Jurnal Teknologi Informasi dan Pendidikan
Volume 17, No. 1, March 2024
https://doi.org/10.24036/jtip.v17i1.802

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Analysis of Information Security Awareness of E-Commerce Users Among Micro Small Medium Enterprises

Irham Khairul Muttaqin[1*]✉, Syti Sarah Maesaroh[1], Oding Herdiana[1]
[1]Digital Business, Universitas Pendidikan Indonesia, Tasikmalaya, Indonesia
Corresponding Author: irham@upi.edu

Article Information

Article history:

No. 802
Rec. October 10, 2023
Rev. January 18, 2024
Acc. January 18, 2024
Pub. January 30, 2024
Page. 149 – 160

Keywords:

- *Awareness*
- *e-commerce*
- *Business*
- *System Information*
- *Security*

ABSTRACT

Information security is vital in today's digital era. Micro small medium enterprises are always required to survive with the unfavorable conditions. Through e-commerce, businesses can be helped to sell their products widely. Carelessness in managing information in e-commerce applications by business owners can cause great losses. In this article, the information security awareness of micro small medium enterprises will be analyzed using the Knowledge Attitude Behaviour model developed by Kruger-Kearney. The sample of respondents was taken using a purposive sampling technique where the criteria for respondents were categorized micro small medium enterprises owners and using e-commerce applications to sell their products. This article succeeded in analyzing, that the awareness of business owners was in a good category. The resulting score is 93 out of 100 and is considered a high value. There are several factors that cause the high awareness score obtained, one of which is the training held by the state-owned creative house. This article can be developed for further research.

How to Cite:

Muttaqin, I. K., Maesaroh, S. S., & Herdiana, O. (2024). Analysis of Information Security Awareness of E-Commerce Users Among Micro Small Medium Enterprises. Jurnal Teknologi Informasi Dan Pendidikan, 17(1), 149-160. https://doi.org/10.24036/jtip.v17i1.802

1. INTRODUCTION

Security is a vital thing in today's digital era [1]. The rapid development of technology on life components has a huge impact ranging from social, political, security and economic. Security is important today after many attacks on various agencies and companies [2]. One of the business sectors that is growing rapidly is the e-commerce sector. E-commerce itself is an online buying and selling media site that can make it easier for users to make transactions when shopping [3]. In research conducted [4], an increase in the

purchase of goods occurred through e-commerce compared to direct sales (offline). Items sold online slowly increased from 1500 units sold to 2700 units. Meanwhile, offline sales slowly decreased from 3000 units to 2000 units.

In 2021, 88.1% of Indonesian internet users used e-commerce applications to buy the desired items [5]. Competition occurs among others due to homogeneous products and markets [6]. E-commerce applications are an option for businesses to survive. The pressure to continue to innovate in order to survive in fierce competition makes an impetus to turn obstacles into new opportunities [7]. Unpreparedness in preparing for change can cause carelessness which can harm business owners who are included in the MSMEs (Small Medium Enterprises) group [8] who still have limited resources. MSMEs must always maintain the information held in e-commerce applications both in terms of sellers and buyers. Through an article [9], a data leak occurred on Tokopedia amounting 90 million user data. These data include personal information such as population identification numbers, telephone numbers, and home addresses.

Data leaks that occur can harm both parties. Leaked data is often used for criminal purposes or to resell information irresponsibly [10]. As a consequence, consumer confidence in the seller will be damaged and cause a decrease in transactions. MSMEs need to spend a lot of money to bear material losses caused by carelessness. The increasing use of the internet by MSME owners is not accompanied by a strong awareness to protect information security. As many as 29 percent of MSMEs experiencing cyber attacks admit that they do not have adequate information security solutions [11]. This shows that MSMEs that are running lack information in the field of information technology.

A lot of important information is held by e-commerce companies during transactions between merchants and buyers. According to information obtained [12], Indonesian MSMEs have experienced data leaks that are detrimental to business people. Employee data, intellectual and financial information has been leaked. In an article [13], Phishing has become a widely used method when stealing victim data. Unconsciously, important information is lost in an instant. At this time, information can be a measuring tool [14] to predict the future direction of the economy.

In general, owners or employees who have control over the information they hold are not fully aware of the importance of the information they have. Of the 500 MSMEs that have been interviewed [15] show that 8 out of 10 MSMEs do not have careful planning for information security system planning. However, only a small portion of MSMEs have a good approach to information security. Some MSMEs has obtained education related to information security and are aware of their daily activities related to the internet [16]. This suggest that there are some educational initiative or institutions involved in this knowledge enrichment.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

In an article titled "Digital Literacy for the Purwokerto Digital Marketer Community in Efforts to Prevent Data Security Threats in the Cyber World" [16], this research was conducted to increase educational understanding and literacy regarding information security. This education was carried out through Zoom meetings with material regarding cyber crime presented to MSME participants. There is a pre-test and post-test to measure understanding of the material that has been provided. As the outcome, this research produces a significant increase in the participants' understanding.

There are several threats that entrepreneurs should be aware of, one of which is information leakage originating from the employees themselves. Personal and business information can be mixed and cause data leaks from employee carelessness. Social engineering [17] is one way for perpetrators to trick victims in cybercrime. Since the Covid-19 outbreak, the intensity of social engineering attacks has become more frequent. The perpetrator will use all means to make the victim fall into the trap that has been prepared.

In determining the value of information security awareness [18] in a person, there are 3 factors that are the focus of the assesment. There is a knowledge factor which is a set of information used as a measuring tool for someone to recognize threats and how to secure information. Attitude factors also affect a person's behavior and decision-making process in responding to a danger to information security. Behavior is the last factor in determining a person's level of awareness in information security. Behavior is a real action in making a decision. These three factors become the basis for someone to determine the level of information security awareness of e-commerce users.

The more widespread the use of e-commerce, the higher the information security risks that will be faced by MSME owners. Research on this MSME subject has high urgency. MSMEs need to know how important the data they have. The results of this study will also be useful for developers of security systems from e-commerce as well as for academics in developing this topic further, so that knowledge about the awareness of information security of buyers and sellers in e-commerce can continue to grow and be applied in various related fields.

An article with the title of the Analysis of Security Awareness among E-Wallet Users in Indonesia [19]. This research uses the Kruger-Kearney models, which explains the problems of knowledge, behavior, and attitudes in e-wallet users. The security of the e-wallet itself still has several vulnerabilities and the carelessness of users, such as connecting to public Wi-Fi networks or accessing fake sites. This research succeeded in measuring the level of awareness of Indonesian e-wallet users, however this research still cannot guarantee that e-wallet users are precisely determined.

An article with the title of Measurement of Information Security and Privacy Awareness of Android Users in Bandung City [20]. In this article, research uses the Kruger and Kearney models to find out security and privacy related to Android smartphone users. This study succeeded in finding a percentage of the level of awareness, behavior, habits, and knowledge, but this study did not have respondent data in terms of education.

Education itself is vital in influencing knowledge related to information security.

2. RESEARCH METHOD

This research will use a quantitative method where the data will be processed with the KAB (Knowledge Attitude Behaviour) model adapted from the Kruger-Kearney creation model [21]. In this study, the KAB object variables include Knowledge which will measure the level of understanding of MSME owners in securing data in e-commerce applications. Attitude will be measured through the awareness of MSME owners regarding data security in e-commerce. Behavior will be measured by how actions will be taken based on several questions given. The focus areas in this research are Authentication to determine the authenticity of users, passwords to secure account data, and information stored to ensure the security of MSME information. The data will be obtained through a questionnaire survey on Google Form. Questions will be divided into 3 parts based on the KAB model with questions in the following Table 1.

Table 1. KAB model questions

Dimensions	Question	Answer Options
Knowledge	1. Authentication feature is a feature that can strengthen e-commerce account security (finger print, email, SMS) 2. Linking accounts with phone numbers is a measure to prevent account breaches 3. Account authentication is a feature that can help track the location of the account when logging in. 4. It is important to store passwords in a safe place to avoid forgetting passwords. 5. Using a combination of letters, numbers, characters, uppercase and lowercase letters in your password will make your account more secure. 6. Updating passwords regularly will secure your account from harm. 7. Updating your app is one way to keep your account secure 8. Maintaining the confidentiality of information when transacting can avoid unwanted things. 9. By improving information security from unwanted attacks, business reputation will be maintained	True, False, Don't Know
Attitude	1. I realize that authentication can facilitate account access (finger print, email, SMS) 2. I am aware of linking my account with my phone number to avoid account breaches. 3. I am aware that the authentication feature helps to track the location of my account at login time. 4. I am aware of securing my e-commerce account password 5. I realize that using a combination of numbers, characters, uppercase and lowercase letters in my password will make my password stronger. 6. I am aware of updating my password regularly 7. I am conscious of keeping my e-commerce app up to date	True, False, Don't Know

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

	8. I am aware of always maintaining information when a transaction is in progress 9. I am aware of the need to always improve information security to maintain business reputation.	
Behaviour	1. I logged into the app and account using authentication features (finger print, email, SMS) 2. I am used to linking my phone number with my account to avoid account breaches. 3. I always enable the authentication feature to help track my location when logging in. 4. I am used to keeping passwords in a safe place 5. I am used to using passwords with a combination of letters-numbers, characters, uppercase and lowercase letters to secure my account. 6. I am used to updating my passwords to secure my account from any harm. 7. I always update the application version if there is an update notification. 8. I am accustomed to maintaining information when making transactions to avoid unwanted things. 9. I am used to always improving information security at the business	True, False

The data obtained from the questionnaire will be accumulated and processed quantitatively with the total score obtained by all respondents with a value of 10 for the true answer, don't know with a score of 5, and 0 for the false answer.

To be able to determine the level of awareness, weighting will be carried out using the Analytical Hierarchy Process that have been made by Kruger and Kearney [21]. The weight of each score will be different with different scores between 0% - 100%. The percentage distribution will have different weights on each dimension according to the impact that is affected, such as attitude which is smaller than behavior because attitude is an action that is limited to awareness, while behavior is an action that will have a direct effect. The data will be calculated using the Multiple Criteria Decision Analysis formula [22] to determine the weighting value of the dimensions with the score value formula below.

$$V(a) = \sum_{i=1}^{n} v_i(a)\, w_i \quad (1)$$

In this formula, V(a) is an overall value of criterion a, v_i(a) is the score value obtained by the respondent according to the focus area associated with the weighting, and w_i is the weight of a predetermined dimension as the value of knowledge, attitude, and behavior. The division of dimensional weights in the table is as follows:

Table 2. Dimension weight share

Dimension	Weight
Knowledge	30%
Attitude	20%
Behavior	50%

The focus areas in the KAB model have a balanced weight between authentication, passwords, and information stored. These three focus areas have aspects that need to be taken into account to determine the level of information security awareness. The distribution of questions will be shown in the following table:

Table 3. Focus area

Focus Area	Question
Authentication	1, 2, 3
Password	4, 5, 6
Information stored	7, 8, 9

After identification and analysis, the calculation of information security awareness data will be assessed according to the criteria. The percentage value is taken according to the model applied by Kruger-Kearney in the KAB model. The criteria are divided into three parts, good, average, and bad. The percentage value and description of the value can be seen in Table 4 below:

Table 4. Criteria

Criteria	Value (%)	Description
Good	80-100	Already good, no action needed
Average	60-79	Good enough, still needs improvement
Bad	<59	Poor, need to improve

This survey is targeted at MSME owners who use e-commerce applications such as Tokopedia, Lazada, Shopee, and other applications. The E-Commerce application is the most used application in Indonesia [23]. The survey will be conducted using purposive sampling technique [24] which is distributed to 71 MSME owners who also sell on e-commerce applications. The data of 71 respondents is a number that has been validated using Criterion Validity where the validity of the data must be in accordance with predetermined criteria such as having an MSME business and selling their own product on e-commerce applications. Furthermore, the survey results will be calculated using the KAB model which has been adapted to display the results of MSME information security awareness.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

3. RESULTS AND DISCUSSION

MSME owners who participated in this study have filled out the questionnaire provided. The characteristics of the respondents will be displayed in accordance with the predetermined criteria. The data will be presented in tabular form to provide an overview of the respondents' contributions in the following table:

Table 5. Characteristics

Gender	Total	Percentage
Men	26	37%
Women	45	63%
Age		
18-30	46	65%
>30	25	35%
Education		
Junior high school / equivalent	1	1%
High school / equivalent	28	39%
Bachelor's Degree / equivalent	39	55%
Master's Degree / equivalent	3	4%
Revenue		
< Rp2 Billion	68	96%
>Rp2 Billion-Rp15 Billion	3	4%
Device		
Android	53	75%
IOS	18	25%

The characteristics table shows information about the gender of respondents, 37% of whom are men while 63% are women. This happens because one of the factors is that men work as employees in companies, while women tend to have free time and choose to run small businesses which will later develop into MSMEs. This is supported by the article [25] which states that the MSME field is strongly influenced by women.

In the age aspect, the range of 18 years to 30 years dominates at 65%. The use of technology greatly affects the motivation and adaptability of respondents in running a business with the role of technology. Meanwhile, the age of respondents above 30 has a

percentage of 35%. In this age range there are fewer with a difference of 21, compared to the age range 18-30 which amounts to 46 because it takes time and energy to relearn the use of technology and the difficulty of adapting if the e-commerce application changes.

Characteristics in the education aspect have a diverse range, in the junior high school / equivalent education range there is one respondent with a percentage of 1% who is at this level of education. This is not a barrier to running MSMEs because running a business does not require a minimum education limit. At the high school / equivalent level has a percentage of 39% with 28 respondents. Meanwhile, the number of respondents with bachelor's / equivalent education has a higher percentage, namely 55% with 39 respondents. At the bachelor / equivalent level, MSME owners already have a mature level of education. The highest level of education for respondents is master's degree with a small number, namely 4% with 3 respondents. The master's degree education level has a small number of respondents due to the difficulty of access to this education and career choices at this level tend to be in the professional field.

In terms of income, there is a big difference where income of less than 2 billion has a response of 96% with 68 respondents while the range of 2 billion to 15 billion has 3 respondents or the equivalent of 4%. The use of devices in MSMEs is android with a percentage of 75% with 53 respondents. For IOS devices, there are 18 respondents with a percentage of only 25%.

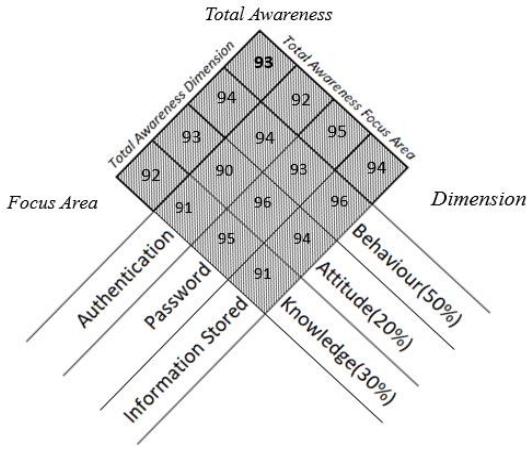

Figure 1. Awareness result

The result from Figure 1 above conducted with the KAB model resulted in a percentage of the total awareness value of 93 out of 100, which means that MSMEs are already aware of information security in the business being run. In the total awareness dimension, the knowledge dimension, the total awareness dimension value has a value of 92, where authentication has a value of 91, password 95, and information storage 91. In the

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

attitude dimension, the total awareness dimension value is 93 with an authentication value of 90, password 96, and information stored 94. In the behavior dimension, the total value of the Awareness dimension is 94 with authentication having a value of 94, password 93, and information stored 96.

In the total value of awareness focus area, the information stored area has a value of 94, while in the password section it has a value of 95, and in the authentication focus area it has a value of 92. The total value obtained in the focus areas and dimensions will be calculated with the appropriate weighting in each dimension where knowledge has a weight of 30%, attitude has a weight of 20%, and behavior has a weight of 50%. The number obtained after the calculation is 93, which is the value of the information security awareness of e-commerce users among MSMEs is good.

With the high number obtained in the total KAB awareness score, this shows that MSMEs have a good level of understanding. An understanding of the importance of security in business has been able to be applied well by MSME owners. The high value of information security awareness is partly supported by trainings agencies conducted by state-owned companies (BUMN) in the BUMN Creative House program. This is explained by the article on the readiness of MSMEs in using e-commerce applications as a supporting medium for developing the creative industry [26]. MSMEs are ready to use e-commerce applications to develop their business. The value in the attitude dimension authentication focus area gets a low score among other focus areas, but the value at this point is in the good criteria.

Having a low understanding of passwords is not necessarily a negative thing compared to other values in this focus area. However, it is better if the authentication focus area in the attitude dimension can be further improved so that MSME owners can maximize the security potential of e-commerce applications. To improve attitude in the authentication focus area can be done by increasing literacy [27], [28] regarding information security such as passwords, access authorization, and security so that MSME owners can be more aware of information security. This value is a high value and has a low risk compared to a value that has poor criteria.

The highest score is obtained by the attitude dimension password focus area and the behavior dimension information stored focus area with a score of 96. MSME owners already have an attitude about a good understanding of passwords in e-commerce applications. Passwords are vital to e-commerce devices and applications in supporting information security. MSME owners already have a good understanding, although there are 4% of MSME owners who do not understand well about passwords in the attitude dimension.

Information stored has been carried out properly by MSME owners in e-commerce applications which are useful for preventing and avoiding application vulnerabilities from cyber attacks and phishing [12]. MSMEs training conducted by training institutions always teaches MSME owners to be aware of maintaining confidential MSMEs information for the

continuity of the business being undertaken.

4. CONCLUSION

This study shows the results that MSME owners are already aware of information security awareness in the use of e-commerce applications. The total awareness value shows a value of 93 out of 100, which is good in this category. Thus, MSME owners are already aware of the importance of information security in MSMEs. This value is expected for MSME owners to maintain consistency in securing their business information. From Table 5 characteristics, the level of education does not really affect the level of understanding of information security. However, Additional research is necessary to determine the appropriate subjects for discussing the educational backgrounds of MSME owners.

For academics, institutions, and training agencies, the results of the scores obtained by MSMEs show the participants' success during the training. The training agencies must continue to conduct training related to information security awareness for MSME owners. Further training can be developed on authentication awareness. Relationships with MSMEs and training agencies need to be well maintained to guide and assist MSMEs' future decisions.

This article serves as a for future researchers, providing valuable insights into the characteristics of MSME owners and their awareness of information security. The following research can explore these aspects in greater detail and other aspects, focusing on specific regions or expanding the scope to cover a broader range of variables and focus areas. By building upon the foundations of this study, future research can contribute significantly to the understanding of information security awareness among MSMEs and enhance the overall knowledge in this field.

REFERENCES

[1] S. Destya, "Pengukuran Tingkat Kesadaran Keamanan Informasi Berdasarkan Behavior Dan Offence Scale," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 2, p. 236, 2020, doi: 10.24114/cess.v5i2.18206.

[2] Makbull Rizki, "Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi," *Polit. J. Ilmu Polit.*, vol. 14, no. 1, pp. 54–62, 2022, doi: 10.32734/politeia.v14i1.6351.

[3] R. L. Batu, T. L. Situngkir, I. Krisnawati, and S. Halim, "Pengaruh Digital Marketing Terhadap Online Purchase Decision Pada Platform Belanja Online Shopee," *Ekon. Bisnis*, vol. 18, no. 2, pp. 144–152, Jan. 2020, doi: 10.32722/eb.v18i2.2495.

[4] N. R. Fauzi and K. Sisilia, "Analisis Perbandingan Keputusan Pembelian Online Dan Offline Customer Pada or-K 689 Clothing," *J. Menara Ekon. Penelit. dan Kaji. Ilm. Bid. Ekon.*, vol. 6, no. 2, 2020, doi: 10.31869/me.v6i2.1812.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

[5] Andrea Lidwina, "Penggunaan E-Commerce Indonesia Tertinggi di Dunia," *Databooks*, 2021. https://databoks.katadata.co.id/datapublish/2021/06/04/penggunaan-e-commerce-indonesia-tertinggi-di-dunia (accessed Feb. 21, 2023).
[6] S. Maesaroh, A. Hermawan, and A. Fauziyah, "Analisis Faktor Penentu Daya Saing Umkm Batik," *Conf. Innov. Appl. Sci. Technol. (CIASTECH 2020)*, no. Ciastech, pp. 69–76, 2020.
[7] Yenita Lisna, "Tantangan Umkm Indonesia Di Masa Pandemi Covid-19," *BI Institute*, 2022. https://www.bi.go.id/id/bi-institute/BI-Epsilon/Pages/Tantangan-UMKM-Indonesia-di-Masa-Pandemi-Covid-19.aspx (accessed Feb. 21, 2023).
[8] A. Sani, N. Wiliani, A. Budiyantara, and N. Nawaningtyas, "Pengembangan Model Adopsi Teknologi Informasi Terhadap Model Penerimaan Teknologi Diantara Umkm," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 5, no. 2, pp. 151–158, 2020, doi: 10.33480/jitk.v5i2.1055.
[9] Wahyu Isnaini, "Literasi Digital Bagi Komunitas Digital Marketer Purwokerto Dalam Upaya Mencegah Ancaman Keamanan Data Di Dunia Siber," vol. 6, pp. 1795–1801, 2022.
[10] N. P. N. Suharyanti and N. K. Sutrisno, "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat," *Pros. Semin. Nas. Fak. Huk. Univ. Mahasaraswati Denpasar 2020*, vol. 1, no. 1, pp. 119–134, 2021, [Online]. Available: http://e-journal.unmas.ac.id/index.php/psnfh/article/view/2395
[11] I. R. Putranti, A. Amaliyah, and R. Windiani, "Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah," *J. Ketahanan Nas.*, vol. 26, no. 3, p. 359, 2020, doi: 10.22146/jkn.57322.
[12] S. Fitra, "60 Persen UKM Indonesia Mengalami Pencurian Data Pelanggan," *Katadata.co.id*, 2021. https://katadata.co.id/safrezifitra/digital/6174dde63e877/60-persen-ukm-indonesia-mengalami-pencurian-data-pelanggan (accessed Mar. 24, 2023).
[13] V. F. Putra Y, "Modus Operandi Tindak Pidana Phising Menurut UU ITE," *Jurist-Diction*, vol. 4, no. 6, 2021, doi: 10.20473/jd.v4i6.31857.
[14] K. Osei Bonsu, "Turbulence On The Global Economy Influenced By Artificial Intelligence And Foreign Policy Inefficeincies," *J. Lib. Int. Aff. Inst. Res. Eur. Stud. - Bitola*, vol. 2, pp. 113–122, 2020, doi: 10.47305/jlia2020113ob.
[15] E. Sumirih, D. Rahmawati, M. S. Staf, P. Jurursan, P. A. Universitas, and N. Yogyakarta, "Persepsi Umkm Kota Yogyakarta Mengenai Fraud Teknologi Informasi," *J. Profita Kaji. Ilmu Akunt.*, no. 3, 2020, [Online]. Available: https://journal.student.uny.ac.id/ojs/index.php/profita/article/view/16870
[16] Wahyu Isnaini, "Literasi Digital Bagi Komunitas Digital Marketer Purwokerto Dalam Upaya Mencegah Ancaman Keamanan Data Di Dunia Siber," vol. 6, pp. 1795–1801, 2022.
[17] E. W. Tyas Darmaningrat et al., "Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi," Sewagati, vol. 6, no. 2, 2022, doi: 10.12962/j26139960.v6i2.92.
[18] L. Jessica, "IT Security Awareness Best Practices," *Budi Rahardjo - Makal. Secur.*, pp. 7–8, 2020.
[19] M. S. Alif and A. R. Pratama, "Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia," *J. Inf.*, vol. 2, no. 1, pp. 1–7, 2021, [Online]. Available: https://journal.uii.ac.id/Automata/article/view/17279
[20] A. A. Pratama, I. M. Ghufron, J. Ma'ruf, S. Hanafi, A. Hafidh, and Anas, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Android Di Kota Bandung," *J. TIMES*, vol. 9, no. 2, pp. 1–8, 2022, doi: 10.21456/vol8iss2pp115-122.
[21] H. A. Kruger and W. D. Kearney, "A Prototype For Assessing Information Security Awareness,"

Comput. Secur., vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.

[22] V. Belton and T. Stewart, "Multiple Criteria Decision Analysis: An Integrated Approach," 2002, [Online]. Available: http://books.google.es/books?hl=es&lr=&id=mxNsRnNkL1AC&oi=fnd&pg=PR11&dq=belton+stewart&ots=DJNvNOBuDF&sig=8hQyPT3RD5UzaLT0uzE7XL-WGCQ

[23] V. A. Dihni, "10 E-Commerce dengan Pengunjung Terbanyak Kuartal I 2022," *Databooks*, 2022. https://databoks.katadata.co.id/datapublish/2022/07/19/10-e-commerce-dengan-pengunjung-terbanyak-kuartal-i-2022

[24] I. Lenaini, "Teknik Pengambilan Sampel Purposive Dan Snowball Sampling," *J. Kajian, Penelit. Pengemb. Pendidik. Sej.*, vol. 6, no. 1, pp. 33–39, 2021, [Online]. Available: p-ISSN 2549-7332 %7C e-ISSN 2614-1167%0D

[25] F. M. A. Hasugian and L. Panggabean, "Peran Perempuan dalam Mengembangkan Usaha Mikro Kecil dan Menengah dalam rangka menuju Masyarakat Ekonomi ASEAN di Kota Tangerang Selatan," *J. Ina. Kaji. Peremp. Indones. di Drh. Tertinggal, Terdepan, dan Terluar*, vol. 2, no. 2, pp. 111–135, 2020, doi: 10.33541/ji.v2i2.1359.

[26] R. Gunanta and N. Hadian, "18 Imperative E –Commerce:Analisis Kesiapan Pelaku UMKM Kota Bandung Dalam Mengembangkan Industri Kreatif Digital," *J. Akunt. Maranatha*, vol. 11, no. 1, pp. 187–198, 2019, doi: 10.28932/jam.v11i1.1550.

[27] D. Revilia and N. Irwansyah, "Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness," *J. Penelit. Komun. Dan Opini Publik*, vol. 24, no. 1, pp. 1–15, 2020, doi: 10.33299/jpkop.24.1.2375.

[28] O. Herdiana, N. M. Aprily, and L. P. On, "Pelatihan Skill Literasi Digital dalam Pengelolaan Data bagi Pelaku Usaha UMKM," *J. Abdimas Ekon. dan Bisnis*, vol. 2, no. 2, pp. 86–95, 2022, doi: 10.31294/abdiekbis.v2i2.1432.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id