p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 5, No. 11, November 2024 http://jist.publikasiindonesia.id/

The Influence of Cyber Security Knowledge, Cyber Security Awareness, and Behaviour Protection on Intention to Use Among Mobile Banking Users in Jakarta

Diki Muliawan[1*], Hasnawati[2]
Universitas Trisakti, Indonesia
Email: diki.muliawan@gmail.com[1*], hasnawati@trisakti.ac.id[2]

*Correspondence

Keywords: cybersecurity awareness; cybersecurity knowledge; behavior protection; intention to use.

ABSTRACT

Businesses and individuals, especially banks, must use risk assessment methods and preventive measures to protect mobile banking application users. Looking at these events, the researcher aims to see whether cyber security awareness, knowledge & behavior protection of users affect the intention to use mobile banking applications and whether these three variables are important for mobile banking users to understand in maintaining the security of transactions using mobile banking which will test the influence of these 3 variables on users' interest in continuing to use mobile banking even though users know the high risk if there is negligence in carrying out these 3 things and believing in the security of the mobile banking system in Indonesia. The population of this study is people who work in Jakarta. The respondents' answers were taken using Google Docs and distributed in general. The researcher obtained a total of 130 respondents. The data was processed using SPSS 27 with the analysis method of validity, reliability, and hypothesis test including the R2 test, F test, and T-test.

Introduction

The Industry 4.0 era has had a significant impact, especially in the field of online buying and selling through platforms by each E-Commerce company in Indonesia. The dissemination of information and the online buying and selling process have made the emergence of various types of data spread online in Indonesia to meet the needs of today's society. The emergence of the Big Data phenomenon that requires technological development in processing and integrating data in large quantities and variants aims to make it easier for information users to be faster in making decisions. (Gao, 2022) argues that with the help of big data technology, paperless offices can also be realized, which can comprehensively improve network transmission efficiency, reduce paper waste, reduce investment costs, and improve company efficiency in the field of financial accounting information.

The amount of data that must be processed due to the existence of this big data phenomenon is also supported by the development of payment technology to make it easier for users to make payments quickly and safely. This certainly causes the increasing number of online transactions that occur in Indonesia. The change in payment transactions that were originally cash to non-cash has become the current trend. The type of payment that is currently developing in Indonesia is the electronic wallet. According to (Rahmawati & Sari, n.d.), an electronic wallet is an electronic service that functions as a place to store payment instrument data, either in the form of a payment instrument using cards and/or electronic money, which can accommodate funds to make payment transactions. Users tend to use e-wallets for convenience reasons, therefore consumers prefer to use e-wallets over cash. Because they don't need to carry money and debit/credit cards and feel safe with the right money and change when transacting. The use of electronic wallets is currently regulated by the Central Bank of the Republic of Indonesia in Regulation Number 20/6/PBI/2018 itself in 2018. The most use of mobile banking is in developing countries, according to Hameed research (2023) developing countries such as Malaysia have an increase of 29% in 2023 in the use of mobile banking, of course, one of these is also supported by tourists who visit developing countries because vacationers certainly tend to adjust to using the most familiar means of payment in the country because tourists prefer to use mobile banking which is easy in currency conversion, safe and familiar with local payments. According to (Usman, 2022) in several locations of the Glodok Jakarta Trade Area, most businesses there have used payment methods to suppliers through bank transfers, online debits, and virtual account transfers. According to (Usman, 2022) research, this payment method is a payment method that is quite dominant among traders. In this case, transactions through E-commerce platforms increased to 65% compared to the previous one which was only less than 30% of total transactions. These merchants not only sell online through online marketplaces but offline businesses also make online payments as well.

The increase in the use of mobile banking is due to the development of the times that require people to make payments online, even though some restaurants now do not accept cash payments. Mobile banking is also often used anywhere as long as it is connected to the internet, making it easier for buyers to make payments. According to (Limna, Kraiwanit, & Siripipattanakul, 2023), mobile banking allows customers to make financial transactions from anywhere, anytime, using mobile phones, handheld devices, and internet data packages, which certainly eliminates the limitations of space and time associated with traditional banking activities such as checking account balances or transferring funds from one account to another.

In addition to the convenience of using mobile banking, some risks arise from its use. Security risks in using mobile banking are real and can be experienced around us. According to the 2023 Indonesian Cyber Security Landscape Annual Report from the State Cyber and Cryptography Agency (BSSN), Indonesia is ranked first above the United States and Singapore in terms of anomalous traffic detection, which briefly states the number of hackers using Indonesian IP addresses and the source of the hack's purpose

also the most in the world is Indonesia. The total anomalous traffic in Indonesia during 2023 is 403,990,813 anomalies with the highest type of anomalous traffic, namely the Generic Trojan RAT, which indicates backdoor communication activities to malicious domains that are indicated as command and control servers belonging to threat actors. According to this BSSN report, the activities of this Generic Trojan RAT have the potential to be used to carry out various suspicious activities such as information theft, data deletion, blocking, copying information, and running programs on infected devices against the user's will. Based on the results of Cyber Threat Intelligence monitoring and analysis, BSSN also traced alleged cyber incidents with a total of 347 alleged cyber incidents with the highest number of alleged incident types, namely Data Breach. The results of a search on the darknet found that there were 1,674,185 findings of exposure data that had an impact on 429 stakeholders in Indonesia. In the case of web defacement, it was found that as many as 189 cases had been notified by BSSN with the most case classification being web defacement on hidden pages. Based on reports received from stakeholders in the cyber complaint service, 1,417 complaints were obtained with the most complaint category being cybercrime at 86%. As we know, fraud or scams in the form of cybercrime that occur in our daily lives are increasingly rampant. This crime may befall the people closest to us, thus lowering our intention to use technological advances that help our lives and also our daily activities.

Seeing the many cases of Cybercrime, there is therefore a previous study that tested the role of Cyber Security Knowledge, Awareness & Behaviour Protection in the use of mobile banking in Thailand. According to (Limna et al., 2023), Cyber Security Knowledge & Cyber Security Awareness has a positive effect on the Behavioural Protection of mobile banking users in the ability to choose, not only being told what to do or only given one thing, but users are aware of the high risk of Cyber Security, therefore mobile banking users prefer actions that aim to prevent and guard against user behavior on the internet that causes data leaks to protect their respective devices from the threat of Cybercrime. The results of (Zwilling et al., 2022) research show that internet users who understand the term cyber security, users with good cyber security knowledge, cyber security awareness & behavioral protection have a positive influence on interest in using better and safer measurable protection when using advanced technology. Reid (2016) showed that the campaign to increase cyber security knowledge, awareness, and behavioral protection also has the effect of increasing cyber security culture or culture to maintain cyber security in the lives of respondents from this research by instilling education about these 3 things which certainly affect the respondents' daily actions and intentions Respondents in maintaining cyber security in their respective environments. The purpose of these 3 things is of course to maintain security in our transactions or work. This study modifies the previous research by adding the dependent variable Intention to Use from the Unified Theory of Acceptance and Use of Technology (UTAUT) model (Venkatesh, Thong, & Xu, 2012) and making the variables Cyber Security Knowledge, Cyber Security Awareness & Behavioural Protection as independent variables that affect users' interest in using Mobile banking that exists now and beyond when cybersecurity

threats are emerging in the surrounding environment. The researcher wants to test the 3 variables with different objects, namely testing in Indonesia with mobile banking available here, the purpose of this study is to see if cyber security awareness, knowledge & behavior protection affect the intention to use mobile banking applications. By seeing whether these 3 things are important for mobile banking users to understand in maintaining the security of transactions using mobile banking, which affects the user's interest in continuing to use mobile banking even though the user knows the high risk if there is negligence in carrying out these 3 things and believes in the security of the mobile banking system in Indonesia to make transactions daily.

The practical benefits of this research are expected to provide input for bank management as a consideration in improving the preparation of cybersecurity strategies. The theoretical benefit of this study is to provide additional empirical evidence on the development of the concept theory of the cyber security awareness, knowledge & behavior protection model. The results of this study are also expected to clarify the concept of the Unified Theory of Acceptance and Use of Technology (UTAUT) model, especially the variable-dependent intention to use in the mobile banking phenomenon in Indonesia. This study is expected to add additional references from previous research by changing the research object.

Method

This study will use a quantitative approach by distributing questionnaires to employees who use mobile banking applications. The questionnaire questions used references from (Limna et al., 2023) which were modified with questions for dependent variables of the UTAUT model from (Zhao, Anong, & Zhang, 2019). The questions in the questionnaire were also modified by the researcher to adjust to the research object because there was a difference between the research object and the previous researcher.

Research Population and Sample

The population of the study is mobile banking users in Jakarta in 5 banks with book 4 status. Researchers use the convenience sampling method, namely convenience sampling which is considered the best way to get basic information quickly and efficiently. Convenience sampling is the collection of information from members of the population who are easily contacted to provide it (Sekaran & Bougie, 2016). The sample of this study is respondents from the population, namely people who use mobile banking applications in Jakarta.

Independent Variable (X)

Independent variables are variables that can influence other variables that have a positive or negative influence on other variables. According to (Sekaran & Bougie, 2016), independent variables are variables that affect dependent variables positively or negatively. Independent variables can influence and be the cause of changes or the emergence of dependent variables, so it can be concluded that an increase or decrease in the independent variable will affect an increase or decrease in the dependent variable. The independent variables in this study are:

1. Cyber security knowledge (X1)
2. Cyber security awareness (X2)
3. Behaviour protection (X3)

Variabel Depend (Y)

Dependent variables are variables that can be influenced by independent variables, so dependent variables can change based on the influence of independent variables. Dependent variables are variables that can be influenced or changed due to the existence of independent variables, the purpose of the study is to be able to describe or forecast dependent variables (Sekaran & Bougie, 2016). This study will use intention to use (Y) as a dependent variable or variable that can be influenced by independent variables.

Data Analysis Methods

This study uses SPSS with a classical assumption test and then if it is normal, it will proceed to multiple linear regression analysis on the condition that it does not contain multicoloniality, autocorrelation, and heteroscedasticity. Multiple linear analysis is used to determine the influence of independent variables that number more than one dependent variable. $IU = \alpha + \beta 1CSK + \beta 2CSA + \beta 2BP + \varepsilon$

The validity test will use the Pearson correlation which according to (Utami, 2023) if the correlation is less than a value of 0.05, then the question item will be considered valid if it is greater than 0.05, then the question item is considered invalid and must be removed. Reliability will be tested with Cronbach alpha (Utami, 2023) arguing which will test whether the instrument used in this study reliable is or not and will be considered reliable if the test result is greater than 0.60.

Researchers will also conduct hypothesis testing. Hypothesis testing is a test based on sample evidence that is used to examine whether the hypothesis that has been made is a reasonable statement and therefore not rejected, or the hypothesis is unreasonable and therefore rejected. This hypothesis test is useful for examining or testing, whether the regression coefficient obtained is significant or different from real and hypothesis testing. Hypothesis tests include the R2 Test, F test, and T-test.

Using the SPSS program all variables are abbreviated such as:

1. Cyber security knowledge (CSK)
2. Cyber security awareness (CSA)
3. Behavior protection (BP)
4. Intention to use (IU)

The researcher made changes in the construction and measurement of questionnaire questions from sources to adjust to the form of research made by the researcher. The form of the questionnaire construct will be tested with validity and reliability tests to show that the item has been tested.

Results and Discussion

Demographic Respondent

One hundred and thirty-eight (138) respondents who have filled out the questionnaire online through Google *documents* that have been created by the researcher. However, the researcher only took a sample of employees who worked in the Jakarta area, so the researcher set aside 8 respondents who did not work in Jakarta and only used the answers of 130 respondents who worked in Jakarta. The following are the characteristics of the respondents researched by the researcher.

Table 2
Respondent Demographics

Respondent's Character	Frequency	Presented
Gender		
a. Man	86	66,2%
b. Woman	44	33,8%
Total	130	100%
Age		
a. 20-30 Years	126	96,9%
b. 30.1-40 Years	3	2,3%
c. 40.1-50 Years	1	0,7%
Total	130	100%
Education		
a. SMA	2	1,5%
b. D4	1	0,8%
c. S1	112	86,2%
d. S2	15	11,5%
Total	130	100%
Job Type		
a. Self-employed	17	13,1%
b. Employee	111	85,4%
c. Other	2	1,5%
Total	130	100%
Income or allowance for a month		

a. <5 Million	14	10,8%
b. 5.1-15 Million	68	52,3%
c. 15.1-30 Million	39	30.0%
d. 30.1-45 Million	3	2,3%
e. > 45 Million	6	4,6%
Total	130	100%
Length of Use of *Mobile Banking*		
a. 2-3 Years	11	8,5%
b. >4 Years	119	91,5%
Total	130	100%
Frequency of Mobile *Banking Usage*		
a. 1x a week	1	0,8%
b. 2-5x a week	38	29,2%
c. >5x a week	91	70,0%
Total	130	100%
Sumber: *Processed*		

Most of the respondents were male (66.2%), younger than 31 years old (96.9%), educated as S1 (86.2%), working as an employee (85.4%), and earning the most in the range of 5.1 million – 15 million per month (52.3%). It can be concluded from the characteristics in the demographic table of these respondents that the average respondent has a minimum S1 education and an income above 5 million Rupiah with most of them under the age of 31 years. Most of them have been using *mobile banking* for more than 4 years and the frequency of using *mobile banking* is 5x a week, so it can be concluded that according to demographic characteristics, it is appropriate to be used as a respondent.

The most common types of transactions made by respondents when using *mobile banking* are making payments using QRIS (22.2%), the same bank transfers, different banks, and virtual accounts (21.7%), the third checking savings balances, mutations, and deposits (20.2%), and the fourth *e-wallet* top up(19.5%), fifth, payment of credit card bills, internet, telephone, electricity, PDAM, train tickets, BPJS, and insurance (15.7%), and others amounted to (0.7%).

Hypothesis Test Results

Table 3
Uji Hipotesa

IU = α + β1CSK + β2CSA + β2BP + ε							
Variable	**Prediction**	**Unstandardized Coef**		**t**	**Sig**	**Sig/2**	**Decision**
		B	**Std Error**				
(Constant)	+	5,827	1,750	3,330	0,001		
C*yber security knowledge*	+	0,208	0,053	3,882	<0,001	<0,001	H1: Accepted
C*yber security awareness*	+	0,304	0,081	3,761	<0,001	<0,001	H2: Accepted
Behavior protection	+	0,178	0,044	4,036	<0,001	<0,001	H3: Accepted
Adjusted R^2	0,508						
F test	45,311						
F significance	<0,001						
Dependent Variable: Intention to Use							
Sumber: SPSS							

It can be stated that the results of the answers to the tested variable items are declared *valid* because the significance value (Sig/2) is at < 0.05. The model explains that the magnitude of the correlation value of the *output* can be obtained with a determination coefficient (R *Square*) of **0.508** which means that the influence of *independent variables* (cyber security knowledge, cyber security awareness, & behavior protection) on *dependent* variables (*intention to use*) is **50.8%**. It can be explained that *the variable dependent* can be explained by the predictor of 50.8%.

From the table above, it is also explained that the F value is calculated **at 45.311** with a significance level of **0.000<0.05**. It can be stated that the regression model can be used to predict *independent variables* (cyber security knowledge, cyber security awareness, & behavior protection) and *variable dependent* (*intention to use*).

The significance value of the F test in the table explains that the sig value < 0.05, then it can be stated that simultaneously there is an influence between *the independent variable* and the *dependent variable*. In the table above, it is explained that the Constant value is **5.827** while the CSA, CSK, and BP values are 0.208; 0.304; and 0.178 so that the regression equation can be written.

IU = 5.827+0.208+0.304+0.178

This means that every 1% increase in the values of CSK, CSA, and BP also increases by 0.208; 0.304; and 0.178 IU coefficient values. The regression value

coefficient is positive so it can be said that the influence *of the variables* CSK, CSA, and BP on IU is positive.

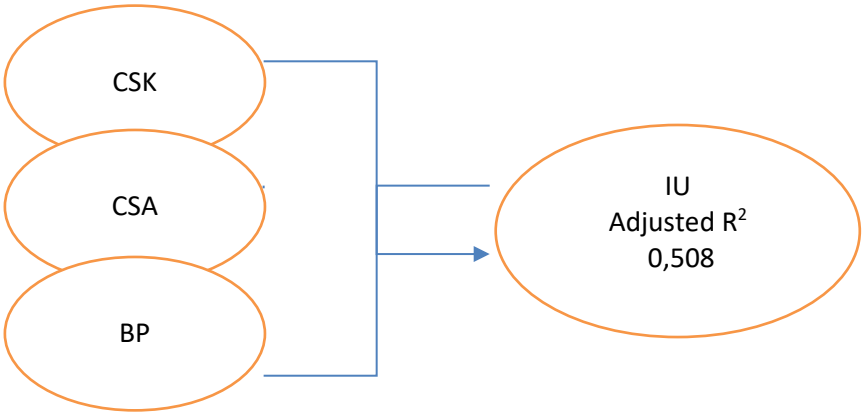

Figure 2
Regression Model Test Results

The regression model and the results of the above test prove that cyber security knowledge, cyber security awareness, & behavior protection have a significant effect on the intention to use. Therefore, H1, H2, and H3 in this study are all supported overall, the relationship phenomenon can be explained by about 50.8% (R2=0.508).

Hypothesis 1: Cybersecurity knowledge has a positive effect on the intention to use mobile banking.

This study shows that cyber security knowledge has a positive effect on the intention to use mobile banking because the results of the t-test < 0.001, the significance value of the t-test in the table shows a < number of 0.05 which is smaller than the standard error of 0.05 and the beta coefficient of 0.053 which indicates that having cyber security knowledge increases the intention to use mobile banking. Knowledge such as having participated in training to maintain online data security, the importance of keeping data from leaking, understanding the importance of using licensed software, proper authentication mechanisms in every mobile banking, and avoiding sharing personal data affect people's intentions to use technology, especially in this case mobile banking.

According to the Diffusion of Innovation (DOI) Theory, humans in general will use something when the use of this innovation is more profitable or beneficial (Feng, 2023), when someone is faced with an innovation around them they may choose to avoid the innovation and reject it, and other people may be open-minded and more willing to adopt the innovation. Users with an open mind and more willing to use innovations are proven to be supported by a deeper knowledge of cybersecurity so that it affects users' interest in continuing to use mobile banking because it can be concluded that the use of mobile banking for people who know about cybersecurity can be felt safe so that mobile banking proves to be useful and profitable because users can transact safely.

The results of this study are in line with research from Bruijin and Janssen (2017) who stated that knowledge about cyber security from IT Infrastructure and types of cyber

attacks allows people to understand and avoid leaking security data from the technology we use so that person's intention to continue to feel safe and use the application appears. The results of this study also support the research of (Limna et al., 2023) that cyber security knowledge can be improved by increasing the perception that not sharing personal information can also minimize security breaches or as a form of action to maintain the security of personal data. The increase in awareness of online transactions, either from oneself or from an application, will increase a person's intention to continue using the application or technology. Human resources and cybersecurity knowledge are the most important factors to achieve technical competence in the field, the cybersecurity competency model, is a form of contextual and high-value information and experience that is ready to be applied to decisions and actions. Wang (2013) proved that the lack of cybersecurity knowledge and a clear understanding of cybersecurity solutions results in reduced protection against phishing, and the potential for leakage of sensitive personal information that causes a person to be reluctant to use the application he or she has to transact.

Hypothesis 2: Cybersecurity awareness has a positive effect on the intention to use mobile banking.

This study shows that cyber security awareness has a positive effect on the intention to use mobile banking because the results of the t-test < 0.001, the significance value of the t-test in the table shows a < number of 0.05, which is smaller than the standard error of 0.05 and the beta coefficient of 0.081. Of course, this states the importance of awareness of maintaining cyber security, always being aware of cyber attacks, guarding when entering passwords, changing passwords regularly, and realizing that before using a mobile banking application, one must know the security techniques in personal mobile banking to be able to increase one's intention to use mobile banking because it is felt that it is the importance of security that determines whether someone will continue to use technology or not.

In other words, this study supports the theory of Planned Behavior (TPB) which explains that subjective norms, behavioral control, and behavioral attitudes can affect a person's intentions (Tian, 2023). So it can be concluded that for users who have cyber security awareness, it has a positive effect on the user's intention to use mobile banking.

This study supports research from (Mamonov & Benbunan-Fich, 2018) that awareness of information security threats increases the protection of behavioral choices, a person's intention to continue using mobile banking is influenced by a person's level of awareness of the importance of cybersecurity. According to Limna et al (2022), promoting and encouraging users to take precautions and train them on online security measures is very important because it can influence a person to or increase their behavior on someone's intention to use and believe in the security of the mobile banking application they use or not. The more mobile phone users are informed about cybersecurity awareness regarding threats, attacks, and cybersecurity protection measures, the better they can make decisions according to So (2013).

Hipotesis 3: Behaviour protection berpengaruh positif terhadap intention to use of mobile banking.

This study shows that cyber security awareness has a positive effect on the intention to use mobile banking because the results of the t-test < 0.001, the significance value of the T-test in the table shows a < number of 0.05 which is smaller than the standard error of 0.05 and the beta coefficient of 0.044 which means that passwords are never shared with others, periodic password changes, The nature of being careful in uploading applications to personal devices, and the use of good antivirus software show good protective behavior and can affect the level of a person's intention to want to use a mobile banking application because they already have protection from within themselves.

In other words, the results of this study are also about behavior protection having a positive effect on supporting the Theory of Planned Behavior (TPB) theory. So it can be concluded that for users who have protective behavior in using the internet, it has a positive effect on the user's intention to use mobile banking.

This research supports the research of (Zhao et al., 2019) which states that it is important for mobile payment companies, as well as merchants, to emphasize technology security features to protect consumer data when promoting mobile banking applications, to maintain security, and avoid data leaks that cause financial losses as well as a person's interest in using the mobile banking application. It also supports the research of Linma et al (2022), which realizes that the precautions and behaviors displayed by internet users are very useful to protect their devices from all cyber attacks, thereby ensuring that the use of safe and convenient applications increases a person's intention to use the mobile banking application. This can be attributed to the application of behavior protection techniques to ensure the security of services and transactions, privacy and data protection are considered top priorities among mobile banking users (Almaiah et al., 2023).

Conclusion

This study proves that cyber security knowledge, cyber security awareness, and behavior protection have a positive effect on the intention to use mobile banking in Jakarta. This research contributes to the existing literature on cyber security knowledge, cyber security awareness, behavior protection, and intention to use, especially for mobile banking applications in Jakarta. Banks need to pay attention to the level of knowledge and awareness of users, and the level of knowledge in marketing their products and services. Increasing user training and knowledge levels can lead to user acceptance and adoption of mobile banking applications. The importance of keeping data from leaking, always being aware of cyberattacks, and showing good protective behavior when using the internet are important things that users pay attention to and must be considered by banks when conducting promotions, especially if their marketing targets are vulnerable users in the age of 20-30. This can be said to be one of the things that users pay attention to if they want to continue using mobile banking applications.

It is also an opportunity and social responsibility for educational institutions to provide more effective cybersecurity programs and courses to increase user knowledge

about cybersecurity risks. The results of this study can also be used to assess how important the security factor is to increasing the frequency of a person's use of mobile banking, of course, if it is used more often, it will also increase the revenue from the bank, which will have a positive impact on the bank's financial statements. Of course, if we increase knowledge, awareness, and user protection behavior, we can support the advancement of the use of technology around us to make human work easier in Indonesia.

The limitation of this research is more specific to areas in Indonesia, namely in Jakarta with a range of age groups that tend to be young (20-30 years old) and are more open to changes and technological developments. The researcher suggested for future research to further increase the number of samples by enlarging the search coverage area, namely throughout Indonesia if possible with a more diverse age group and a more diverse field of work. The researcher also provided advice for banks operating in Jakarta to create a targeted marketing strategy to be able to market mobile banking promotions for the age group of 20-30 years old, it is known that in this study there is a significant positive tendency to continue using their mobile banking application.

Bibliography

Almaiah, Mohammed Amin, Al-Otaibi, Shaha, Shishakly, Rima, Hassan, Lamia, Lutfi, Abdalwali, Alrawad, Mahmoad, Qatawneh, Mohammad, & Alghanam, Orieb Abu. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability*, *15*(13), 9908.

Gao, Jun. (2022). Research on the corporate financial transformation with big data technologies. *International Journal of Progressive Sciences and Technologies*, *32*(2), 8–12.

Limna, Pongsakorn, Kraiwanit, Tanpat, & Siripipattanakul, Sutithep. (2023). The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, *7*, 1133–1151.

Mamonov, Stanislav, & Benbunan-Fich, Raquel. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44.

Rahmawati, Devi, & Sari, Shinta Permata. (n.d.). *Application of the UTAUT 2 Model in the Use of Electronic Wallets*.

Sekaran, Uma, & Bougie, Roger. (2016). *Research methods for business: A skill building approach*. john wiley & sons.

Usman, Teuku Ali. (2022). Analisa model utaut (unified theory of acceptance and use of technology) dalam peningkatan penggunaan layanan transaksi digital Bank Mandiri pada masa pandemi covid-19. *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan*, *4*(9), 4186–4192.

Utami, Yulia. (2023). Uji Validitas dan Uji Reliabilitas Instrument Penilaian Kinerja Dosen. *Jurnal Sains Dan Teknologi*, *4*(2), 21–24.

Venkatesh, Viswanath, Thong, James Y. L., & Xu, Xin. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157–178.

Zhao, Haidong, Anong, Sophia T., & Zhang, Lini. (2019). Understanding the impact of financial incentives on NFC mobile payment adoption: An experimental analysis. *International Journal of Bank Marketing*, *37*(5), 1296–1312.

Zwilling, Moti, Klien, Galit, Lesjak, Dušan, Wiechetek, Łukasz, Cetin, Fatih, & Basim, Hamdullah Nejat. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.