

DIGITAL FRAUD PREVENTION EDUCATION FOR MSMEs IN ONLINE TRADING ACTIVITIES IN BATAM CITY

Fadlan^{1*}, E. Arinda Chikita², Ika Novita Sari³

^{1,3}Universitas Batam, Batam Kota, Indonesia

²Universitas Internasional Batam, Batam Kota, Indonesia

*email (fadlan@univbatam.ac.id)

Received: 01/02/2026 | Revised: 20/02/2026 | Accepted: 10/03/2026 | Published: 30/03/2026

Abstract

The development of online commerce provides opportunities for Micro, Small, and Medium Enterprises (MSMEs) to expand their markets, increase sales, and reach consumers without geographical boundaries. However, the increase in digital commerce activity is also accompanied by various risks of digital fraud, such as phishing, payment manipulation, fake accounts, malicious links, and data theft. MSMEs play a crucial role in the digital commerce ecosystem because they not only act as sellers but also as managers of accounts, customer data, transaction communications, and payments. This Community Service (PkM) activity aims to increase the knowledge and awareness of MSMEs in Batam City in recognizing and preventing digital fraud in online commerce activities. The activity was carried out through lectures, discussions, and simulations of digital fraud cases involving 30 MSMEs. Evaluation was carried out using pre-test and post-test questionnaires consisting of 20 multiple-choice questions. The results showed an increase in participants' knowledge after being provided with education. The average score increased from 58.4 ± 12.6 in the pre-test to 84.7 ± 9.3 in the post-test, or an increase of 26.3 points. The proportion of participants with good knowledge increased from 13.3% to 63.3%, while the proportion with poor knowledge decreased from 46.7% to 6.7%. The Wilcoxon Signed Rank test showed $p < 0.001$, indicating a statistically significant increase in knowledge after the education. Satisfaction evaluation also showed a positive response with an average score of 4.0–4.7. This activity demonstrates that education combined with discussions and case simulations can be an effective strategy to improve digital fraud prevention literacy for MSMEs.

Keywords: MSMEs, digital fraud, online trading, digital literacy, cybersecurity, Batam City

1. INTRODUCTION

Digital transformation has changed the pattern of trade in society, including business activities carried out by Micro, Small, and Medium Enterprises (MSMEs). The use of marketplaces, social media, instant messaging applications, and digital payment systems allows MSMEs to conduct promotions and transactions more quickly, flexibly, and efficiently. Trading through electronic systems also provides opportunities for business actors to expand consumer reach, increase market access, and develop business models that are no longer limited by space and time (OECD 2016). These developments indicate that the use of digital technology has become an important part of modern economic and trade activities. The Central Bureau of Statistics has also specifically developed e-commerce statistics that cover business profiles, worker characteristics, business activities, and the value of electronic commerce transactions in Indonesia (Central Bureau of Statistics (BPS) 2025).

Batam City is characterized as a growing trade, industry, and service area and holds a strategic position in regional economic activity. The development of various economic activities in Batam City is reflected in the publications of the Batam City Central Statistics Agency, which regularly present developments in various business fields in the region (Batam City Central Statistics Agency 2025). This condition also supports the development of digital-based trading activities among MSMEs. The use of digital platforms is an alternative for businesses to market products, communicate with consumers, accept payments, and manage transactions more practically.

On the other hand, the increasing use of digital technology also presents new risks for businesses. MSMEs can be targets of various forms of digital fraud, such as fake messages, phishing, fake marketplace accounts, payment receipt manipulation, malicious links, identity theft, and account credential theft. These risks are further complicated by the use of social engineering techniques to manipulate victims into believing that communications are from consumers, marketplace platforms, financial institutions, or other legitimate parties. Phishing essentially exploits the manipulation of messages and the identity of the communication source to obtain information, account access, or

financial gain from victims (Yudhiyati et al., 2024). Research (Yudhiyati, Rahmawati, and Putritama 2024) shows that the increasing reliance of MSMEs on internet-based services can increase their vulnerability to spear-phishing attacks. The study also highlights the importance of MSMEs' ability to recognize the characteristics of phishing messages as part of cyberattack prevention efforts. Users' ability to identify suspicious messages is becoming increasingly important because prevention technology cannot always replace users' role as decision-makers when receiving digital communications. The risk of digital fraud is not only related to financial losses, but can also impact data security and consumer trust. In e-commerce, trust is a crucial factor because consumers and businesses conduct transactions without always meeting face-to-face. The OECD emphasizes the importance of consumer protection in e-commerce, including information transparency, payment protection, data security and privacy, consumer education, and dispute resolution mechanisms (OECD 2016). Therefore, digital transaction security is not only a technical issue, but also part of consumer protection and the sustainability of the relationship between businesses and consumers.

In the context of Indonesian law, electronic commerce is regulated, among other things, through Government Regulation Number 80 of 2019 concerning Electronic Commerce. This regulation provides a framework for the implementation of electronic commerce and emphasizes that electronic commerce must be conducted legally, honestly, and with due regard for consumer rights protection. Government Regulation Number 80 of 2019 also places clarity of information as a crucial aspect in electronic transactions, both before, during, and after the transaction (Government Regulation of the Republic of Indonesia 2019).

Beyond transactional aspects, personal data protection is a crucial part of digital commerce activities. Law Number 27 of 2022 concerning Personal Data Protection provides the legal basis for personal data protection, including the rights of personal data subjects, the processing of personal data, and the obligations of parties processing data. In online commerce, MSMEs have the potential to manage various consumer information, such as names, telephone numbers, shipping addresses, and transaction information (Government of the Republic of Indonesia 2022). Therefore, understanding personal data security and management is a crucial part of MSME digital literacy. The electronic transaction aspect is also related to Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. This regulation serves as one of the legal bases for conducting electronic information and transaction activities in Indonesia. (Republic of Indonesia 2024). Meanwhile, consumer protection in trade activities remains based on Law Number 8 of 1999 concerning Consumer Protection, which regulates various aspects of consumer protection in the relationship between consumers and business actors (Republic of Indonesia 1999).

The issue of digital fraud is becoming increasingly important because technological security depends not only on the systems used but also on users' ability to recognize and respond to risks. MSMEs, as direct users of marketplaces, social media, instant messaging applications, and digital payment systems, need basic skills to recognize suspicious transactions, verify information, maintain the confidentiality of credentials, and secure business and consumer data. Therefore, increasing digital literacy and cybersecurity awareness among MSMEs is an important preventative measure (Yudhiyati et al. 2024). This issue becomes even more relevant based on the initial identification results from this Community Service (PkM) activity. Of the 30 MSME participants, 11 (36.7%) stated they had experienced digital fraud, while 19 (63.3%) had not. This data indicates that digital fraud is a real risk in online commerce and requires attention through preventative education.

Based on these conditions, this Community Service (PkM) activity was implemented to provide education on digital fraud prevention to MSMEs in online trading activities in Batam City. The activity was designed not only in the form of lectures, but also through discussions and simulations of digital fraud cases. This approach was chosen so that participants not only gain theoretical knowledge but also can recognize fraud methods through situations close to everyday business activities. The use of examples and simulations is expected to help participants understand the characteristics of suspicious messages, payment manipulation, requests for confidential information, and other forms of social engineering. Thus, the goal of this activity is to increase MSMEs' knowledge of the forms of digital fraud, improve their ability to recognize indicators of suspicious transactions, increase caution in managing accounts and data, and enhance participants' ability to take preventive measures when facing suspected digital fraud. More broadly, this activity is expected to contribute to the development of safer, more responsible online trading behavior that aligns with the principles of consumer protection and data security.

2. IMPLEMENTATION METHOD

Activity Design

The Community Service Program (PKM) uses an educational-participatory approach. This approach was chosen so that participants not only gain theoretical information but also actively participate in identifying and

analyzing examples of digital fraud that could potentially occur in online trading activities. The event took place at the Sub-district Meeting Hall in Batam City, with 30 MSME participants. The event's stages included:

- Identify participant characteristics and experiences;
- Implementation of pre-test;
- Delivery of educational materials;
- Discussion and Q&A;
- Simulation of digital fraud cases;
- Implementation of the post-test;
- Evaluation of participant satisfaction.

Educational Materials

The educational material covers several main topics, namely:

- Definition and characteristics of digital fraud;
- Types of fraud that often target MSMEs;
- Phishing and social engineering;
- Fake accounts and fake consumer identities;
- Manipulation of transfer evidence;
- Malicious links and files;
- Theft of usernames, passwords, OTPs, and sensitive information;
- Security of marketplace and social media accounts;
- Customer data protection;
- Steps to take when fraud is suspected;
- The importance of keeping evidence of electronic transactions;
- Legal aspects related to digital transactions.

The legal material is linked to Law Number 8 of 1999 concerning Consumer Protection, Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems.

Educational Methods

The methods used consisted of three main forms. First, a lecture. The resource person explained the concept of digital fraud, the characteristics of fraudulent methods, and preventative measures. Second, a discussion. Participants were given the opportunity to share their experiences, challenges, and questions related to online transaction security. Third, a case simulation. Participants were given examples of cases such as messages impersonating marketplaces, requests for OTP codes, fake payment receipts, and links directing users to fake login pages. Participants were then asked to determine whether these cases were normal transactions or indications of fraud.

Instrument

Knowledge assessment was conducted using a 20-question multiple-choice questionnaire. A pre-test was administered before the educational material, while a post-test was administered after the entire educational series and simulation were completed.

Knowledge is categorized into:

Less: score ≤ 60

Fair: score 61–80

Good: score > 80

Evaluation

Data were analyzed descriptively using frequency distribution, percentage, mean, standard deviation, median, and minimum-maximum values. Differences in scores before and after education were analyzed using the Wilcoxon Signed Rank Test because the data were compared on the same participants before and after the intervention. The statistical significance level was set at $\alpha = 0.05$.

3. RESULTS AND DISCUSSION

Participant Characteristics

The event was attended by 30 MSMEs. Participant characteristics included gender, age, education, length of online business experience, primary platform used, and experience with digital fraud.

Table 1. Characteristics of Community Service Activity Participants (n=30)

Characteristics	Category	n	%
Gender	Woman	21	70.0
	Man	9	30.0
Age	20–30 years	8	26.7
	31–40 years	14	46.7
	41–50 years	8	26.7
last education	High school/equivalent	17	56.7
	Diploma/Bachelor's Degree	13	43.3
Length of online business	<1 year	9	30.0
	1–3 years	15	50.0
	>3 years	6	20.0
Main platform	Marketplace	18	60.0
	Social media	12	40.0
Have you ever experienced digital fraud?	Yes	11	36.7
	No	19	63.3

The majority of participants were female (70.0%), aged 31–40 years (46.7%), had a high school education or equivalent (56.7%), and had run an online business for 1–3 years (50.0%). A total of 36.7% of participants had experienced digital fraud.

Changes in Knowledge Before and After Education

The results of the evaluation of participants' knowledge before and after the activity are presented in Table 2.

Table 2. Distribution of Participants' Knowledge Categories Before and After Education

Knowledge Category	Pre-test		Post-test	
	n	%	n	%
Less (≤ 60)	14	46.7	2	6.7
Enough (61–80)	12	40.0	9	30.0
Good (> 80)	4	13.3	19	63.3
Total	30	100	30	100

There was an increase in knowledge after education, indicated by an increase in the good category from 13.3% to 63.3% and a decrease in the less than good category from 46.7% to 6.7%.

Comparison of Pre-test and Post-test Knowledge Scores

Table 3. Statistics of Participants' Knowledge Scores

Statistics	Pre-test	Post-test
Mean $\pm$ SD	58.4 $\pm$ 12.6	84.7 $\pm$ 9.3
Median	60	85
Minimum–Maximum	35–85	60–100

The mean knowledge score increased from 58.4 ± 12.6 to 84.7 ± 9.3 , with an increase of 26.3 points after education.

Wilcoxon Signed Rank Test Results

Table 4. Results of the Knowledge Score Difference Test

Variables	Pre-test	Post-test	Statistical Test	p-value
Digital fraud prevention knowledge	58.4 ± 12.6	84.7 ± 9.3	Wilcoxon Signed Rank Test	<0.001

The Wilcoxon test showed a significant increase in knowledge after education with a p value < 0.001.

Participant Satisfaction Evaluation

In addition to measuring increased knowledge, the activity also evaluates participants' perceptions of the implementation of the activity.

Table 5. Participant Satisfaction Evaluation

Rated aspect	Average Score	Category
Clarity of material	4.5	Very satisfied
Resource person's ability	4.6	Very satisfied
Material benefits for business	4.7	Very satisfied
Availability of discussion/question and answer time	4.2	Satisfied
Suitability of place and facilities	4.0	Satisfied

Participants gave a positive assessment of the activity with an average score of 4.0–4.7; the highest score was for the aspect of material benefits for the business (4.7).

4. DISCUSSION

The results of the activity showed an increase in knowledge of MSME actors after being given education on digital fraud prevention. The average knowledge score increased from 58.4 ± 12.6 in the *pre-test* to 84.7 ± 9.3 in the *post-test*, or an increase of 26.3 points. The results of the *Wilcoxon Signed Rank test* showed a p-value < 0.001, so there was a statistically significant difference in knowledge between before and after the educational activity. This increase was also seen from changes in the knowledge category, namely participants with the good category increased from 13.3% to 63.3%, while the poor category decreased from 46.7% to 6.7%. These findings indicate that education provided through lectures, discussions, and case simulations was able to increase participants' knowledge about the forms and prevention of digital fraud.

This increase in knowledge aligns with the findings of Prümmer et al. (2025), who, through a meta-analysis of 69 studies, found that cybersecurity training generally has a positive effect on users, particularly on knowledge and attitudes. The effects of training on knowledge and behavioral predictors were reported to be stronger than the direct effect on behavioral change (Prümmer, van Steen, and van den Berg 2025). These findings are relevant to the results of this activity because the main indicator measured was changes in knowledge through *pre-* and *post-tests*. Therefore, the increase in participants' scores can be seen as an early indicator of the success of education in increasing knowledge capacity regarding digital transaction security.

The change in knowledge category distribution during this activity also indicates that the education provided benefits, particularly for participants with low prior knowledge. Before the education, nearly half of the participants were in the poor category, while after the education, the majority were in the good category. This demonstrates that the material provided was able to reduce the knowledge gap among participants. These results are important because the ability to recognize digital threats is a key component in technology-based fraud prevention.

(Yudhiyati et al. 2024) specifically demonstrated that MSMEs in Indonesia face vulnerability to *phishing* due to their increasing reliance on internet-based services. The study also developed an instrument to measure MSME owners' ability to distinguish between *phishing* and legitimate messages and emphasized that the measurement results can be used as a basis for developing training materials and *phishing prevention guidelines*. These findings reinforce

the relevance of this Community Service Program (PKM) activity because the education provided relates not only to technological security but also to users' ability to recognize and respond to suspicious digital communications.

The lecture, discussion, and case simulation methods used in this activity are also relevant to the development of cybersecurity education approaches. (Bada and Nurse 2019) emphasize that cybersecurity education and *awareness programs* for MSMEs need to be structured and consider the real-world needs and conditions of small and medium-sized businesses. Cybersecurity education should not only provide information about threats but also help MSMEs understand how to protect the data and services used in business activities.

The use of case simulations in this activity is crucial because digital fraud often exploits the human factor through social engineering techniques. Perpetrators can impersonate consumers, marketplaces, financial institutions, or other parties deemed trustworthy. (Yudhiyati et al. 2024) explain that *phishing* uses message manipulation and social engineering to trick recipients into believing the communication comes from a legitimate source. If victims follow these instructions, the perpetrators can obtain information, identities, account access, or commit financial fraud. Therefore, education for MSMEs needs to be directed at practical skills such as pausing, checking, verifying, and making careful decisions before responding to digital communications.

The finding that 11 participants (36.7%) had experienced digital fraud also provides important context for the need for educational programs. This data demonstrates that digital fraud is not just a potential threat, but has been a real-life experience for some participants. This reinforces the importance of improving digital security literacy among MSMEs. However, based on the available data, no analysis has been conducted to determine the difference in scores between participants who have experienced fraud and those who have not. Therefore, this study cannot conclude that fraud experience is associated with a significant increase in knowledge.

These findings can also be seen in research (Rochmadi et al. 2026) on MSMEs' information security awareness of *phishing* via WhatsApp. The study of 24 MSMEs showed that although most respondents were familiar with the term *phishing*, their ability to recognize its signs and understand basic response steps was still low. These results indicate a gap between awareness of threats and the ability to recognize and handle them. This situation reinforces the importance of educational activities that not only provide definitions of digital fraud but also use examples and simulations relevant to business activities.

The need to improve cybersecurity capacity in MSMEs is also supported by research on the cybersecurity preparedness of small and medium-sized businesses. A 2024 study on *cybersecurity preparedness in small-to-medium businesses* showed that threat awareness, implementation of security practices, and access to support and guidance are critical aspects of MSME cybersecurity preparedness (Chidukwani, Zander, and Koutsakis 2024). Therefore, education provided to MSMEs can be a form of *capacity building* to strengthen their readiness to face digital risks.

In the context of online commerce, increasing digital security knowledge is also linked to consumer trust. MSMEs are not only responsible for the security of their own accounts and transactions, but also for interacting with consumers and managing information related to these transactions. Therefore, digital security is an integral part of service quality in e-commerce. Protection of payments, personal data, information transparency, and dispute resolution mechanisms are crucial aspects of building trust in e-commerce. This aligns with the OECD recommendations on consumer protection in e-commerce.

The characteristics of the platforms used by participants indicate that 18 (60.0%) used marketplaces, while 12 (40.0%) used social media as their primary trading platform. This situation indicates that MSMEs face a diverse digital environment. Marketplace users may face risks such as fake accounts, communications impersonating the platform, payment information manipulation, and links that direct users to fake pages. Meanwhile, social media users may face risks of identity impersonation, *phishing*, malicious links, and requests for personal information or account credentials.

These findings suggest that digital security education should not be delivered in a single format for all MSMEs. Materials should consider the platforms used, transaction patterns, types of communication with consumers, and the type of information managed by the business. Bada and Nurse (2019) also emphasize the importance of developing cybersecurity education programs tailored to the characteristics and needs of MSMEs. However, this activity did not analyze knowledge gains based on platform, so it cannot be determined whether marketplace and social media users experienced different levels of knowledge gains.

Participant satisfaction evaluations showed a positive response to the activity. The material benefits for businesses received the highest score of 4.7, followed by resource person skills at 4.6 and material clarity at 4.5. These results indicate that the educational material was perceived as relevant to participants' needs in conducting online trading activities. The high assessment of material benefits also demonstrates that digital fraud prevention is a practical necessity for MSMEs.

Meanwhile, the availability of discussion time and Q&A sessions scored 4.2, while the suitability of the venue and facilities scored 4.0. While still in the satisfactory category, these results can serve as input for future activities. Discussion time could be extended and simulation facilities could be improved to provide participants with more opportunities to practice identifying suspicious messages, checking links, verifying payments, and securing accounts. While the knowledge gains from this activity were substantial, these results should be interpreted with caution. Improved *post-test scores* demonstrate the success of education in increasing short-term knowledge, but do not directly demonstrate sustained long-term behavioral change. This is consistent with findings (Prümmer et al. 2025), which suggest that the effects of cybersecurity training are stronger on knowledge and attitudes than on actual behavioral change. This meta-analysis found an overall positive effect of training, but the effect on behavioral change was relatively smaller and did not demonstrate the same robustness.

Similar things were also found in *the scoping review*. (Marshall, Sturman, and Auton 2024) reviewed 42 studies on *phishing training*. The review showed that the short-term impact of training was quite consistent, but evidence of sustained long-term behavioral changes was limited. The research also showed that active engagement, repeated practice, and feedback can enhance training effectiveness. These findings support the use of case simulations in this PkM activity and indicate the need for follow-up activities to strengthen educational outcomes.

Thus, educational activities should not stop at a single presentation. Subsequent programs can be supplemented with regular *phishing simulations*, *account security practices*, *the use of two-factor authentication*, *password management*, payment verification, and customer data protection. A repetitive, practice-based approach can help participants retain knowledge and improve their ability to recognize digital threats. This aligns with Marshall et al. (2024) who emphasize the importance of *active engagement*, repeated practice, and feedback in improving the effectiveness of *phishing security training*.

For subsequent PkM activities, evaluation can be expanded by conducting a *follow-up test* one to three months after the training. This evaluation can be used to assess knowledge retention and identify changes in digital security behavior. Possible indicators include the ability to recognize *phishing*, the use of two-factor authentication, the habit of verifying payments before sending goods, the use of secure *passwords*, and the ability to maintain the confidentiality of account information. This approach will provide a more comprehensive picture of the program's sustainable impact.

Overall, the results of the activity indicate that digital fraud prevention education through lectures, discussions, and case simulations effectively increased the knowledge of MSMEs in the short term. The average score increased from 58.4 to 84.7, the good knowledge category increased from 13.3% to 63.3%, and the Wilcoxon test results with $p < 0.001$ indicated a significant increase in knowledge after the activity. These findings are consistent with literature showing that cybersecurity training can improve user knowledge, while reinforcement through repeated practice is needed to support more sustainable behavioral changes.

Thus, digital security education can be a preventative strategy to increase the capacity of MSMEs to face the risks of online commerce. Sustainable, case-based programs tailored to the digital platforms used by MSMEs have the potential to increase their preparedness to deal with digital fraud, strengthen transaction security, and support the creation of safer and more reliable online commerce.

5. CONCLUSION

A Community Service (PkM) activity providing digital fraud prevention education for MSMEs operating online in Batam City has demonstrated positive results. The education, through lectures, discussions, and case simulations, has increased participants' knowledge of the forms, risks, and prevention measures of digital fraud. This is indicated by an increase in the average knowledge score from 58.4 ± 12.6 in the pre-test to 84.7 ± 9.3 in the post-test, or an increase of 26.3 points. The proportion of participants with good knowledge also increased from 13.3% to 63.3%, while the poor category decreased from 46.7% to 6.7%. *The Wilcoxon Signed Rank test results* showed $p < 0.001$, indicating a significant increase in knowledge after the educational activity.

Satisfaction evaluations also showed positive results, with an average score of 4.0–4.7. The material benefits aspect for businesses received the highest score of 4.7, indicating that the educational materials were deemed relevant to the needs of MSMEs conducting online commerce. Thus, this educational activity can be a preventative measure to improve digital security literacy among MSMEs in Batam City. However, the results primarily indicate short-term knowledge gains and do not yet demonstrate long-term behavioral changes. Therefore, it is recommended that further activities be carried out on an ongoing basis through digital security simulations and exercises, as well as *follow-up* to measure knowledge retention and the application of security practices in online trading activities.

6. SUGGESTION

Based on the results of the Community Service activities that have been carried out, several suggestions that can be given are as follows:

- a. For MSMEs, the knowledge gained through educational activities needs to be consistently applied in online trading activities, especially in verifying identity, checking proof of payment, maintaining the confidentiality of passwords and OTPs, and avoiding suspicious links or messages.
- b. For PkM implementers, educational activities regarding digital fraud prevention should be carried out continuously by adding more diverse practice and case simulations, such as phishing, fake accounts, payment proof manipulation, and account takeovers.
- c. For subsequent activities, evaluation is not only conducted through pre-tests and post-tests, but also through follow-ups after several months to determine knowledge retention and the implementation of digital security practices by MSME actors.
- d. For stakeholders, collaboration between universities, local governments, MSME communities, and digital platform providers is needed to improve cybersecurity literacy through training, mentoring, and providing information on the latest digital fraud methods.
- e. For subsequent research or PkM, it is recommended to develop evaluations based on the type of platform used, previous fraud experiences, and measuring changes in digital security behavior so that the impact of the program can be known more comprehensively.

7. THANK-YOU NOTE

The implementation team expressed their gratitude to the LPPM (Institute for Community Service) of Batam University, all MSMEs who actively participated in the educational activities, and the sub-districts in Batam City for their support. Appreciation was also expressed to all parties who assisted in the implementation of this Community Service activity.

REFERENCES

- Bada, Maria, and Jason R. C. Nurse. 2019. "Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs)." *Information & Computer Security* 27(3):393–410. doi: 10.1108/ICS-07-2018-0080.
- Badan Pusat Statistik (BPS). 2025. *Statistik E-Commerce 2024*. Jakarta.
- Badan Pusat Statistik Kota Batam. 2025. *Produk Domestik Regional Bruto Kota Batam Menurut Lapangan Usaha 2020–2024*. Batam.
- Chidukwani, Alladean, Sebastian Zander, and Polychronis Koutsakis. 2024. "Cybersecurity Preparedness of Small-to-Medium Businesses: A Western Australia Study with Broader Implications." *Computers & Security* 145:104026. doi: 10.1016/j.cose.2024.104026.
- Marshall, Nina, Daniel Sturman, and Jaime C. Auton. 2024. "Exploring the Evidence for Email Phishing Training: A Scoping Review." *Computers & Security* 139:103695. doi: 10.1016/j.cose.2023.103695.
- OECD. 2016. *OECD Recommendation of the Council on Consumer Protection in E-Commerce*. Paris: OECD Publishing.
- Pemerintah Republik Indonesia. 2022. *Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. Jakarta.
- Peraturan Pemerintah Republik Indonesia. 2019. *Peraturan Pemerintah (PP) Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik*.
- Prümmer, Julia, Tommy van Steen, and Bibi van den Berg. 2025. "Assessing the Effect of Cybersecurity Training on End-Users: A Meta-Analysis." *Computers & Security* 150:104206. doi: 10.1016/j.cose.2024.104206.
- Republik Indonesia. 1999. *Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen*.
- Republik Indonesia. 2024. *Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. Jakarta.
- Rochmadi, Tri, Martalia Ardiyaningrum, Rita Mulyandari, Sarwo Miju, Septian Ibnu Rosadi, Angga Dwi Wahyudi, Wa Ode Nurlani, and Isna Deayanti Saputri. 2026. "Pengukuran Kesadaran Keamanan Informasi UMKM Terhadap Phising Pada Aplikasi Whatsapp." *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*

12(1):10–16. doi: 10.34010/jtk3ti.v11i3.18935.

Yudhiyati, Ratna, Diana Rahmawati, and Afrida Putritama. 2024. “Indonesian SMEs and Cybersecurity: Developing Instrument to Test SMEs Owners’ Capability in Detecting Phishing Emails.” *Riset Akuntansi Dan Keuangan Indonesia* 9(3):318–37. doi: 10.23917/reaksi.v9i3.6955.