Walisongo Journal of Information Technology, Vol. 5 No. 2 (2023): 103-128
DOI: https://doi.org/10.21580/wjit.2023.5.2.17334

Information Security Awareness Analysis on Digital Bank Customer Using Analytic Hierarchy Process: Case Study at XYZ Application from Bank ABC

Kemas Khaidar Ali Indrakusuma[1,*], **Achmad Nizar Hidayanto**[1]

[1]Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia
*Corresponding author: kemask69@gmail.com

Abstract

Digital banking is an innovation from banks to deal with the high demand of the retail customer. This study aims to analyse and measure the level of information security awareness of the customers of XYZ as one of the digital banks in Indonesia and provide recommendations for steps that need to be taken to reduce fraud cases caused by customer negligence. Focus areas that included in this research are the adaptation and extension of the HAIS-Q framework and becoming a new theoretical framework to measure information security awareness for end-user. The measurement is carried out by distributing questionnaires with five Likert scales to 385 respondents and then processed using the Analytic Hierarchy Process (AHP) method which involves eight experts measuring the weight of several identified focus areas and then classified using the Kruger scale. The information security awareness measurement has a result of 81,9770 which indicates that the information security awareness of XYZ users has a good level. The results of data processing show that there are two focus areas and ten focus sub-area that is still not in the good category. In addition, several recommendations are given to XYZ so that the focus areas and sub-areas that are not categorized as good can be improved to make sure the information security awareness of XYZ users becomes better.

Keywords: Analytic hierarchy process, Digital bank, Information security awareness

1 Introduction

Threats to information security will always exist regardless of any countermeasures, but preventive measures can minimize the possibility of the realization of these threats (Whitman and Mattord, 2021). Threats to information security can come from technological aspects as well as human factors (Hassandoust et al., 2022). A report from the IBM Cyber Security

Intelligence Index states that almost 95% of security incidents are caused by human factors, which shows that human factors are critical element to information security (Desolda et al., 2022). Many security and warning tools are provided as solutions to information security threats, but the end-user side is often poorly understood and explored (Das et al., 2022). Every company needs to change its policies and regulations to create guidance on information security awareness for end users to increase user knowledge about information security (Abulhaija et al., 2022), due to lack of knowledge is one of the human factors that can make users vulnerable to threats to information security (Desolda et al., 2022).

The user is the weakest point in fraud crimes (Syafitri et al., 2022) that can be easily influenced and persuaded to provide confidential data to perpetrators of fraud by using human psychology (Ali and Mohd Zaharon, 2024). By examining users' information security awareness, it can be analyzed the tendency of XYZ users to avoid fraud cases that harm customers and banks.

The most common framework to measure information security awareness is the Human Aspects of Information Security Questionnaire (HAIS-Q) (Mahardika et al., 2020). But primarily HAIS-Q is intended to measure employees' information security awareness. There is also Cybersecurity Awareness and Training (CAT) Framework that is developed for remote working employees (Hijji and Alam, 2022). Furthermore, there is no current framework to measure end-user information security awareness. This research intends to build a framework to measure end-user information security framework.

To reach the technology-savvy retail customer segment, Bank ABC launched a service in the retail banking segment which is its digital innovation called XYZ in 2016 (*Bank XYZ Report*, 2021). XYZ is a digital bank that helps customers manage life finance, namely the bond between life and finances. XYZ as a pioneer of digital banking in Indonesia has a growing number of customers every year (Kamar, n.d.). In addition to the number of customers which increases every year, XYZ also has the highest number of active customers per month in 2021 for the digital bank category in Indonesia (Pahlevi, 2022) which makes the majority of Indonesia's digital bank customers using XYZ. This makes research with the subject of XYZ users able to describe the majority of digital bank customers in Indonesia. With more and more customers, the volume and number of transactions at XYZ are also increasing.

In Indonesia, fraud cases are one of the most common cybercrime cases. In the period 2020-2021, there has been an increase in fraud cases reported to the police (Annur, 2020). The rise of fraud cases that have occurred in Indonesia has had an impact on fraud cases in the digital bank sector. Fraud cases in the digital bank sector have increased in percentage terms from the second quarter of 2020 to the first quarter of 2021 (AppsFlyer, n.d.). Digital-based transactions that are getting easier at XYZ are increasing every year accompanied by an increase in cybercrime cases so digital fraud cases are also increasingly prevalent (Chang et al., 2022). With that said, this research will explore the information security awareness of digital bank users in Indonesia.

Fraud cases cause financial losses

for affected customers. Apart from customers, cases of fraud can cause several negative impacts on the bank, such as disclosure of confidential information that should be protected such as intellectual property, competitive advantage, and customer data, the risk of declining bank reputation, operational losses, direct financial losses, even financial extortion with ransom money (Ohrimenco et al., 2021). Because of these impacts, banks certainly do not want fraud cases to occur to their customers and these financial and non-financial loss are of particular concern for the bank to deal with (Abidin et al., 2019).

From the bank's internal data, there are around 50 reports per day regarding indications of fraud that need to be handled by the bank so the potential for fraud is still very high in XYZ (*Bank XYZ Report*, 2021). Massive sharing of data via social networks regardless of data privatization by customers can also expose customers to privacy threats [18]. The three most common consequences of fraud cases in the form of identity fraud are identity theft, account takeover, and application submission fraud (Soomro et al., 2019).

There are two research questions in this study, namely:

1. "What level of information security awareness do XYZ users have?"
2. "What are the efforts that can be made by Bank ABC to reduce the number of fraud cases caused by customer negligence that occur in its digital bank services, namely XYZ?"

2 Literature Review

The following is an explanation of some of the theoretical foundations that are used as a reference in this study.

2.1 Digital Bank

A digital bank is a form of digitization of bank services that uses technology and innovation to personalize customers' individual needs and can provide easy, smooth, and transparent services to consumers (Ghani et al., 2022). The existence of a digital bank can increase the accessibility of banking services to a larger population, especially in developing countries like Indonesia, so that it can significantly improve a country's economy (Ozili, 2018).

2.2 Fraud

Fraud is an intentional act by a person or several people among managers, employees, or third parties, by deceiving to gain unjustified or illegal benefits (Utami et al., 2020). David Cressey developed the concept of the fraud triangle which explains the factors that cause someone to commit fraud, namely pressure, opportunities, and rationalization (Tickner and Button, 2021). In its development, the theory developed with the addition of a new factor, namely capability, which made the fraud triangle theory evolve into the fraud diamond (Ozcelik, 2020).

2.3 Information Security Awareness

Information security awareness can be defined as an assessment of a person's understanding, commitment, and behavior by applicable information security policies, guidelines, and rules (Kruger and Kearney, 2006). By having good information security awareness, one can act in a good way and implement best practices to maintain security, safety, and privacy (Salem et al., 2021). Thus, increasing information security awareness is one of the most effective ways of maintaining information security (McIlwraith, 2022) and also educating the consequences if a security breach occurs (Prakoso et al., 2020). There are three methods of assessing information security awareness of users, namely questionnaires, passive measurements, and attack simulations (Solomon et al., 2022).

2.4 Human Aspects of Information Security Questionnaire

Human Aspects of Information Security Questionnaire (HAIS-Q) is a survey preparation technique used to measure information security awareness in the dimensions of knowledge, attitude, and behavior called the KAB model (Wiley et al., 2020). The KAB model itself can be a benchmark for a company to solve various problems (Mahardika et al., 2020) which has its weighting for each dimension used by Kruger (Kruger and Kearney, 2006), with Knowledge having a weight of 30%, Attitude having a weight of 20%, and Behavior having a weight of 50%. HAIS-Q has seven focus areas, namely password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting (Mahardika et al., 2020). Each focus area has its focus subareas.

2.5 Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) is a multi-criteria decision-making (MCDM) model (Asadabadi et al., 2019) which uses human subjects who are experts in their fields to make a decision and can be used for both qualitative and qualitative research (Mahardika et al., 2020). AHP was originally developed to make effective decisions on complex problems so that the problem is simplified and speeds up the decision-making process (Liu et al., 2020). With AHP, complex problems are converted into a hierarchy based on the complexity of the problem where the highest level is the goal to be achieved followed by the criteria levels (Orji et al., 2020).

3 Theoretical Framework

In determining the theoretical framework of user information security awareness in digital bank, a systematic literature review is carried out so that the literature can be reviewed in a systematic, explicit, and comprehensive manner to identify, evaluate, and make a synthesis of previous research (Okoli and Schabram, 2010). The methodology developed by Okoli and Schabram supports qualitative and quantitative research in the field of information systems (Ifenthaler and Yau, 2020). Obtained five related literature that comes from IEEEXplore (3 pieces of literature) and LONTAR (Universitas Indonesia's database with two pieces of literature), namely:

- L1: Measurement of Information Security Awareness Level: A Case

Study of Mobile Banking (M-Banking) Users (Firsty Arisya et al., 2020), from IEEEXplore

- L2: Measurement of Information Security Awareness Level: A Case Study of Online Transportation Users (Prakoso et al., 2020), from IEEEXplore
- L3: Evaluation of Information Security Awareness among Palestinian Learners (Salem et al., 2021), from IEEEXplore
- L4: Analysis of Information Security Awareness Level in Credit Card Customers Using Multiple Criteria Decision Analysis (MCDA): Case Study of Bank XYZ (Fariz, 2020), from LONTAR
- L5: Analysis of Factors Influencing Information Security Awareness and Educational Recommendations for E-Wallet Users in Indonesia (Akbar, 2021), from LONTAR

From previous research, a 3C + 2S analysis was carried out to select focus areas and instruments to be used in this study. The 3C+2S analysis describes all previous research into five parts, namely compare, contrast, criticize, synthesize, and summarize. This analysis aims to ensure the relevance of previous research with the research that the author will conduct. Nine focus areas were identified and used in this study which can be seen in Figure 1.

The identified focus areas are validated and explored by Bank ABC's internal IT team that deals directly with XYZ. The result of this process is the theoretical framework that can be seen in Figure 1. The elaboration of the framework can be seen in Table 1.

4 Methods

Firstly, a theoretical framework for this research was constructed by using a systematic literature review. The result can be seen in Figure 1. After the framework was constructed, it needs to be weighed for each focus area and sub-focus area. The weighing process utilized AHP with constructing the AHP questionnaire. The AHP questionnaire aims to weigh each focus area and sub-focus area using 9 scales and involving 8 experts. An expert is defined as someone who has comprehensive knowledge in a particular field that is not shared by many people (Volkmar et al., 2022). Thus, the experts assigned to this research are practitioners who develop XYZ directly for more than a year so they have in-depth knowledge of XYZ.

The next process is getting the value for each focus area and sub-focus area using the Likert questionnaire. For the Likert questionnaire, there are 72 questions, consisting of 36 positive questions and 36 negative questions that has been gone through validity and readability testing. The questions can be seen in Appendix 1. The use of positive questions and negative questions is intended to avoid biased responses that can reduce the validity of the research (Suárez-Álvarez et al., 2018). Answers from respondents were measured by a Likert scale which has five values. The scale can be seen in Table 2.

Table 2. Likert Scale

Indicator	Strongly disagree	Dis-agree	Neutral	Agree	Strongly Agree
Positive question	1	2	3	4	5
Negative question	5	4	3	2	1

This Likert questionnaire involved

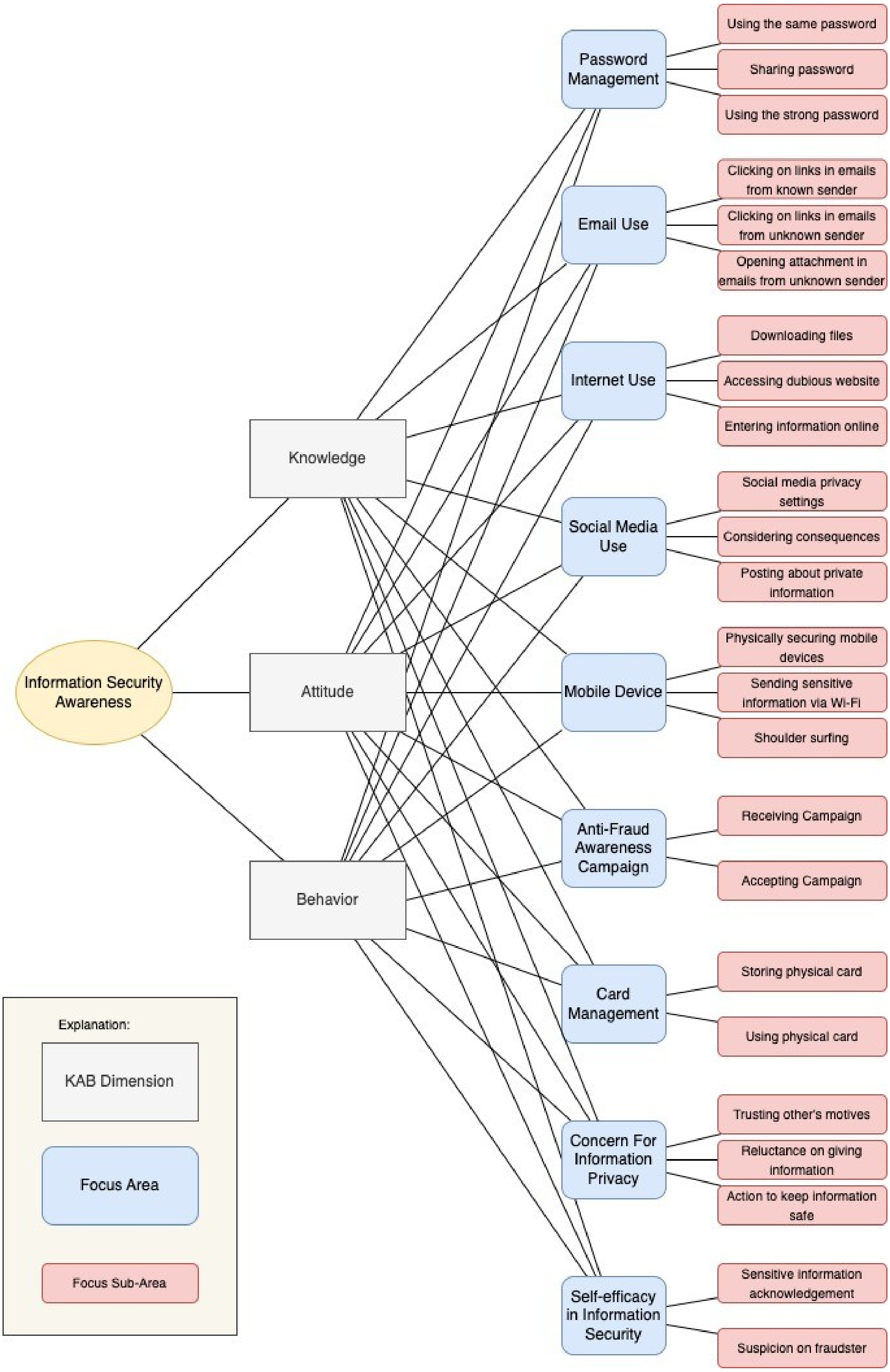
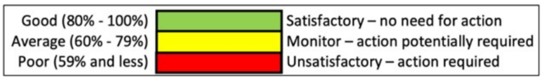

Information Security Awareness
Knowledge
Attitude
Behavior
Password Management
Using the same password
Sharing password
Using the strong password
Email Use
Clicking on links in emails from known sender
Clicking on links in emails from unknown sender
Opening attachment in emails from unknown sender
Internet Use
Downloading files
Accessing dubious website
Entering information online
Social Media Use
Social media privacy settings
Considering consequences
Posting about private information
Mobile Device
Physically securing mobile devices
Sending sensitive information via Wi-Fi
Shoulder surfing
Anti-Fraud Awareness Campaign
Receiving Campaign
Accepting Campaign
Card Management
Storing physical card
Using physical card
Concern For Information Privacy
Trusting other's motives
Reluctance on giving information
Action to keep information safe
Self-efficacy in Information Security
Sensitive information acknowledgement
Suspicion on fraudster
Explanation:
KAB Dimension
Focus Area
Focus Sub-Area

Figure 1. Theoretical Framework.

Table 1. Theoretical Framework Elaboration

Focus Area	Focus Sub-Area	Justification	References
Password Management (PM)	*Using the same password* (PM1)	If the password is known by other people, then the risk of being misused and fraudulent actions will arise is very large	L1, L2, L3, L4, L5
	Sharing password (PM2)		
	Using the strong password (PM3)		
Email Use (EU)	*Clicking on links in emails from known sender* (EU1)	Email can be used by fraudsters to retrieve sensitive data from users who are not careful in their use	L1, L2, L3, L4
	Clicking on links in emails from unknown sender (EU2)		
	Opening attachment in emails from unknown sender (EU3)		
Internet Use (IU)	*Downloading files* (IU1)	Fraud perpetrators can create fake web links that can trap unscrupulous users to provide sensitive data about their accounts and misuse them	L1, L2, L4
	Accessing dubious website (IU2)		
	Entering information online (IU3)		
Social Media Use (SM)	*Social media privacy settings* (SM1)	Users who are not careful can spread sensitive data on their social media and risk being misused by irresponsible people	L1, L2, L3, L4
	Considering consequences (SM2)		
	Posting about private information (SM3)		
Mobile Device (MD)	*Physically securing mobile devices* (MD1)	Careless use of mobile devices and network usage can make user's account sensitive information retrieved by other people who can access it other than the user himself and vulnerable to be misused	L1, L2, L3, L4
	Sending sensitive information via Wi-Fi (MD2)		
	Shoulder surfing (MD3)		
Anti-Fraud Awareness Campaign (AF)	*Receiving campaign* (AF1)	Bank's explanation regarding the prevention of fraud cases is very important to be known and accepted in order to increase the information security awareness of its users	L4
	Accepting campaign (AF2)		
Card Management (CM)	*Storing physical card* (CM1)	On a physical card, there is some sensitive information that needs to be kept confidential by the user and storage and usage must be observed	L4
	Using physical card (CM2)		
Concern for Information Privacy (CI)	*Trusting other's motives* (CI1)	Users' awareness of the use of sensitive account information by other parties is important for user's information security awareness	L5
	Reluctance on giving information (CI2)		
	Action to keep information safe (CI3)		
Self-efficacy in Information Security (SI)	*Sensitive information acknowledgement* (SI1)	Sensitive information on a user's account will be safe if the user has good personal skills in protecting that information	L5
	Suspicion on fraudster (SI2)		

385 respondents. The data obtained from the Likert questionnaire will be calculated for reliability by calculating the Cronbach Alpha value with SPSS. After the reliability test, the data will be processed for each focus area to get a percentage. The processing results will be classified using the Kruger Scale (Kruger and Kearney, 2006) which can be seen in Figure 2.



Good (80% - 100%)	🟩	Satisfactory – no need for action
Average (60% - 79%)	🟨	Monitor – action potentially required
Poor (59% and less)	🟥	Unsatisfactory – action required

Figure 2. Kruger Scale

The results of this classification determine the level of information security awareness of XYZ users in related focus areas. From this classification, it can be identified focus areas that have deficiencies in XYZ users' information security awareness that recommendations can be made to improve these focus areas by adding several theories that support the literature. After the classification of all focus areas is completed, a thorough classification is carried out for XYZ users' information security awareness using the focus area weighting obtained with AHP. The final step was to conduct follow-up interviews with three stakeholders at Bank ABC to discuss acceptance of the recommendations from the research.

5 Result and Discussion

Table 3 shows the final weighting results from pairwise comparison questionnaireusing AHP. Furthermore, the processing of the Likert questionnaire was carried out. Furthermore, the processing of the Likert questionnaire was carried out. The demography of the valid respondents with the total count of 385 can be seen in Figure 3.

For the 385 respondents selected, the Cronbach Alpha value is 0.831 according to calculations with SPSS which indicates the results of this study have very good reliability and are acceptable. For each question item, the total point value (TPV) of all selected respondents is calculated and then divided by the maximum possible TPV to get the percentage value of the question items. This percentage value will be used for data analysis.

For the analysis of focus sub-areas, the percentage value of each research focus sub-area will be sought. The method is to map the percentage of each question from the relevant sub-area with the weight of the information security awareness dimensions. With this mapping, the percentage value P of the focus sub-area can be calculated in this way:

$$P = \frac{30K + 20A + 50B}{100} \tag{1}$$

where K is the percentage value of the knowledge dimension question items, A is the attitude dimension question item percentage value, and B is the behavior dimension question item percentage value. Each percentage value can be classified with the Kruger scale.

After analyzing the sub-areas of focus, then an analysis of the research focus areas is carried out. From this analysis, the percentage value of the research focus area will be generated as also the classification of information security awareness with the Kruger scale. The percentage value of the focus area can be calculated by accumulating the percentage value of the focus area related to the focus area multiplied by the weight of the focus area. The percentage values of focus areas and sub-areas of research focus can be seen in Table 4.

After the percentage value of each focus area is obtained, the percentage value of information security awareness of XYZ users can be calculated by accumulating the multiplication of the percentage value of the focus area with the weight of the focus area. As a result, XYZ users' information security awareness value is 81.9770. With the Kruger scale, this value can be classified as good. Thus, XYZ users' information security awareness is in a good category.

Table 3. AHP Processing Result

Focus Area	Focus Area Weight	Focus Sub-Area	Focus Sub-Area Weight
Password Management (PM)	10,19 %	*Using the same password* (PM1)	17,75 %
		Sharing password (PM2)	46,06 %
		Using the strong password (PM3)	36,19 %
Email Use (EU)	5,61 %	*Clicking on links in emails from known sender* (EU1)	19,44 %
		Clicking on links in emails from unknown sender (EU2)	35,89 %
		Opening attachment in emails from unknown sender (EU3)	44,67 %
Internet Use (IU)	8,38 %	*Downloading files* (IU1)	13,84 %
		Accessing dubious website (IU2)	26,44 %
		Entering information online (IU3)	59,72 %
Social Media Use (SM)	9,44 %	*Social media privacy settings* (SM1)	36,36 %
		Considering consequences (SM2)	26,90 %
		Posting about private information (SM3)	36,73 %
Mobile Device (MD)	8,19 %	*Physically securing mobile devices* (MD1)	39,73 %
		Sending sensitive information via Wi-Fi (MD2)	28,88 %
		Shoulder surfing (MD3)	31,39 %
Anti-Fraud Awareness Campaign (AF)	10,37 %	*Receiving campaign* (AF1)	44,01 %
		Accepting campaign (AF2)	55,99 %
Card Management (CM)	10,10 %	*Storing physical card* (CM1)	59,45 %
		Using physical card (CM2)	40,55 %
Concern for Information Privacy (CI)	18,34 %	*Trusting other's motives* (CI1)	11,99 %
		Reluctance on giving information (CI2)	26,51 %
		Action to keep information safe (CI3)	61,50 %
Self-efficacy in Information Security (SI)	19,38 %	*Sensitive information acknowledgement* (SI1)	58,53 %
		Suspicion on fraudster (SI2)	41,47 %

Ten focus sub-areas have a category of information security that is not yet good, which come from six focus areas, and two focus areas that have a category of information security that is not good. To determine the priority of recommendations, the focus area and sub-focus areas are ranked which

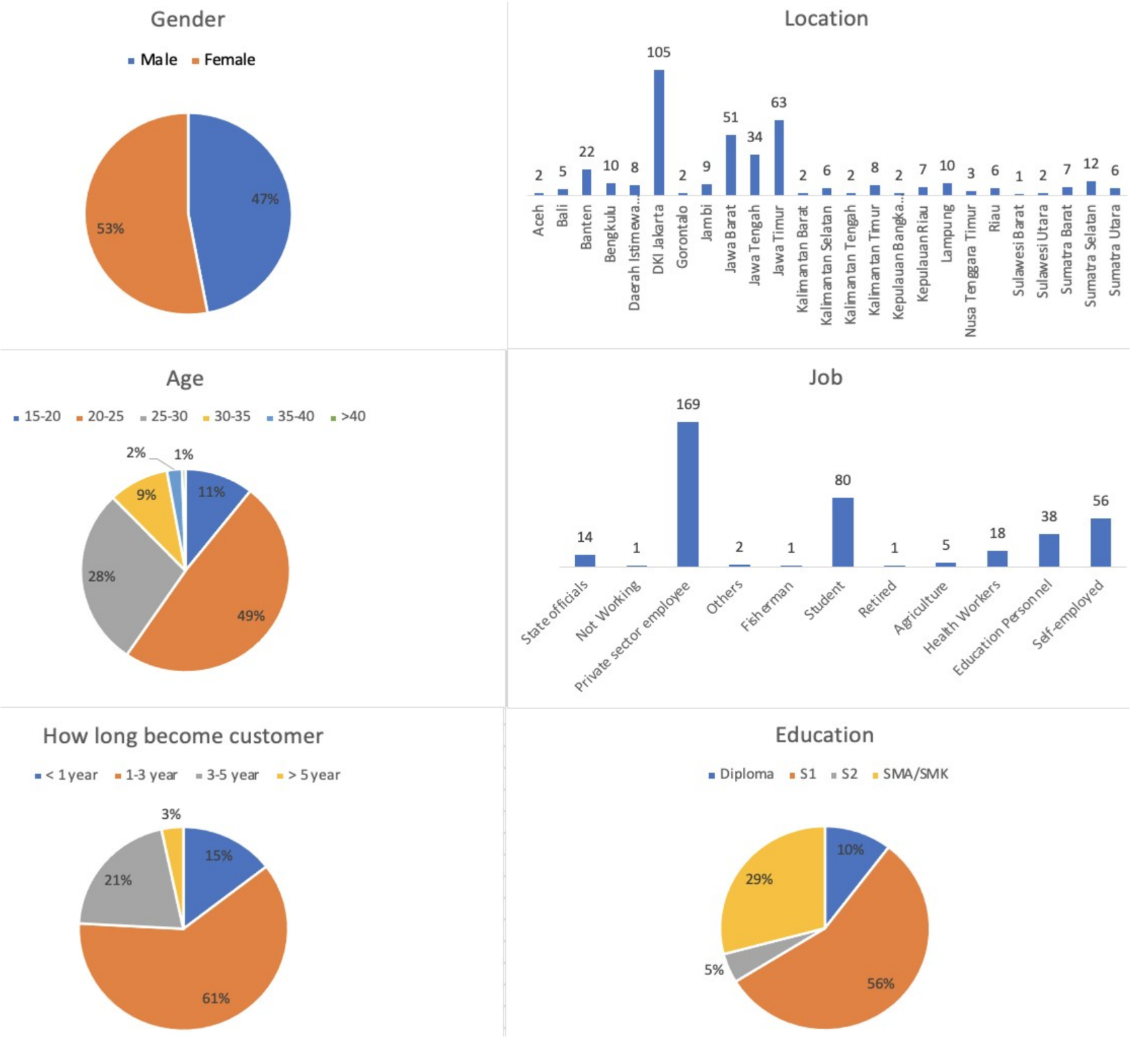


Figure 3. Respondents Demography

have a not good category based on the percentage value of information security awareness.

A worse percentage value indicates a greater urgency for improvement in the focus areas and focus sub-areas. The sub-areas of focus along with the focus areas that have been ranked can be seen in Table 5.

The following is a discussion of focus areas and focus sub-areas that do not have good information security awareness.

5.1 Internet Use

In the internet use focus area, the focus sub-area which has a moderate category is downloading files and entering information online. This indicates that there is a vulnerability in the information security of XYZ users in using the internet in the aspects of the two sub-areas mentioned.

The number of files on the internet continues to increase every day and there is no guarantee that all files are safe and virus-free because virus can be embedded in the file or program (Matveev et al., 2021). If the user downloads a file that contains a virus

Table 4. Processing Results of Focus Areas and Sub-Areas of Research Focus

Focus Area	Percentage	Focus Sub-Area	Percentage
Password Management (PM)	81,8282	*Using the same password* (PM1)	65,2883
		Sharing password (PM2)	84,4468
		Using the strong password (PM3)	86,6078
Email Use (EU)	78,6707	*Clicking on links in emails from known sender* (EU1)	79,4026
		Clicking on links in emails from unknown sender (EU2)	79,4130
		Opening attachment in emails from unknown sender (EU3)	77,7558
Internet Use (IU)	77,2575	*Downloading files* (IU1)	66,4104
		Accessing dubious website (IU2)	81,6571
		Entering information online (IU3)	77,8234
Social Media Use (SM)	80,1255	*Social media privacy settings* (SM1)	84,8364
		Considering consequences (SM2)	79,0805
		Posting about private information (SM3)	76,2494
Mobile Device (MD)	81,5671	*Physically securing mobile devices* (MD1)	85,5429
		Sending sensitive information via Wi-Fi (MD2)	68,5299
		Shoulder surfing (MD3)	88,5299
Anti-Fraud Awareness Campaign (AF)	83,7069	*Receiving campaign* (AF1)	84,1403
		Accepting campaign (AF2)	83,3662
Card Management (CM)	83,7181	*Storing physical card* (CM1)	86,4987
		Using physical card (CM2)	79,6416
Concern for Information Privacy (CI)	84,2425	*Trusting other's motives* (CI1)	81,0701
		Reluctance on giving information (CI2)	86,0935
		Action to keep information safe (CI3)	84,0675
Self-efficacy in Information Security (SI)	82,1485	*Sensitive information acknowledgement* (SI1)	83,1481
		Suspicion on fraudster (SI2)	80,7377

or other malware (harmful content), the user's device can be infected and there is a possible threat of loss or theft of user data, including user XYZ account data (Wang, 2022).

Users can also spread confidential XYZ account information unknowingly if they are not careful in filling in this information on fake websites created by fraudsters, which allows misuse of users' XYZ accounts by irresponsible parties (Kelley et al., 2023).

Table 5. Priority Areas and Focus Sub-Areas that Are Not in Good Category

Focus Area	Percentage	Focus Sub-Area	Percentage
Internet Use (IU)	77,2575	*Downloading files* (IU1)	66,4104
		Entering information online (IU3)	77,8234
Email Use (EU)	78,6707	*Opening attachment in emails from unknown sender* (EU3)	77,7558
		Clicking on links in emails from known sender (EU1)	79,4026
		Clicking on links in emails from unknown sender (EU2)	79,4130
Social Media Use (SM)	80,1255	*Posting about private information* (SM3)	76,2494
		Considering consequences (SM2)	79,0805
Mobile Device (MD)	81,5671	*Sending sensitive information via Wi-Fi* (MD2)	68,5299
Password Management (PM)	81,8282	*Using the same password* (PM1)	65,2883
Card Management (CM)	83,7181	*Using physical card* (CM2)	79,6416

5.2 Email Use

In the email use focus area, the focus sub-areas that have a moderate category are clicking on links in emails from known senders, clicking on links in emails from unknown senders, and opening attachments in emails from unknown senders. This indicates that the information security awareness of XYZ users in this focus area has weaknesses in all its sub-areas. This focus area is concerned with how XYZ users use email or other communication media, especially in terms of clicking on links and downloading attachments in emails or other communication media.

The biggest threat in this focus area is the practice of email phishing, which are activity carried out by fraudsters by sending emails claiming false identities to obtain sensitive information from their victims (Jalali et al., 2020). In email phishing, the email can contain a link to an internet page that has been prepared by the fraudster or it can also attach a file that can endanger the device security of the user who downloads it (Jáñez-Martino et al., 2023).

There are also phishing threats in the form of text or known as smishing which is more personal so they can make the victim less alert (Mishra and Soni, 2020). If the user clicks on the link or downloads the attachment, information about the user's XYZ account becomes compromised (Baki and Verma, 2023).

5.3 Social Media Use

In the focus area of social media use, the focus sub-area which has a moderate category is considering the consequences and posting about private information. This indicates that XYZ users tend to think less about the consequences of sharing personal information on social media. Social media allows people to connect and exchange contents (Olanrewaju et al., 2020).

However, social media also has an impact on privacy because everyone can share any information, including personal information. If the information has been shared, then no one guarantees the security of the information that has been shared because the information or the user-generated data will become a digital footprint that can be seen by other people (Beigi and Liu, 2020). This is a threat to the security of the user's XYZ account because personal information that should not be shared may be taken by fraudsters to help them access the user's XYZ account.

5.4 Password Management

In the password management focus area, the focus sub-area that has a moderate category is using the same password. This indicates that XYZ users still tend to use the same password for XYZ accounts and various other applications on their devices. This can be a vulnerability because a password guesser can find out the password of a user's account (Murray and Malone, 2022). Even people who are known to the user have the possibility of knowing the password of an application belonging to user XYZ. If the application password is the same as the user's XYZ password, or user's application passwords are stored plainly in user records like notes, the security of the user's account will be threatened (Yıldırım and Mackie, 2019).

5.5 Mobile Device

In the mobile device focus area, the focus sub-area which has a moderate category is sending sensitive information via Wi-Fi. This indicates that not all XYZ users are aware of the dangers of accessing and sending sensitive information, including access to XYZ applications via public Wi-Fi networks.

Public Wi-Fi networks can be exploited by criminals by eavesdropping (knowing all activity that users do without the user knowing while using Wi-Fi), DNS hijacking, cryptojacking (the act of hijacking a computer to mine cryptocurrencies against the user's will), and deployment of malicious hotspots (Wi-Fi set up by fraudsters to retrieve information from connected devices) (Gao et al., 2021). IP spoofing (pretending to be someone else) and ARP poisoning (corrupt the ARP or Address Resolution Protocol to a local network) also can happen when using public Wi-Fi (Sinha et al., 2019).

5.6 Card Management

In the card management focus area, the focus sub-area which has a moderate category is using physical cards. The use of XYZ physical cards in transactions or the use of ATMs is a separate threat to the security of the user's XYZ account. Sensitive information printed on the user's physical card such as card number, card expiration date, and CVV has the possibility of being known by other people during transactions. If this information is known, then people who know this can use the user's XYZ account to make transactions, and eventually, fraud occurs (Ezennaya-Gomez et al., 2022). In addition, there is a possibility of skimming if the user's card still uses magnetic strip technology (Guers et al., 2022).

6 Conclusion

This study aims to measure the level of information security awareness of XYZ users so that appropriate actions can be determined to increase the information security awareness of XYZ users according to the areas of focus that need to be improved. This study has nine focus areas taken from several previous studies and validated by Bank ABC's internal IT team that deals directly with XYZ. The nine focus areas are password management, email use, internet use, social media use, mobile devices, social engineering, anti-fraud awareness campaign, PIN management, card management, concern for information privacy, user competency, and self-efficacy in information security. Each focus area has its sub-areas with a total of 24 research sub-areas. Knowledge, Attitude, and Behavior dimensions are also used to measure each sub-area.

After the focus areas were identified, focus area weighting was carried out involving 8 experts who were practitioners who had directly developed XYZ for more than a year to have in-depth knowledge about XYZ. To determine the level of information security awareness, 385 respondents were active XYZ users and filled out a questionnaire with 72 questions with five Likert scales. The data collected has a Cronbach Alpha value of 0.831 which indicates high reliability. The data is then classified using the Kruger scale to determine whether the measured object has a good, moderate, or poor level of information security awareness.

From the results of data collection, the value of information security awareness of XYZ users is 81.9770 which indicates that the level of information security awareness is at a good level. Furthermore, there are ten sub-areas out of six focus areas that have poor or moderate information security awareness classification and two focus areas whose information security awareness classification is not good or moderate. From each sub-area and research focus area that is not good enough, recommendations for efforts that can be made by the bank are given to increase the information security awareness of XYZ users as a whole and have been validated and accepted by the bank.

In the following, several suggestions can be made by Bank ABC to increase the information security awareness of XYZ users:

1. Creating education about information security awareness on the XYZ social media channel which does not yet have information security awareness educational content like TikTok.
2. Prioritize increasing awareness of information security in the focus areas of internet use and email use that have poor or moderate information security awareness classifications.
3. Provide education about virus threats and also check the validity of websites that users visit for internet use focus areas.
4. Provide education about the threat of email phishing and smishing and check the validity of email senders and links contained in emails for email use focus areas.
5. Encouraging XYZ users to be wise in using social media and monitoring trends that endanger the security of user information for social media use focus areas.
6. Provide education about the dangers of sending sensitive

information with public Wi-Fi, education about device permissions, and detect the network used by users when accessing XYZ for mobile device focus areas.

7. Provide education about using XYZ passwords that are different from other applications and storing and changing XYZ passwords regularly for password management focus areas.
8. Replacing the user's physical card with chip technology that has better security effectivity, removing sensitive information from the physical card, and educating on how to use the card properly and safely for card management focus areas.
9. Conduct research that aims to determine the level of education acceptance from XYZ towards its users.

For future works, these items are interesting to be studied for:

1. Create a framework for solving external fraud problems that has a list of lessons learned from resolving various fraud cases that have occurred. This is useful for providing appropriate steps in resolving future fraud cases. This can also help document the modus operandi of fraud cases that have never existed before because the modus operandi of fraud will always evolve along with technological developments.
2. Creating a framework to continuously measure user information security awareness. This can assist in monitoring the information security awareness of XYZ users and can also be aimed at helping maintain the information security awareness of its users at a good level. The focus areas in this research can be a good reference for the dimensions of the framework.
3. Exploring the critical success factors of campaign acceptance given related to information security awareness. This can help companies to create educational content about information security awareness that can be better received by their users.

Reference

Abidin, M. A. Z., Nawawi, A. and Salin, A. S. A. P. (2019), 'Customer data security and theft: a Malaysian organization's experience', *Information & Computer Security* **27**(1), 81–100. doi: 10.1108/ICS-04-2018-0043.
URL: *https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2018-0043/full/html*

Abulhaija, S., Hattab, S. and Qusef, A. (2022), Cyber Security Awareness, Knowledge and Behavior in the Banking Sector in Jordan, *in* '2022 13th International Conference on Information and Communication Systems (ICICS)', IEEE, pp. 48–53. doi: 10.1109/ICICS55353.2022.9811212.
URL: *https://ieeexplore.ieee.org/document/9811212/*

Akbar, M. (2021), Analisis faktor yang mempengaruhi kesadaran keamanan informasi dan rekomendasi edukasi pada pengguna e-wallet di Indonesia, Master thesis, Universitas Indonesia.

Ali, M. M. and Mohd Zaharon, N. F. (2024), 'Phishing—A Cyber Fraud: The Types, Implications and Governance', *International Journal of Educational Reform* **33**(1), 101–121. doi: 10.1177/10567879221082966.
URL: *http://journals.sagepub.com/doi/10.1177/10567879221082966*

Annur, C. M. (2020), 'Daftar Kejahatan Siber yang Paling Banyak Dilaporkan ke Polisi'.
URL: *https://databoks.katadata.co.id/datapublish/2020/09/08/daftar-kejahatan-siber-yang-paling-banyak-dilaporkan-ke-polisi*

AppsFlyer (n.d.), 'Mobile attribution & marketing analytics for Finance app marketers – the complete guide'.
URL: *https://www.appsflyer.com/resources/guides/finance-apps-mobile-attribution-analytics/*

Asadabadi, M. R., Chang, E. and Saberi, M. (2019), 'Are MCDM methods useful? A critical review of Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP)', *Cogent Engineering* **6**(1). doi: 10.1080/23311916.2019.1623153.
URL: *https://www.tandfonline.com/doi/full/10.1080/23311916.2019.1623153*

Baki, S. and Verma, R. M. (2023), 'Sixteen Years of Phishing User Studies: What Have We Learned?', *IEEE Transactions on Dependable and Secure Computing* **20**(2), 1200–1212. doi: 10.1109/TDSC.2022.3151103.
URL: *https://ieeexplore.ieee.org/document/9713733/*

Bank XYZ Report (2021), Technical report.

Beigi, G. and Liu, H. (2020), 'A Survey on Privacy in Social Media', *ACM/IMS Transactions on Data Science* **1**(1), 1–38. doi: 10.1145/3343038.
URL: *https://dl.acm.org/doi/10.1145/3343038*

Chang, V., Doan, L. M. T., Di Stefano, A., Sun, Z. and Fortino, G. (2022), 'Digital payment fraud detection methods in digital ages and Industry 4.0', *Computers and Electrical Engineering* **100**, 107734. doi: 10.1016/j.compeleceng.2022.107734.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0045790622000465*

Das, S., Nippert-Eng, C. and Camp, L. J. (2022), 'Evaluating user susceptibility to phishing attacks', *Information & Computer Security* **30**(1), 1–18. doi: 10.1108/ICS-12-2020-0204.
URL: *https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2020-0204/full/html*

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T. and Costabile, M. F. (2022), 'Human Factors in Phishing Attacks: A Systematic Literature Review', *ACM Computing Surveys* **54**(8), 1–35. doi: 10.1145/3469886.
URL: *https://dl.acm.org/doi/10.1145/3469886*

Ezennaya-Gomez, S., Blumenthal, E., Eckardt, M., Krebs, J., Kuo, C., Porbeck, J., Toplu, E., Kiltz, S. and Dittmann, J. (2022), Revisiting Online Privacy and Security Mechanisms Applied in the In-App Payment Realm from the Consumers' Perspective, *in* 'Proceedings of the 17th International Conference on Availability, Reliability and Security', ACM, New York, NY, USA, pp. 1–12. doi: 10.1145/3538969.3543786.
URL: *https://dl.acm.org/doi/10.1145/3538969.3543786*

Fariz, A. (2020), Analisis tingkat kesadaran keamanan informasi pada nasabah kartu kredit menggunakan multiple criteria decision analysis (MCDA): studi kasus Bank XYZ, Master thesis, Universitas Indonesia.

Firsty Arisya, K., Ruldeviyani, Y., Prakoso, R. and Lailatul Fadhilah, A. (2020), Measurement of Information Security Awareness Level: A Case Study of Mobile Banking (M-Banking) Users, *in* '2020 Fifth International Conference on Informatics and Computing (ICIC)', IEEE, pp. 1–5. doi: 10.1109/ICIC50835.2020.9288516.
URL: *https://ieeexplore.ieee.org/document/9288516/*

Gao, D., Lin, H., Li, Z., Qian, F., Chen, Q. A., Qian, Z., Liu, W., Gong, L. and Liu, Y. (2021), A nationwide census on wifi security threats, *in* 'Proceedings of the 27th Annual International Conference on Mobile Computing and Networking', ACM, New York, NY, USA, pp. 242–255. doi: 10.1145/3447993.3448620.
URL: *https://dl.acm.org/doi/10.1145/3447993.3448620*

Ghani, E. K., Ali, M. M., Musa, M. N. R. and Omonov, A. A. (2022), 'The Effect of Perceived Usefulness, Reliability, and COVID-19 Pandemic on Digital Banking Effectiveness: Analysis Using Technology Acceptance Model', *Sustainability* **14**(18), 11248. doi: 10.3390/su141811248.
URL: *https://www.mdpi.com/2071-1050/14/18/11248*

Guers, K., Chowdhury, M. M. and Rifat, N. (2022), Card Skimming: A Cybercrime by Hackers, *in* '2022 IEEE International Conference on Electro Information Technology (eIT)', IEEE, pp. 575–579. doi: 10.1109/eIT53891.2022.9813890.
URL: *https://ieeexplore.ieee.org/document/9813890/*

Hassandoust, F., Subasinghage, M. and Johnston, A. C. (2022), 'A neo-institutional perspective on the establishment of information security knowledge sharing practices', *Information & Management* **59**(1), 103574. doi: 10.1016/j.im.2021.103574.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0378720621001488*

Hijji, M. and Alam, G. (2022), 'Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees', *Sensors* **22**(22), 8663. doi: 10.3390/s22228663.
URL: *https://www.mdpi.com/1424-8220/22/22/8663*

Ifenthaler, D. and Yau, J. Y.-K. (2020), 'Utilising learning analytics to support study success in higher education: a systematic review', *Educational Technology Research*

and Development **68**(4), 1961–1990. doi: 10.1007/s11423-020-09788-z.
URL: *https://link.springer.com/10.1007/s11423-020-09788-z*

Jalali, M. S., Bruckes, M., Westmattelmann, D. and Schewe, G. (2020), 'Why Employees (Still) Click on Phishing Links: An Investigation in Hospitals', *Journal of Medical Internet Research* **22**(1), e16775. doi: 10.2196/16775.
URL: *http://www.jmir.org/2020/1/e16775/*

Jáñez-Martino, F., Alaiz-Rodríguez, R., González-Castro, V., Fidalgo, E. and Alegre, E. (2023), 'A review of spam email detection: analysis of spammer strategies and the dataset shift problem', *Artificial Intelligence Review* **56**(2), 1145–1173. doi: 10.1007/s10462-022-10195-4.
URL: *https://link.springer.com/10.1007/s10462-022-10195-4*

Kamar, O. (n.d.), 'Jenius BTPN: Jumlah Nasabah, Simpanan, dan Pengaduan'.
URL: *https://orangkamar.com/statistik-jenius-btpn/*

Kelley, N. J., Hurley-Wallace, A. L., Warner, K. L. and Hanoch, Y. (2023), 'Analytical reasoning reduces internet fraud susceptibility', *Computers in Human Behavior* **142**, 107648. doi: 10.1016/j.chb.2022.107648.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S074756322200468X*

Kruger, H. and Kearney, W. (2006), 'A prototype for assessing information security awareness', *Computers & Security* **25**(4), 289–296. doi: 10.1016/j.cose.2006.02.008.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0167404806000563*

Liu, Y., Eckert, C. M. and Earl, C. (2020), 'A review of fuzzy AHP methods for decision-making with subjective judgements', *Expert Systems with Applications* **161**, 113738. doi: 10.1016/j.eswa.2020.113738.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0957417420305625*

Mahardika, M. S., Hidayanto, A. N., Paramartha, P. A., Ompusunggu, L. D., Mahdalina, R. and Affan, F. (2020), 'Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia', *Advances in Science, Technology and Engineering Systems Journal* **5**(3), 501–509. doi: 10.25046/aj050362.
URL: *https://astesj.com/v05/i03/p62/*

Matveev, V., Nykytchenko, O. E., Stefanova, N., Khrypko, S., Ishchuk, A., Ishchuk, O. and Bondar, T. (2021), 'Cybercrime in the Economic Space: Psychological Motivation and Semantic-Terminological Specifics', *IJCSNS International Journal of Computer Science and Network Security* **21**(11), 135–142.
URL: *http://paper.ijcsns.org/07_book/202111/20211118.pdf*

McIlwraith, A. (2022), *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*, 2nd edn, Routledge, New York, NY, USA.

Mishra, S. and Soni, D. (2020), 'Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis', *Future Generation Computer Systems* **108**, 803–815. doi: 10.1016/j.future.2020.03.021.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0167739X19318758*

Murray, H. and Malone, D. (2022), Choosing Wordlists for Password Guessing: An Adaptive Multi-armed Bandit Approach, *in* E. Aïmeur, M. Laurent, R. Yaich, B. Dupont and J. Garcia-Alfaro, eds, 'Foundations and Practice of Security. FPS 2021. Lecture Notes in Computer Science, vol 13291', Springer, Cham, pp. 393–413. doi: 10.1007/978-3-031-08147-7_27.
URL: *https://link.springer.com/10.1007/978-3-031-08147-7_27*

Ohrimenco, S., Borta, G. and Cernei, V. (2021), Estimation of the Key Segments of the Cyber Crime Economics, *in* '2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)', IEEE, pp. 103–107. doi: 10.1109/PICST54195.2021.9772165.
URL: *https://ieeexplore.ieee.org/document/9772165/*

Okoli, C. and Schabram, K. (2010), 'A Guide to Conducting a Systematic Literature Review of Information Systems Research', *SSRN Electronic Journal* . doi: 10.2139/ssrn.1954824.
URL: *http://www.ssrn.com/abstract=1954824*

Olanrewaju, A.-S. T., Hossain, M. A., Whiteside, N. and Mercieca, P. (2020), 'Social media and entrepreneurship research: A literature review', *International Journal of Information Management* **50**, 90–110. doi: 10.1016/j.ijinfomgt.2019.05.011.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0268401218311708*

Orji, I. J., Kusi-Sarpong, S., Huang, S. and Vazquez-Brust, D. (2020), 'Evaluating the factors that influence blockchain adoption in the freight logistics industry', *Transportation Research Part E: Logistics and Transportation Review* **141**, 102025. doi: 10.1016/j.tre.2020.102025.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S1366554520306761*

Ozcelik, H. (2020), An Analysis of Fraudulent Financial Reporting Using the Fraud Diamond Theory Perspective: An Empirical Study on the Manufacturing Sector Companies Listed on the Borsa Istanbul, *in* S. Grima, E. Boztepe and P. Baldacchino, eds, 'Contemporary Issues in Audit Management and Forensic Accounting (Contemporary Studies in Economic and Financial Analysis, Vol. 102)', Emerald Publishing Limited, pp. 131–153. doi: 10.1108/S1569-375920200000102012.
URL: *https://www.emerald.com/insight/content/doi/10.1108/S1569-375920200000102012/full/html*

Ozili, P. K. (2018), 'Impact of digital finance on financial inclusion and stability', *Borsa Istanbul Review* **18**(4), 329–340. doi: 10.1016/j.bir.2017.12.003.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S2214845017301503*

Pahlevi, R. (2022), 'Jumlah Pengguna Aktif Bulanan Bank Digital Jenius Tertinggi di Indonesia'.

URL: *https://databoks.katadata.co.id/datapublish/2022/01/18/jumlah-pengguna-aktif-bulanan-bank-digital-jenius-tertinggi-di-indonesia#: :text=Pada 2021%2C jumlah pengguna aktif,mencapai 2%2C34 juta pengguna*

Prakoso, R., Ruldeviyani, Y., Arisya, K. F. and Fadhilah, A. L. (2020), Measurement of Information Security Awareness Level: A Case Study of Online Transportation Users, *in* '2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)', IEEE, pp. 170–175. doi: 10.1109/ISRITI51436.2020.9315375.
URL: *https://ieeexplore.ieee.org/document/9315375/*

Salem, Y., Moreb, M. and Rabayah, K. S. (2021), Evaluation of Information Security Awareness among Palestinian Learners, *in* '2021 International Conference on Information Technology (ICIT)', IEEE, pp. 21–26. doi: 10.1109/ICIT52682.2021.9491639.
URL: *https://ieeexplore.ieee.org/document/9491639/*

Sinha, P., kumar Rai, A. and Bhushan, B. (2019), Information Security threats and attacks with conceivable counteraction, *in* '2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)', IEEE, pp. 1208–1213. doi: 10.1109/ICICICT46008.2019.8993384.
URL: *https://ieeexplore.ieee.org/document/8993384/*

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R. and Shabtai, A. (2022), 'Contextual security awareness: A context-based approach for assessing the security awareness of users', *Knowledge-Based Systems* **246**, 108709. doi: 10.1016/j.knosys.2022.108709.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0950705122003276*

Soomro, Z. A., Ahmed, J., Shah, M. H. and Khoumbati, K. (2019), 'Investigating identity fraud management practices in e-tail sector: a systematic review', *Journal of Enterprise Information Management* **32**(2), 301–324. doi: 10.1108/JEIM-06-2018-0110.
URL: *https://www.emerald.com/insight/content/doi/10.1108/JEIM-06-2018-0110/full/html*

Suárez-Álvarez, J., Pedrosa, I., Lozano, L. M., García-Cueto, E., Cuesta, M. and Muñiz, J. (2018), 'Using reversed items in Likert scales: A questionable practice.', *Psicothema* **30**(2), 149–158. doi: 10.7334/psicothema2018.33.
URL: *http://www.ncbi.nlm.nih.gov/pubmed/29694314*

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R. and Ibrahim, M. A. (2022), 'Social Engineering Attacks Prevention: A Systematic Literature Review', *IEEE Access* **10**, 39325–39343. doi: 10.1109/ACCESS.2022.3162594.
URL: *https://ieeexplore.ieee.org/document/9743471/*

Tickner, P. and Button, M. (2021), 'Deconstructing the origins of Cressey's Fraud Triangle', *Journal of Financial Crime* **28**(3), 722–731. doi: 10.1108/JFC-10-2020-0204.

URL: *https://www.emerald.com/insight/content/doi/10.1108/JFC-10-2020-0204/full/html*

Utami, W., Nugroho, L., Mappanyuki, R. and Yelvionita, V. (2020), 'Early Warning Fraud Determinants in Banking Industries', *Asian Economic and Financial Review* **10**(6), 604–627. doi: 10.18488/journal.aefr.2020.106.604.627.
URL: *https://archive.aessweb.com/index.php/5002/article/view/1947*

Volkmar, G., Fischer, P. M. and Reinecke, S. (2022), 'Artificial Intelligence and Machine Learning: Exploring drivers, barriers, and future developments in marketing management', *Journal of Business Research* **149**, 599–614. doi: 10.1016/j.jbusres.2022.04.007.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0148296322003381*

Wang, P. (2022), 'Analysis of Computer Virus Defense Strategy Based on Network Security', *Academic Journal of Computing & Information Science* **5**(14), 33–39. doi: 10.25236/AJCIS.2022.051405.
URL: *https://francis-press.com/papers/8650*

Whitman, M. E. and Mattord, H. J. (2021), *Principles of Information Security*, 7th edn, Cengage Learning.

Wiley, A., McCormac, A. and Calic, D. (2020), 'More than the individual: Examining the relationship between culture and Information Security Awareness', *Computers & Security* **88**, 101640. doi: 10.1016/j.cose.2019.101640.
URL: *https://linkinghub.elsevier.com/retrieve/pii/S0167404819301841*

Yıldırım, M. and Mackie, I. (2019), 'Encouraging users to improve password security and memorability', *International Journal of Information Security* **18**(6), 741–759. doi: 10.1007/s10207-019-00429-y.
URL: *http://link.springer.com/10.1007/s10207-019-00429-y*

Appendix 1. The Questionnaire

Code	Focus Area	Sub-Focus Area	Question
PM1 - K (-)	*Password Management - Knowledge*	*Using the same password*	Using other personal account password for XYZ is acceptable.
PM1 - A (-)	*Password Management - Attitude*		Using other personal account password for XYZ is safe.
PM1 - B (+)	*Password Management - Behavior*		My XYZ account have different password from my other personal accounts.
PM2 - K (-)	*Password Management - Knowledge*	*Sharing password*	Sharing XYZ account password with people I know is acceptable.
PM2 - A (+)	*Password Management - Attitude*		Sharing XYZ account password with people I know is a bad idea although that people ask for it.
PM2 - B (-)	*Password Management - Behavior*		I share XYZ account password to people I know.
PM3 - K (+)	*Password Management - Knowledge*	*Using the strong password*	A combination of letter, number, and symbol is needed for password security.
PM3 - A (-)	*Password Management - Attitude*		Password that consists of just letters is safe.
PM3 - B (+)	*Password Management - Behavior*		I use combination of letter, number, and symbol for my XYZ account password.
EU1 - K (-)	*Email Use - Knowledge*	*Clicking on links in emails from known sender*	Clicking any link in email from people I know is acceptable.
EU1 - A (-)	*Email Use - Attitude*		Clicking any link in email from people I know is safe.
EU1 - B (+)	*Email Use - Behavior*		I don’t always click any link in email just because it’s sent from people I know.
EU2 - K (+)	*Email Use - Knowledge*	*Clicking on links in emails from unknown sender*	Clicking any link in email from unknown sender is not acceptable.
EU2 - A (-)	*Email Use - Attitude*		Nothing bad will happen if I click any link in email from unknown sender.
EU2 - B (-)	*Email Use - Behavior*		I click the link in email from unknown sender if it’s interesting.
EU3 - K (-)	*Email Use - Knowledge*	*Opening attachment in emails from unknown sender*	Opening attachment in email from unknown sender is acceptable.
EU3 - A (+)	*Email Use - Attitude*		Opening attachment in email from unknown sender is risky.

Code	Focus Area	Sub-Focus Area	Question
EU3 - B (+)	*Email Use - Behavior*		I don't open attachment if it's from unknown sender.
IU1 - K (-)	*Internet Use - Knowledge*	*Downloading files*	Downloading any file from internet to my device is acceptable.
IU1 - A (+)	*Internet Use - Attitude*		Downloading any file from internet to my device is risky.
IU1 - B (-)	*Internet Use - Behavior*		I download any file from internet to finish my task.
IU2 - K (+)	*Internet Use - Knowledge*	*Accessing dubious website*	Not every website in internet is safe to be accessed.
IU2 - A (+)	*Internet Use - Attitude*		I'm not sure all website is safe to be accessed.
IU2 - B (-)	*Internet Use - Behavior*		I open any website, even I use VPN (Virtual Private Network) to access it if it can't be opened normally.
IU3 - K (-)	*Internet Use - Knowledge*	*Entering information online*	Entering any information in website to finish a task is acceptable.
IU3 - A (-)	*Internet Use - Attitude*		If it can finish a task, I don't care what information that I enter in website.
IU3 - B (+)	*Internet Use - Behavior*		I assess website security before entering information inside it.
SM1 - K (+)	*Social Media Use - Knowledge*	*Social media privacy settings*	I supposed to review my social media privacy setting regularly.
SM1 - A (+)	*Social Media Use - Attitude*		Reviewing my social media privacy setting regularly is a good idea to be done.
SM1 - B (-)	*Social Media Use - Behavior*		I don't review my social media privacy setting regularly.
SM2 - K (-)	*Social Media Use - Knowledge*	*Considering consequences*	Things I share in social media will not be misused by other people.
SM2 - A (-)	*Social Media Use - Attitude*		Sharing something in social media that I will not share in public is acceptable.
SM2 - B (+)	*Social Media Use - Behavior*		I don't share something in social media before considering negative consequences that can happen.
SM3 - K (-)	*Social Media Use - Knowledge*	*Posting about private information*	I can share any information about myself in social media.
SM3 - A (+)	*Social Media Use - Attitude*		Sharing information about myself in social media is risky.
SM3 - B (-)	*Social Media Use - Behavior*		I share anything that I want to share in social media.

Code	Focus Area	Sub-Focus Area	Question
MD1 - K (+)	*Mobile Device - Knowledge*	*Physically securing mobile devices*	When in public and carrying a handphone, I always make sure I keep an eye on my handphone.
MD1 - A (-)	*Mobile Device - Attitude*		Leaving my handphone or laptop in public even for just a minute without supervision is safe.
MD1 - B (-)	*Mobile Device - Behavior*		When in public, I often don't keep an eye on my handphone or laptop.
MD2 - K (-)	*Mobile Device - Knowledge*	*Sending sensitive information via Wi-Fi*	Sending any information with public Wi-Fi is acceptable.
MD2 - A (+)	*Mobile Device - Attitude*		Sending any information with public Wi-Fi is risky.
MD2 - B (-)	*Mobile Device - Behavior*		I send any information with public Wi-Fi
MD3 - K (+)	*Mobile Device - Knowledge*	*Shoulder surfing*	When opening sensitive information or document, I must make sure nobody can see my handphone or laptop screen.
MD3 - A (+)	*Mobile Device - Attitude*		It is risky if there's someone who can see my handphone or laptop screen when opening sensitive information or document.
MD3 - B (+)	*Mobile Device - Behavior*		I make sure nobody can see my handphone or laptop screen when opening sensitive information or document.
AF1 - K (+)	*Anti-Fraud Awareness Campaign - Knowledge*	*Receiving XYZ campaign*	XYZ send notifications about how to secure personal data.
AF1 - A (+)	*Anti-Fraud Awareness Campaign - Attitude*		XYZ notifications about how to secure personal data is important.
AF1 - B (-)	*Anti-Fraud Awareness Campaign - Behavior*		I switch off notification from XYZ.
AF2 - K (+)	*Anti-Fraud Awareness Campaign - Knowledge*	*Accepting XYZ campaign*	XYZ has provided a way to secure personal data.
AF2 - A (+)	*Anti-Fraud Awareness Campaign - Attitude*		Knowing how to secure personal data is important
AF2 - B (-)	*Anti-Fraud Awareness Campaign - Behavior*		I don't read and delete XYZ notification about how to secure personal data immediately.
CM1 - K (-)	*Card Management - Knowledge*	*Storing physical card*	Letting anyone keeping my XYZ card is acceptable.
CM1 - A (+)	*Card Management - Attitude*		Letting anyone keeping my XYZ card is risky.
CM1 - B	*Card Management -*		I keep my XYZ card by myself.

Code	Focus Area	Sub-Focus Area	Question
(+)	*Behavior*		
CM2 - K (+)	*Card Management - Knowledge*	*Using physical card*	Sensitive information that exists in the back side of the card must be kept secret.
CM2 - A (-)	*Card Management - Attitude*		There is no risk if anyone see the back side of my card.
CM2 - B (-)	*Card Management - Behavior*		I let cashier see the back side of my card when doing transaction.
CI1 - K (+)	*Concern for Information Privacy - Knowledge*	*Trust in other's motives*	Clarity of the purpose of the request of personal data is acceptable.
CI1 - A (-)	*Concern for Information Privacy - Attitude*		I believe everyone has good intention by requesting personal data.
CI1 - B (+)	*Concern for Information Privacy - Behavior*		I ask the purpose of request of personal data from other people.
CI2 - K (+)	*Concern for Information Privacy - Knowledge*	*Reluctance on giving information*	I know which personal data that can be shared and cannot be shared to others.
CI2 - A (-)	*Concern for Information Privacy - Attitude*		Sharing personal data that can't be known by other people is safe.
CI2 - B (+)	*Concern for Information Privacy - Behavior*		I refuse sharing personal data that cannot be shared to others.
CI3 - K (+)	*Concern for Information Privacy - Knowledge*	*Action to keep information safe*	Sensitive information must be stored safely.
CI3 - A (-)	*Concern for Information Privacy - Attitude*		Storing sensitive information in a place that can be accessed anyone is not risky.
CI3 - B (-)	*Concern for Information Privacy - Behavior*		I don't pay attention to the security of storage to store sensitive information.
SI1 - K (-)	*Self-efficacy in Information Security - Knowledge*	*Sensitive information acknowledgement*	All information about personal data can be known by other people, including XYZ employee.
SI1 - A (+)	*Self-efficacy in Information Security - Attitude*		Sharing all personal data to others is risky.
SI1 - B (+)	*Self-efficacy in Information Security - Behavior*		I filter what personal data that I will share to others.
SI2 - K (+)	*Self-efficacy in Information Security - Knowledge*	*Suspicion on fraudster*	XYZ has official channels to communicate with customers.
SI2 - A (-)	*Self-efficacy in Information Security - Attitude*		Trusting XYZ official channels as the only option to communicate with bank is a bad idea.
SI2 - B (-)	*Self-efficacy in Information Security - Behavior*		I don't confirm the authenticity of the party claiming to be from XYZ who is trying to contact me.