ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 14 (2024) No. 8, pp. 394-404
DOI:10.33168/JSMS.2024.0825

Examining the Role of Security Self-Efficacy in Shaping Multi-Factor Authentication Adoption Intentions

Jason Matthew, Elfindah Princes

Information Systems Management Department, BINUS Graduate Program, Master of Information Systems Management, Bina Nusantara University, Jakarta, 11480, Indonesia

jason.matthew002@binus.ac.id, elfindah.princes@binus.edu

Abstract. This study analyzed how perceived security self-efficacy influences multi-factor authentication adoption intentions among 212 Indonesian consumers using partial least squares structural equation modeling (PLS-SEM). Findings confirmed positive impacts on perceived usefulness and ease beliefs, shaping subsequent usage attitudes and intentions. However, the student-concentrated sample limits generalizability. While highlighting psychosocial drivers, bounded rationality constraints like overconfidence biases require deeper examination. Ensuring balanced technology regulation mandating appropriate identity safeguards yet easing citizen adoption remains pivotal. Longitudinal probes into motivational factors inhibiting multifaceted authentication acceptance across various demographics can illuminate targeted protections balancing security, privacy, and convenience amidst heightening data breach risks.

Keywords: Security Self-Efficacy, Multi-Factor Authentication (MFA), Technology Adoption, Usage Attitudes, Partial Least Squares - Structural Equation Model (PLS-SEM).

1. Introduction

Technology, especially online applications such as social networks, e-commerce, and digital payments have been an integral part of people's lives. However, with the increase of technology usage in society, also comes the increase of cyber threats. This happens mainly because data is considered valuable information, and online platforms like Facebook and other online platforms save the users' personal and oftentimes confidential information including payment details and address (Kusyanti, Catherina, & Sari, 2019). To protect people from cyber threats, several methods such as passwords, PINs, and OTP codes are utilized by these application providers. Several platforms also prompt users to create a strong password to secure their accounts better. Unfortunately, these methods can still be bypassed using a number of methods including brute force attacks, phishing, and social engineering (Karim, et al., 2023).

In Indonesia, cyber security is one of the largest concerns for both the society and the government. According to the National Cyber Security Index (NCSI), Indonesia's cyber security is amongst the lowest among G20 countries with an index score of 38,96 out of 100 points. Indonesia's Criminal Investigation Department (Bareskrim Polri) also noted that cyber crime numbers in Indonesia have risen from 612 cases in 2021 to 8,831 cases in 2022 (Pusiknas Bareskrim Polri, 2022).

In creating passwords, usually longer, more complex passwords mean more secure passwords. However, it also means that it is harder to remember. Knowing this, the majority of people prefer short passwords that are easy to remember (NordPass, 2022). Research conducted by Google and YouGov confirms that 89% of research respondents in Indonesia are actively using non-secure passwords. Several institutions have used massive campaigns to increase awareness of these topics. However, even the people that understand the importance of data security still perform bad practices. According to (Wash, Rader, Berman, & Wellmer, 2016), 43-51% of internet users re-use passwords across accounts. This includes people that created a complex password at some point, then used the same password across several accounts.

Prior research has been conducted to find the best methods of password creation, password management, and even additional measures such as Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA). However, even if organizations implement high security standards, cyber criminals are still able to utilize social engineering practices to get around the security system. Social engineering itself is directly related to users' behavior towards technologies and security practices. Unfortunately, studies related to behavioral or psychological factors influencing internet users' adoption of safer methods remains to be seen, especially in Indonesia. One behavioral aspect of technology use is self-efficacy, in this case security self-efficacy. Since self-efficacy is related to security behaviors (Anwar, et al., Gender Difference and Employees' Cybersecurity Behaviors, 2017), this study will focus on whether it results in people intending to use MFA or not.

2. Literature Review

2.1. Information Security

Most, if not all online systems or applications collect information from users. These could include usage data from data tracker points which is collected automatically using cookies, or personal information collected when a user inputs data into the system. Information security is the concept of protecting this information from unauthorized as well as unwanted external or internal access, usage, disclosure, modification, or destruction (Andress, 2019).

2.2. Multi-Factor Authentication

To access information, one must be sure that the person accessing a particular piece of information is indeed the rightful owner or manager. To make sure of this, a set of methods are put in place called authentication (Andress, 2019). The main authentication methods can be defined into three groups, single-factor authentication, two-factor authentication (2FA), and multi-factor authentication (MFA). According to (Karim, et al., 2023), these factors can be based on the following categories:

- Knowledge-based authentication (KBA): Authentication based on personal knowledge or memory (password, PIN, security questions, etc.).
- Possession-based authentication (PBA): Physical devices owned by people that is not easily duplicated (card, key, phone, dongle, etc.).
- Biometric-based authentication (BBA): Related to the physical features of the user (fingerprint, retina, face, etc.).

Single-factor authentication is the most commonly used among most online systems. It usually consists of credentials such as email address or username and password. Although there are several methods of creating secure passwords, previous research shows that single-factor authentication is still vulnerable. To increase the security, another component can be introduced, making it a two-factor authentication. More than two factors will make it a multi-factor authentication, thus making it safer for users. Even if another entity acquires the password, they will not be able to proceed to other layers of authentication.

2.3. Security Self-Efficacy

Self-efficacy refers to confidence in one's own abilities, skills, and knowledge when performing a certain task (Halim, Teng, Hebrard, Sundaram, & Poba-Nzaou, 2023) or in this case, to mitigate cyber-security risks (Halevi, et al., Cultural And Psychological Factors In Cyber-Security, 2017). Self-efficacy can be divided into two, response efficacy and coping self-efficacy. Response efficacy is the belief that one's own actions will be effective against a certain occurrence, while coping self-efficacy is the belief in one's own ability to do a particular action. Therefore, these behaviors can be classified further either into adaptive (protective) by choosing to use MFA, or maladaptive (avoidance) by choosing to avoid the use of MFA. However, the core belief is that higher self-efficacy results in adaptive behaviors rather than maladaptive ones (Howe, Ray, Roberts, Urbanska, & Byrne, 2012).

2.4. Technology Acceptance Model

The Technology Acceptance Model (TAM) introduced in 1989 is considered the most commonly used theory to describe an individual's acceptance of information systems (Davis, 1989). Since its inception, TAM has been used in many studies testing acceptance towards technology. TAM explains that perceived ease of use and perceived usefulness predict an individual's attitude towards using a certain technology, their behavioral intention to use, and their actual system use as seen on Figure 1 below.

Perceived usefulness is defined as how far an individual believes that the usage of a certain technology will improve their work performance. On the other hand, perceived ease of use refers to how far an individual believes that the usage of a certain technology will feel effortless. Both variables then influence an individual's attitude towards using a technology. Then, perceived usefulness as well as attitude towards using influences an individual's behavioral intention to use. Finally, the behavioral intention to use influences the actual system use of a certain technology (Masrom, 2007).

In this research, TAM will have a role in explaining how people perceive Multi-Factor Authentication (MFA) and how it impacts their intention to use the technology. To further enhance the research model, an external variable, security self-efficacy, is added. People's security self-efficacy is expected to have an impact on how they perceive the technology being MFA.

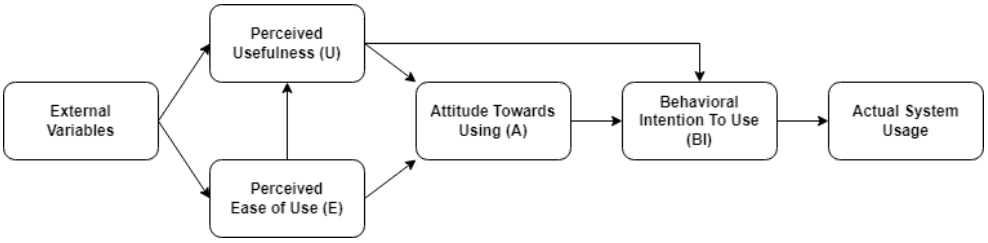

Fig. 1: Technology Acceptance Model

3. Methodology

3.1. Model Building and Hypotheses Development

The research model, shown in Figure 2, utilizes the variables contained in the Technology Acceptance Model (TAM). Since this research focuses on the intention to use Multi-Factor Authentication (MFA), the variable Actual System Usage is omitted. In addition, an external variable Security Self Efficacy is added to the model as an independent variable. In the model proposed, there are 5 variables with 7 hypotheses between them, connecting the variables.

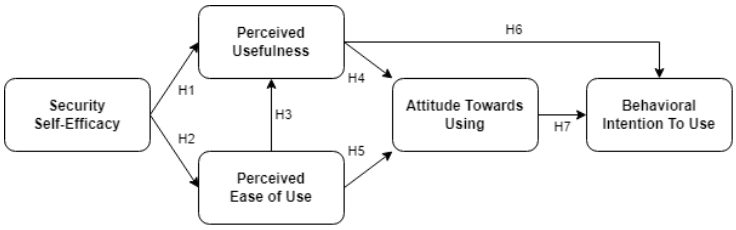

Fig 2: Research Model

H1: Security Self-Efficacy (SS) has a significant impact on users' Perceived Usefulness (PU) of MFA.

H2: Security Self-Efficacy (SS) has a significant impact on users' Perceived Ease of Use (PE) of MFA.

H3: The Perceived Ease of Use (PE) of MFA has a significant impact on users' Perceived Usefulness (PU).

H4: The Perceived Usefulness (PU) of MFA has a significant impact on users' Attitude Towards Using (AT) the MFA technology.

H5: The Perceived Ease of Use (PE) of MFA has a significant impact on users' Attitude Towards Using (AT) the MFA technology.

H6: The Perceived Usefulness (PU) of MFA has a significant impact on users' Behavioral Intention to Use (BI) the MFA technology.

H7: The Attitude Towards Using (AT) MFA has a significant impact on users' Behavioral Intention to Use (BI) the MFA technology.

As shown in Figure 2 and the hypotheses development, 5 variables are included in the research model. The variables are Security Self-Efficacy (SS), Perceived Usefulness (PU), Perceived Ease of Use (PE), Attitude Towards Using (AT), and Behavioral Intention to Use (BI). Each of these variables will have 5 indicators, as shown on Table 1 below.

Table 1. Variables and Indicators

Security Self-Efficacy (SS)		**Ref.**
I am aware of the importance of data security	SS1	(Anwar, et al., Gender Difference and Employees' Cybersecurity Behaviors, 2017) (Halim, Teng, Hebrard, Sundaram, & Poba-Nzaou, 2023) (Kulviwat, Bruner II, & Neelankavil, 2014)
I have the knowledge to secure my internet accounts (emails, messengers, social media, etc.)	SS2	
I feel confident in setting up security measures for my internet accounts	SS3	
I feel confident in managing my security measures without the help of others	SS4	
I feel comfortable handling security problems with my accounts.	SS5	
Perceived Usefulness (PU)		**Ref.**
Using multi-factor authentication (MFA) allows me to secure my accounts better	PU1	(Kurniasari, Hamid, & Qinghui, 2020) (Holden & Roy, 2011) (Kenyta, 2022)
Multi-factor authentication (MFA) increases the effectiveness of securing my accounts	PU2	

Multi-factor authentication (MFA) usage increases my productivity	PU3	
I find multi-factor authentication (MFA) to be useful in my day-to-day activities	PU4	
Overall, multi-factor authentication (MFA) is helpful	PU5	
Perceived Ease of Use (PE)		**Ref.**
I find multi-factor authentication (MFA) easy to learn	PE1	(Kurniasari, Hamid, & Qinghui, 2020) (Holden & Roy, 2011) (Kenyta, 2022)
I find multi-factor authentication (MFA) easy to use	PE2	
I find multi-factor authentication (MFA) flexible to use	PE3	
I easily remember how to use multi-factor authentication (MFA)	PE4	
It is easy for me to become skillful at using multi-factor authentication (MFA)	PE5	
Attitude Towards Using (AT)		**Ref.**
I believe using multi-factor authentication (MFA) is an interesting idea	AT1	(Chin, Zakaria, Purhanudin, & Pin, 2021)
I believe using multi-factor authentication (MFA) is a good idea	AT2	
I believe using multi-factor authentication (MFA) would be a pleasant experience	AT3	
I am interested in using multi-factor authentication (MFA) to secure my account	AT4	
I think everyone should use multi-factor authentication (MFA) to secure their accounts	AT5	
Behavioral Intention to Use (BI)		**Ref.**
I always try to use multi-factor authentication (MFA) to secure my accounts	BI1	(Kurniasari, Hamid, & Qinghui, 2020) (Chin, Zakaria, Purhanudin, & Pin, 2021)
I always use multi-factor authentication (MFA) to secure my accounts even if it is not required of me to do so	BI2	
I intend to use multi-factor authentication (MFA) to secure my accounts	BI3	
I predict that I would use multi-factor authentication (MFA) to secure my accounts	BI4	
I would recommend other people to use multi-factor authentication (MFA) to secure their accounts	BI5	

3.2. Data Collection

This study targets people residing in Jabodetabek (Jakarta, Bogor, Depok, Tangerang, and Bekasi) region in Indonesia. The respondents are expected to have online accounts using at least a single-factor authentication (username/email and password) and ideally already having multiple-factor authentication activated on some of the accounts.

An online questionnaire through Google Forms will be utilized to assist with data collection. The questionnaire will consist of a few parts according to the research model synthesized before the questionnaire was made. To give answers, respondents are required to fill in a Likert scale consisting of 5 possible answers: “Strongly Agree,” “Agree,” “Neutral,” “Disagree,” and “Strongly Disagree”.

The data collection period lasts from 22 January 2024 to 31 January 2024 targeting 200 respondents. The online questionnaire is then posted through social media, private online channels such as messengers, and online survey platforms.

3.3. Data Analysis

The study also uses the multivariate statistical analysis method Structural Equation Model – Partial Least Squares (SEM-PLS). A software, SmartPLS, is also utilized to assist in processing the raw data. SEM enables researchers to incorporate unobservable variables measured indirectly by indicator variables. PLS-SEM focuses on explaining the variance in dependent variables when examining the

model (Hair, Hult, Ringle, & Sarstedt, 2017).

4. Research Findings and Discussion

4.1. Respondents' Demography

This research collected responses from 212 respondents through multiple online channels. Although this research targets people residing in Jabodetabek area (Jakarta, Bogor, Depok, Tangerang, Bekasi), this study also reaches 35 people (16.5%) outside the area. Based on the responses, people from various backgrounds are found across different age groups and education levels. The majority of respondents are from generation Y and Z (89.1%), with over half of the respondents being students (53.3%). Further details on the respondents' demography are listed in Table 2 below.

Table 2. Respondents' Demography

	Characteristics	Frequency	Percentage
Gender	Male	70	33%
	Female	142	67%
Age	15-19	44	20.8%
	20-24	111	52.4%
	25-29	18	8.5%
	30-34	9	4.2%
	35-39	7	3.3%
	40+	23	10.7%
Occupation	Student	113	53.3%
	Private Sector Employee	56	26.4%
	Civil Servant	2	0.9%
	Freelancer	21	9.9%
	Healthcare/Social Worker	2	0.9%
	Unemployed	11	5.2%
	Retired	2	0.9%
	Others	5	2.5%
Latest Education	Junior High School	6	2.8%
	Senior High School	106	50%
	Diploma	14	6.6%
	Academy	1	0.5%
	Bachelor's Degree	79	37.3%
	Master's Degree	6	2.8%
Location	Jakarta	75	35.4%
	Tangerang	52	24.5%
	Bogor	15	7.1%
	Depok	10	4.7%
	Bekasi	25	11.8%
	Others	35	16.5%

All 212 respondents are then given a question to see what authentication methods they use the most. They are given a list of the most common authentication methods, and they can click on the checkboxes listing the methods. Each respondent is allowed to choose more than one method.

Table 3 will list all the responses from 212 respondents regarding the authentication methods they have used before. The list will be organized into which authentication methods are used the most to the ones used the least.

Table 3. Most Used Authentication Methods

	Characteristics	Frequency
Authentication Methods	Password	186
	PIN	176
	Email Verification	163
	Biometrics	149
	SMS OTP Code	135

	Pattern Drawing	111
	Authenticator Applications	57
	Hardware Tokens	38

4.2. Validity and Reliability Testing

The assessment of validity and reliability using Structural Equation Modeling (SEM) is expressed through Convergent Validity which is shown through Average Variance Extracted (AVE) and Outer Loading Factor. Convergent Validity itself refers to the principle where indicators in one construct must be correlated. Before getting to AVE values, the Outer Loading values must be examined beforehand. Each indicator should have an Outer Loading number of over 0.7 to be determined as valid. Accepted AVE values are the ones above 0.5 (Latan & Ghozali, 2015), while Composite Reliability (CR) and Cronbach's Alpha (CA) values are accepted between 0.6 and 0.7 and are satisfying over 0.7 (Hair, Hult, Ringle, & Sarstedt, 2017).

Table 4. Variables and Indicators Validity and Reliability

No.	Variables/Indicators	Outer Loading	AVE	CR	CA
	SS		0.684	0.867	0.769
1	SS1	-			
2	SS2	0.840			
3	SS3	0.808			
4	SS4	0.833			
5	SS5	-			
	PU		0.678	0.913	0.881
6	PU1	0.806			
7	PU2	0.840			
8	PU3	0.814			
9	PU4	0.830			
10	PU5	0.828			
	PE		0.750	0.937	0.916
11	PE	0.874			
12	PE2	0.899			
13	PE3	0.834			
14	PE4	0.859			
15	PE5	0.861			
	AT		0.682	0.915	0.883
16	AT1	0.833			
17	AT2	0.873			
18	AT3	0.808			
19	AT4	0.817			
20	AT5	0.796			
	BI		0.741	0.935	0.912
21	BI1	0.853			
22	BI2	0.828			
23	BI3	0.898			
24	BI4	0.862			
25	BI5	0.861			

On the first round of data processing and analysis, it was found that indicators SS1 and SS5 did not pass the validity and reliability testing, with scores of 0.590 and 0.659 respectively. Therefore, both indicators are then omitted, and the data processing is run for the second time. It is shown in Table 4 that all other indicators pass the validity and reliability assessment. As for Average Variance Extracted (AVE), Composite Reliability (CR), and Cronbach's Alpha (CA), all variables met the minimum value for it to be considered valid and reliable.

The next step is to look at the Discriminant Validity by using the Fornell Larcker Criterion (Hair, Hult, Ringle, & Sarstedt, 2017). Discriminant Validity tests the correlation of a variable to itself. Then, it will be compared to the correlation of a variable to other variables. Ideally, the correlation of the variable tested with its own self must be greater than the correlation of the variable tested with other

variables. Table 5 below will show the Discriminant Validity testing, confirming that the variables are indeed valid with them showing a stronger correlation to themselves rather than to other variables.

Table 5. Discriminant Validity Through Fornell Larcker Criterion

Variable	AT	BI	PE	PU	SS
AT	**0.826**				
BI	0.790	**0.861**			
PE	0.721	0.691	**0.866**		
PU	0.784	0.729	0.743	**0.824**	
SS	0.503	0.607	0.651	0.583	**0.827**

4.3. Evaluation of Structural Model Through Coefficient of Determination

The Coefficient of Determination or R-Square, being the predictive power in the sample, is a measure of the explanatory power of a research model (Purwanto & Sudargini, 2021). It shows how far the dependent (endogenous) variable is affected by the independent (exogenous) variable. R-Square values of 0.75, 0.50. and 0.25 are classified as substantial, moderate, and weak respectively.

From the numbers listed in Table 6, it can be concluded that the independent variable Security Self-Efficacy has a 42.4% influence on the dependent variable Perceived Ease of Use (PE), while it is also influenced by other variables outside of the variables used in this research. Security Self-Efficacy and Perceived Ease of Use (PE) has a 56.9% influence on the dependent variable Perceived Usefulness (PU). Both variables Perceived Ease of Use (PE) and Perceived Usefulness (PU) are also known to have a 65.7% influence towards the variable Attitude Towards Using (AT). Finally, Perceived Usefulness (PU) and Attitude Towards Using (AT) has a 65.5% influence on the variable Behavioral Intention to Use.

Table 6. R-Square Values

Variable	R-Square Value
Perceived Usefulness (PU)	0.569
Perceived Ease of Use (PE)	0.424
Attitude Towards Using (AT)	0.657
Behavioral Intention to Use (BI)	0.655

4.4. Hypotheses Testing

The final step in this research is the hypothesis testing done by calculating and analyzing the Path Coefficient values (or Original Sample), T-Statistics, and P value. Path Coefficient, according to (Sarstedt, Ringle, Smith, Reams, & Hair, 2014), has a value range of -1 to 1. If the Path Coefficient shows a positive number, it means that the relationship between the variables is positive. A T-Statistic value over 1.96 and P value under 0.05 means that the impact of variables is significant, thus confirming the hypothesis proposed beforehand. As shown in Table 7 below, all hypotheses are accepted since each one of them has a T-Statistics value of over 1.96 and P Value of under 0.05.

Table 7. Hypotheses Testing Summary

Relation	Original Sample (O)	T-Statistics	P Values
SS→PU	0.173	2.191	0.028
SS→PE	0.651	13.274	0.000
PE→PU	0.630	8.378	0.000
PU→AT	0.555	6.282	0.000
PE→AT	0.309	3.198	0.001
PU→BI	0.286	3.294	0.001
AT→BI	0.566	7.180	0.000

H1: With a T-Statistic value of 2.191 (>1.96) and a P value of 0.028 (<0.05), it is confirmed that Security Self-Efficacy (SS) has a significant impact on users' Perceived Usefulness (PU) of MFA. Therefore, H1 is accepted.

H2: With a T-Statistic value of 13.274 (>1.96) and a P value of 0.000 (<0.05), it is confirmed that Security Self-Efficacy (SS) has a significant impact on users' Perceived Ease of Use (PE) of MFA. Therefore, H2 is accepted.

H3: With a T-Statistic value of 8.378 (>1.96) and a P value of 0.000 (<0.05), it is confirmed that the Perceived Ease of Use (PE) of MFA has a significant impact on users' Perceived Usefulness (PU). Therefore, H3 is accepted.

H4: With a T-Statistic value of 6.282 (>1.96) and a P value of 0.000 (<0.05), it is confirmed that the Perceived Usefulness (PU) of MFA has a significant impact on users' Attitude Towards Using (AT) the MFA technology. Therefore, H4 is accepted.

H5: With a T-Statistic value of 3.198 (>1.96) and a P value of 0.001 (<0.05), it is confirmed that the Perceived Ease of Use (PE) of MFA has a significant impact on users' Attitude Towards Using (AT) the MFA technology.

H6: With a T-Statistic value of 3.294 (>1.96) and a P value of 0.001 (<0.05), it is confirmed that the Perceived Usefulness (PU) of MFA has a significant impact on users' Behavioral Intention to Use (BI) the MFA technology.

H7: With a T-Statistic value of 7.180 (>1.96) and a P value of 0.000 (<0.005), it is confirmed that the Attitude Towards Using (AT) MFA has a significant impact on users' Behavioral Intention to Use (BI) the MFA technology.

4.5. Discussion

Based on the hypothesis testing done above, it is concluded that all hypotheses are accepted, meaning that each variable has a significant influence on the dependent variables. This is in line with previous research done by (Kulviwat, Bruner II, & Neelankavil, 2014), where self-efficacy was deemed to be a positive influence towards technology acceptance. From that finding, it is concluded that when an individual feels confident and comfortable in using a technology, they tend to perceive that technology as useful or consider it easy to use. The general findings of this research are also in line with previous research conducted by (Halim, Teng, Hebrard, Sundaram, & Poba-Nzaou, 2023) which concluded that most people are aware of data security and are utilizing methods to increase their personal security. This also confirms the theory from (Howe, Ray, Roberts, Urbanska, & Byrne, 2012) that people with high self-efficacy tend to adopt adaptive behaviors, in this case adopt MFA technology rather than avoid it.

Another previous research done by (Anwar, et al., Gender Difference and Employees' Cybersecurity Behaviors, 2017) focuses on gender as a moderating variable. This previous research shows that the self-efficacy of women is significantly lower than that of men. Although at a glance, women respondents in this research score slightly lower than men, it cannot be concluded that the findings are validated through this research. Further detailed analysis is still needed to confirm this finding, which is out of scope. However, it also means that this is an opportunity for further research in the future.

5. Conclusion

5.1. Research Findings Summary

This initial examination of psychological determinants driving consumer authentication technology adoption provides impetus for further academically grounded but practically relevant research. Findings confirm relationships between perceived digital proficiency and intentions to utilize multifaceted identity validation. However, deconstructing rationality limits around overassurance requires behavioral probes complementing techno-centric protections. Holistic cybersecurity envisions preemptive human-centered design thinking rather than reactive control policies. As digital infusion

accelerates across Asia, nurturing cultures of virtue ethics balancing empowerment and accountability can sustain resilience. Beyond one-size-fits-all compliance rules, contextual insights into motivations shaping usage reluctance may reveal tailored safeguards and awareness pathways reconciling security with counterbalancing rights. Longitudinal mixed-methods research transcending demographic silos can engender such revelation.

5.2. Limitations and Future Research

Although this research utilizes public online channels to reach a diverse audience, it is still mainly based in one area of Indonesia. One limitation of this is a possibility of bias as a certain society based in one area may have different behaviors compared to societies in other areas. In further research, other regions of Indonesia can be explored, especially regions or provinces outside Java. Another thing that can be explored is the detailed differences in behavior among various demographics. Gender, age, location, and educational background could possibly influence the results of this study. However, that remains out of scope in this study.

As for the variables, further research can explore other psychological or behavioral factors that influence personal cyber security. This is because one of the causes of data breaches is related to human behavior, especially human error in securing information. The further detailed research on this topic will definitely be valuable for academic and practical purposes as this means we can identify more causes of data breaches and hopefully decrease the number of cyber crime cases in Indonesia.

References

Andress, J. (2019). *Foundations of Information Security: A Straightforward Introduction.* San Francisco: No Starch Press, Inc.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017, April). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior, 69*, 437-443.

Chin, K. Y., Zakaria, Z., Purhanudin, N., & Pin, C. T. (2021). A Paradigm of TAM Model in SME P2P Financing. *International Journal of Economics and Management, 15*(3), 397-414.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3).

Hair, J. F., Hult, G. T., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) Second Edition.* Thousand Oaks, California: SAGE Publications Inc.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., . . . Chen, J. (2017). Cultural Aan Psychological Factors In Cyber-Security. *Journal of Mobile Multimedia, 13*, 43-56.

Halim, E., Teng, A. H., Hebrard, M., Sundaram, D., & Poba-Nzaou, P. (2023, September). The Usage of Password Generators to Enhance Data Security in Most Used Applications. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)*, 632-648.

Holden, H., & Roy, R. (2011). Understanding the Influence of Perceived Usability and Technology Self-Efficacy on Teachers' Technology Acceptance. *Journal of Research on Technology in Education, 43*, 343-367.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012). Social and Human Elements of Information Security: Emerging Trends and Countermeasures. *IEEE Symposium on Security and Privacy*, 209-223.

Karim, N. A., Kanaker, H., Abdulraheem, W. K., Ghaith, M. A., Alhroob, E., & Alali, A. M. (2023). Choosing the right MFA method for online systems: A comparative analysis. *International Journal of Data and Network Science*, 202-212.

Kenyta, C. (2022). Analysis of the Effect of Perceived Usefulness, Perceived Ease of Use, and Trust of Security on Customer Loyalty through Customer Satisfaction on the OVO Application. *International Journal of Review Management, Business, and Entrepreneurship (RMBE), 2*(2), 14-25.

Kulviwat, S., Bruner II, G. C., & Neelankavil, J. P. (2014). Self-Efficacy As An Antecedent Of Cognition And Affect In Technology Acceptance. *Journal of Consumer Marketing, 31*(3), 190-199.

Kurniasari, F., Hamid, N. A., & Qinghui, C. (2020, August 2). The Effect of Perceived Usefulness, Perceived Ease of Use, Trust, Attitude, and Satisfaction Into Continuance of Intention in Using Alipay. *Management & Accounting Review, 19*(2), 131-150.

Kusyanti, A., Catherina, H. P., & Sari, Y. A. (2019). Protecting Facebook Password: Indonesian Users' Motivation. *The Fifth Information Systems International Conference 2019*, 1182-1190.

Latan, H., & Ghozali, I. (2015). *Partial Least Squares: Concepts, Techniques and Applications using SmartPLS 3.* Diponegoro University Press.

Masrom, M. (2007). Technology Acceptance Model and E-learning. *12th International Conference on Education, Sultan Hassanal Bolkiah Institute of Education*, 1-10.

NordPass. (2022). *Top 200 Most Common Passwords*. Retrieved from https://nordpass.com/most-common-passwords-list/

Purwanto, A., & Sudargini, Y. (2021). Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review. *Journal of Industrial Engineering & Management Research*, 114-123.

Pusiknas Bareskrim Polri. (2022). Retrieved from https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Sarstedt, M., Ringle, C. M., Smith, D., Reams, R., & Hair, J. F. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *Journal of Family Business Strategy*, 105-115.

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. *Symposium on Usable Privacy and Security (SOUPS)*, 175-188.