when using a smartphone	3%	9%	28%	***32%***	***28%***
	My ability to set up and use add-on features to increase smartphone security	4%	10%	35%	31%	20%
	My ability to take precautions that can help protect smartphone data	3%	8%	33%	31%	25%
	My ability to recover data after a disaster (both natural disasters and damage caused by human negligence)	5%	11%	34%	27%	23%
Threat Awareness	My awareness regarding threats due to harmful behavior when using a smartphone	5%	5%	18%	**35%**	**37%**
	My awareness of threats caused by not making adjustments and using add-on features to increase smartphone security	6%	7%	28%	34%	25%
	My awareness of the threats caused by not taking precautions that can not help protect smartphone data	5%	7%	23%	35%	30%
	My awareness regarding the threat of not recovering data after a disaster (both natural disasters and damage caused by human negligence)	5%	5%	25%	34%	31%

Overall, respondents reported high motivation, ability, and threat awareness levels in protecting their smartphone devices and data. However, smartphone users' adoption of security behaviors to protect devices and data is reported to be low. It can be seen in Table 7 that the user's motivation in taking preventive actions that can help protect smartphone data is at a higher rate (High and Very High) with a value of 76%, and User awareness of threats due to harmful behavior when using a smartphone is at a higher rate with values 72% .

In addition to being highly motivated to take precautions that can help protect smartphone data, respondents are also very aware of the threat of harmful behavior when using smartphones. However, as shown in Table 8, the average percentage of the answer choices "Frequently" and "Very Frequently" in taking precautions that can help protect smartphone data is 31.44% (31.4%), which means that respondents have dangerous behavior in protecting their smartphones. This contradicts the report that respondents have high motivation and awareness in protecting their smartphone devices and data. One of the reasons for this discrepancy between motivation, threat awareness and implementation of security behavior is that respondents never or rarely change their PIN/password (PB1).

Furthermore, Table 7 also illustrates that the levels of abilities are classified as high, such as the ability of users to recover data after a disaster (both natural disasters and damage due to human error), which is at a high rate, with a value of 60%. However, this is not in line with the evidence of disaster/data recovery implementation presented in Table 8 in which the average percentage of the answer choices "often" and "very often" is only 39%. This is because respondents never or rarely back up data automatically in the cloud (DR5) and manually on a USB/hard disk or other media (DR1).

TABLE VIII
PERCENTAGE OF RESPONDENTS' ANSWERS IN AVOIDING HARMFUL BEHAVIOR, PREVENTIVE BEHAVIOR AND DISASTER BEHAVIOR

Item	Never	Rarely	Occasionally	Frequently	Very Frequently	Item	Never	Rarely	Occasionally	Frequently	Very Frequently
AHB1	32%	29%	22%	11%	6%	**PB1**	14%	25%	38%	**16%**	**7%**
AHB2	52%	28%	15%	4%	1%	PB2	23%	23%	25%	20%	9%
AHB3	72%	16%	8%	**3%**	**1%**	PB3	10%	16%	36%	25%	13%
AHB4	46%	29%	17%	6%	2%	PB4	7%	21%	35%	33%	4%
AHB5	26%	27%	25%	16%	6%	PB5	8%	23%	20%	33%	16%
AHB6	41%	28%	18%	9%	4%	PB6	23%	22%	27%	18%	10%
AHB7	16%	25%	29%	22%	8%	PB7	10%	16%	31%	25%	18%
AHB8	45%	28%	18%	7%	2%	PB8	18%	21%	33%	17%	11%
AHB9	38%	27%	22%	9%	4%	PB9	22%	19%	26%	17%	16%
AHB10	55%	26%	12%	5%	2%	**Average**	**16.67%**	**20.33%**	**31.56%**	**20.78%**	**10.67%**
AHB11	30%	29%	28%	10%	3%	**DR1**	15%	18%	31%	**21%**	**15%**
AHB12	60%	19%	12%	6%	3%	DR2	23%	16%	24%	20%	17%
AHB13	51%	21%	12%	11%	5%	DR3	13%	15%	19%	25%	28%
AHB14	65%	17%	11%	5%	2%	DR4	19%	12%	18%	21%	30%
AHB15	45%	20%	17%	12%	6%	**DR5**	49%	18%	14%	**10%**	**9%**
Average	**44.93%**	**24.60%**	**17.73%**	**9.07%**	**3.67%**	**Average**	**24%**	**16%**	**21%**	**19%**	**20%**

Therefore, the motivation, ability, and threat awareness of smartphone users are not in accordance with the implementation of security behavior of smartphone users. Thus, hypothesis 17 is accepted. This finding is consistent with a previous study conducted by Shah and Agarwal [20] on smartphone users in India, which revealed that motivation, ability, and threat awareness were not correlated with users' adoption of security behaviors. Based on the evaluation of the results mentioned above regarding the behavior of smartphone users, it is necessary to consider designing a special security education, training and awareness (SETA) program to improve information security for smartphone users [37].

IV. Conclusion

This study found that there were significant differences between demographics (i.e., gender, generation, educational background, and operating system) and security behaviors. Descriptive analysis revealed that men are better than women in adopting settings and add-on utilities, preventive behavior, and disaster/data recovery. However, men tend to have worse and riskier behaviors than women in avoiding harmful behaviors. Android users behave more safely than iOS in avoiding harmful behavior. In contrast, iOS users behave more safely than Android in adopting settings and add-on utilities, preventive behavior, and disaster/data recovery.

Post hoc analysis revealed that men behave more securely than women in terms of activating authentication mechanisms. In remote locking of devices, generation Z has a more secure behavior compared to generation Y. Generation Z also shows better behavior than generations X and Y regarding frequent changing of PIN/password and uninstalling/deleting unused apps. In terms of sharing PIN/password information, undergraduate users behave better than high school users. When it comes to automatically back up data in the cloud, iOS users have better behavior than Android users.

This study also found that the motivation, ability, and threat awareness of smartphone users are not under the implementation of the security behavior by smartphone users. One of the reasons for this discrepancy is that the respondents never or rarely change their PIN/password (PB1).

This study's variables and indicators of security behavior can be used as reference material for further research. The researchers only examined the characteristics of respondents based on gender, generation, educational background, and operating system of smartphone users. Future researchers are expected to be able to examine security behavior based on other characteristics such as occupation and income of smartphone users.

Referring to the results of this study, it is recommended that male smartphone users pay more attention to their information security behavior by avoiding dangerous behavior when using smartphones. On the other hand, female smartphone users are expected to adopt settings and add-on utilities and take precautions to protect smartphone data and recover data after a disaster. The results of this study can be considered for designing a special security education, training, and awareness (SETA) program to improve the information security of smartphone users. Smartphone manufacturers' research and design department can also consider these results to add utilities in the devices to help users secure their data.

Acknowledgment

The authors thank Telkom University for providing access to important papers related to this research.

References

[1] A. Farooq, D. Jeske, and J. Isoaho, “Predicting students’ security behavior using information-motivation-behavioral skills model,” *IFIP Advances in Information and Communication Technology*, vol. 562. pp. 238–252, 2019, doi: 10.1007/978-3-030-22312-0_17.

[2] A. Kovacevic, N. Putnik, and O. Toskovic, “Factors Related to Cyber Security Behavior,” *IEEE Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[3] K. A. Abdullahi, O. I. Oladele, and M. Akinyemi, “Attitude, knowledge and constraints associated with the use of mobile phone

applications by farmers in North West Nigeria," *J. Agric. Food Res.*, vol. 6, p. 100212, 2021, doi: 10.1016/j.jafr.2021.100212.

[4] J. Nie, P. Wang, and L. Lei, "Why can't we be separated from our smartphones? The vital roles of smartphone activity in smartphone separation anxiety," *Comput. Human Behav.*, vol. 109, no. September 2019, p. 106351, 2020, doi: 10.1016/j.chb.2020.106351.

[5] P. A. Busch, G. I. Hausvik, O. K. Ropstad, and D. Pettersen, "Smartphone usage among older adults," *Comput. Human Behav.*, vol. 121, no. March, 2021, doi: 10.1016/j.chb.2021.106783.

[6] A. Razgallah, R. Khoury, S. Hallé, and K. Khanmohammadi, "A survey of malware detection in Android apps: Recommendations and perspectives for future research," *Comput. Sci. Rev.*, vol. 39, p. 100358, 2021, doi: 10.1016/j.cosrev.2020.100358.

[7] Q. Xiao, "Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study," *Telemat. Informatics*, vol. 58, no. November 2020, p. 101535, 2021, doi: 10.1016/j.tele.2020.101535.

[8] X. Ma, "IS professionals' information security behaviors in Chinese IT organizations for information security protection," *Inf. Process. Manag.*, vol. 59, no. 1, pp. 1–14, 2022, doi: 10.1016/j.ipm.2021.102744.

[9] Sahiruddin, I. Riadi, and Sunardi, "Analisis Forensik Recovery Dengan Keamanan," no. 12.

[10] P. Kuppusamy, "Systematic Literature Review of Information Security Compliance Behaviour Theories," *Journal of Physics: Conference Series*, vol. 1551, no. 1. 2020, doi: 10.1088/1742-6596/1551/1/012005.

[11] C. Candiwan, M. Azmi, and A. Alamsyah, "Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era," *Int. J. Saf. Secur. Eng.*, vol. 12, no. 2, pp. 229–237, 2022, doi: 10.18280/ijsse.120212.

[12] M. Dupuis, A. Jennings, and K. Renaud, *Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password Hygiene*, vol. 1, no. 1. Association for Computing Machinery, 2021.

[13] P. Salsabila, "Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi," 2020. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi (accessed Dec. 10, 2020).

[14] Candiwan, P. K. Sari, and N. Nurshabrina, "Assessment of information security management on Indonesian higher education institutions," *Lect. Notes Electr. Eng.*, vol. 362, no. 2016-01–01, pp. 375–385, 2016, doi: 10.1007/978-3-319-24584-3_31.

[15] M. Butler and R. Butler, "The influence of mobile operating systems on user security behavior," *2021 IEEE 5th Int. Conf. Cryptogr. Secur. Privacy, CSP 2021*, pp. 134–138, 2021, doi: 10.1109/CSP51677.2021.9357568.

[16] T. Ramakrishnan, D. M. Hite, J. H. Schuessler, and V. Prybutok, "Work ethic and information security behavior," *Inf. Comput. Secur.*, vol. 30, no. 3, pp. 364–381, 2022, doi: 10.1108/ICS-02-2021-0017.

[17] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt, "A survey on smartphone user's security choices, awareness and education," *Comput. Secur.*, vol. 88, p. 101647, 2020, doi: 10.1016/j.cose.2019.101647.

[18] S. Yoo, H. R. Ryu, H. Yeon, T. Kwon, and Y. Jang, "Visual analytics and visualization for android security risk," *J. Comput. Lang.*, vol. 53, no. December 2018, pp. 9–21, 2019, doi: 10.1016/j.cola.2019.03.004.

[19] Y. Gangire, A. Da Veiga, and M. Herselman, "Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory," *IFIP Adv. Inf. Commun. Technol.*, vol. 593 IFIPAI, pp. 144–157, 2020, doi: 10.1007/978-3-030-57404-8_12.

[20] P. Shah and A. Agarwal, "Cybersecurity behaviour of smartphone users in India: an empirical analysis," *Inf. Comput. Secur.*, vol. 28, no. 2, pp. 293–318, 2020, doi: 10.1108/ICS-04-2019-0041.

[21] V. R. Saraswathi, I. S. Ahmed, S. M. Reddy, S. Akshay, V. M. Reddy, and S. M. Reddy, "Automation of Recon Process for Ethical Hackers," *2022 Int. Conf. Adv. Technol. ICONAT 2022*, no. February, 2022, doi: 10.1109/ICONAT53423.2022.9726077.

[22] X. J. Zhang, Z. Li, and H. Deng, "Information security behaviors of smartphone users in China: An empirical analysis," *Electron. Libr.*, vol. 35, no. 6, pp. 1177–1190, 2017, doi: 10.1108/EL-09-2016-0183.

[23] M. Park, O. Yi, and J. Kim, "A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301026, 2020, doi: 10.1016/j.fsidi.2020.301026.

[24] T. Mi, M. Gou, G. Zhou, Y. Gan, and R. Schwarzer, "Effects of planning and action control on smartphone security behavior," *Comput. Secur.*, vol. 97, p. 101954, 2020, doi: 10.1016/j.cose.2020.101954.

[25] E. Anggraeni and A. Alarifi, *Pengantar Sistem Informasi*. Yogyakarta: Penerbit Andi, 2017.

[26] P. Asadi, S. Ahmadi, A. Abdi, O. H. Shareef, T. Mohamadyari, and J. Miri, "Relationship between self-care behaviors and quality of life in patients with heart failure," *Heliyon*, vol. 5, no. 9, p. e02493, 2019, doi: 10.1016/j.heliyon.2019.e02493.

[27] M. Mirtsch, K. Blind, C. Koch, and G. Dudek, "Information security management in ICT and non-ICT sector companies: A preventive innovation perspective," *Comput. Secur.*, vol. 109, p. 102383, 2021, doi: 10.1016/j.cose.2021.102383.

[28] S. Nowrin and D. Bawden, "Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh," *Inf. Learn. Sci.*, vol. 119, no. 7–8, pp. 444–455, 2018, doi: 10.1108/ILS-04-2018-0029.

[29] Y. T. Chen, W. L. Shih, C. H. Lee, P. L. Wu, and C. Y. Tsai, "Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan," *Comput. Educ.*, vol. 164, no. 70, p. 104131, 2021, doi: 10.1016/j.compedu.2021.104131.

[30] S. T. Alanazi, M. Anbar, S. A. Ebad, S. Karuppayah, and H. A. Al-Ani, "Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector," *Symmetry (Basel).*, vol. 12, no. 9, pp. 1–21, 2020, doi: 10.3390/SYM12091544.

[31] T. Rachminingrum and P. K. Sari, "Analisis perilaku keamanan informasi pada pengguna android mobile apps di indonesia," vol. 6, no. 78, pp. 2135–2142, 2019, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/management/article/view/9556.

[32] I. B. Letica, "Some correlates of risky user behavior and ICT security awareness of secondary school students," *Int. J. Electr. Comput. Eng. Syst.*, vol. 10, no. 2, pp. 85–89, 2019, doi: 10.32985/ijeces.10.2.4.

[33] M. Alsaleh, N. Alomar, and A. Alarifi, *Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods*, vol. 12, no. 3. 2017.

[34] Z. Xu and K. Guo, "It ain't my business: a coping perspective on employee effortful security behavior," *J. Enterp. Inf. Manag.*, vol. 32, no. 5, pp. 824–842, 2019, doi: 10.1108/JEIM-10-2018-0229.

[35] N. Ameen, A. Tarhini, M. Hussain Shah, and N. O. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study," *Comput. Human Behav.*, vol. 104, p. 106184, 2020, doi: 10.1016/j.chb.2019.106184.

[36] I. Arend, A. Shabtai, T. Idan, R. Keinan, and Y. Bereby-Meyer, "Passive- and not active-risk tendencies predict cyber security behavior," *Comput. Secur.*, vol. 97, p. 101964, 2020, doi: 10.1016/j.cose.2020.101964.

[37] P. R. Shah and A. Agarwal, "Cybersecurity Behaviour of Smartphone Users Through the Lens of Fogg Behaviour Model," *2020 3rd Int. Conf. Commun. Syst. Comput. IT Appl. CSCITA 2020 - Proc.*, pp. 79–82, 2020, doi: 10.1109/CSCITA47329.2020.9137773.

[38] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance," *Appl. Sci.*, vol. 11, no. 8, 2021, doi: 10.3390/app11083383.

[39] L. Hadlington, M. Popovac, H. Janicke, I. Yevseyeva, and K. Jones, "Exploring the role of work identity and work locus of control in information security awareness," *Comput. Secur.*, vol. 81, pp. 41–48, 2019, doi: 10.1016/j.cose.2018.10.006.

[40] A. M. Y. Chu and M. K. So, "Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective," *Sustain.*, vol. 12, no. 8, pp. 1–25, 2020, doi: 10.3390/SU12083163.

[41] T. Velki and K. Romstein, "User risky behavior and security awareness through lifespan," *Int. J. Electr. Comput. Eng. Syst.*, vol. 9, no. 2, pp. 53–60, 2018, doi: 10.32985/ijeces.9.2.2.

[42] R. T. Adebiyi, O. Babalola, G. Amuda-Yusuf, S. A. Rasheed, and T. O. Olowa, "Effect of knowledge and compliance of health and safety information on construction sites workers' safety in Nigeria," *Int. J. Saf. Secur. Eng.*, vol. 10, no. 2, pp. 269–277, 2020, doi: 10.18280/ijsse.100215.

[43] C. Y. Sang and S. G. Liao, "Modeling and simulation of information dissemination model considering user's awareness behavior in mobile

social networks," *Phys. A Stat. Mech. its Appl.*, vol. 537, p. 122639, 2020, doi: 10.1016/j.physa.2019.122639.

[44] S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telemat. Informatics*, vol. 41, no. February 2019, pp. 55–69, 2019, doi: 10.1016/j.tele.2019.03.003.

[45] S. Bax, T. McGill, and V. Hobbs, "Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs," *Comput. Secur.*, vol. 106, p. 102278, 2021, doi: 10.1016/j.cose.2021.102278.

[46] N. H. Chowdhury, M. T. P. Adam, and T. Teubner, "Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures," *Comput. Secur.*, vol. 97, p. 101963, 2020, doi: 10.1016/j.cose.2020.101963.

[47] M. J. Girsang, Candiwan, R. Hendayani, and Y. Ganesan, "Can Information Security, Privacy and Satisfaction Influence the E-Commerce Consumer Trust?," *2020 8th Int. Conf. Inf. Commun. Technol. ICoICT 2020*, 2020, doi: 10.1109/ICoICT49345.2020.9166247.

[48] K. C. Chung, C. H. Chen, H. H. Tsai, and Y. H. Chuang, "Social media privacy management strategies: A SEM analysis of user privacy behaviors," *Comput. Commun.*, vol. 174, no. April, pp. 122–130, 2021, doi: 10.1016/j.comcom.2021.04.012.

[49] M. Hatamian, J. Serna, and K. Rannenberg, "Revealing the unrevealed: Mining smartphone users privacy perception on app markets," *Comput. Secur.*, vol. 83, no. 675730, pp. 332–353, 2019, doi: 10.1016/j.cose.2019.02.010.

[50] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, 2020, doi: 10.1080/08874417.2020.1712269.

[51] F. Nasirpouri Shadbad and D. Biros, "Technostress and its influence on employee information security policy compliance," *Inf. Technol. People*, vol. 35, no. 1, pp. 119–141, 2022, doi: 10.1108/ITP-09-2020-0610.

[52] A. Asfoor, F. A. Rahim, and S. Yussof, *Factors influencing information security awareness of phishing attacks from bank customers' perspective: A preliminary investigation*, vol. 843. Springer International Publishing, 2019.

[53] M. Sas, G. L. L. Reniers, W. Hardyns, and K. Ponnet, "The impact of training sessions on security awareness: Measuring the security knowledge, attitude and behaviour of employees," *Chem. Eng. Trans.*, vol. 77, pp. 895–900, 2019, doi: 10.3303/CET1977150.

[54] Z. Tang, A. S. Miller, Z. Zhou, and M. Warkentin, "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations," *Gov. Inf. Q.*, vol. 38, no. 2, p. 101572, 2021, doi: 10.1016/j.giq.2021.101572.

[55] Kautsarina, A. N. Hidayanto, B. Anggorojati, Z. Abidin, and K. Phusavat, "Data modeling positive security behavior implementation among smart device users in Indonesia: A partial least squares structural equation modeling approach (PLS-SEM)," *Data Br.*, vol. 30, p. 105588, 2020, doi: 10.1016/j.dib.2020.105588.

[56] K. van der Schyff and S. Flowerday, "Mediating effects of information security awareness," *Comput. Secur.*, vol. 106, p. 102313, 2021, doi: 10.1016/j.cose.2021.102313.

[57] G. Norman and D. Streiner, *Biostatistics : The Bare Essentials*. Shelton: B.C. Decker, 2008.

[58] R. A. Armstrong, "When to use the Bonferroni correction," *Ophthalmic Physiol. Opt.*, vol. 34, no. 5, pp. 502–508, 2014, doi: 10.1111/opo.12131.

[59] Y. Koumpouros, "Major Metrics, Concerns, and Assessment Strategy for Mobility Assistive Divices," in *Research Anthology on Supporting Healthy Aging in a Digital Society*, I. R. M. Association, Ed. IGI Global, 2022, p. 733.

[60] B. S. Everite and C. R. Palmer, *Encyclopaedic Companion to Medical Statistics*. United Kingdom, 2011.