

Security analysis of Indonesia e-commerce platform against the risk of phishing attacks

Gede Arna Jude Saskara, Made Ody Gita Permana, I Made Gede Sunarya

Department of Informatics Engineering, Faculty of Engineering and Vocational, Universitas Pendidikan Ganesha, Bali, Indonesia

Article Info

Article history:

Received Dec 27, 2024

Revised Apr 26, 2025

Accepted May 10, 2025

Keywords:

Action research method

Authentication method

E-commerce security

Phishing attacks

Social engineer toolkit

ABSTRACT

This research analyses the security of e-commerce platforms in Indonesia against the risk of phishing attacks using the social-engineer toolkit (SET) application. Of the 31 platforms tested, it was found that 22 platforms have a low-security level because they can be easily replicated to carry out phishing attacks. In contrast, 9 platforms showed a high level of security, as they implemented the step-wise authentication and embedded login methods, which proved effective in protecting the platform from phishing attacks. The effectiveness rate of the SET application in conducting tests was recorded at 70.9%; the percentage is included in the high category. This research also identified that most low-security platforms still use the single-page login method or a special URL for login, making them very vulnerable to phishing attacks. The action research method was used as the research framework, involving five stages: diagnosis, planning, action, evaluation, and learning. The results of this study provide important guidance for platform owners to improve security mechanisms, how to build a login page to avoid the risk of misuse by cybercrime actors to conduct phishing attacks, and for users as a reference to choose a more secure e-commerce platform.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Gede Arna Jude Saskara

Department of Informatics Engineering, Faculty of Engineering and Vocational

Universitas Pendidikan Ganesha

Singaraja, Bali, Indonesia

Email: jude.saskara@undiksha.ac.id

1. INTRODUCTION

The rapid development of information technology has significantly impacted various sectors, including politics, law, culture, and the economy [1]. Along with technological advancements, software applications, and websites have become integral to daily life. The Google Play Store and App Store offer thousands of applications for Android and iOS devices, including popular e-commerce platforms such as Shopee, Tokopedia, Zalora, and Sociolla, which enable users to buy and sell products online [2]–[5].

A report from data.Indonesia.id reported by Statista Market Insight highlights the rapid growth of e-commerce users in Indonesia. As of 2018, there were 93.42 million active e-commerce users, and this number is projected to rise significantly to 244.67 million by 2027. This upward trend is further supported by a survey conducted by We Are Social in April 2021, which confirmed Indonesia as the country with the highest percentage of internet users in e-commerce, with 88.1% having made online purchases or transactions [6].

Despite the benefits of e-commerce, technological advancements have also led to increased cybercrime. Cybercriminals exploit computer networks, the internet, and digital technology for illicit activities. One prevalent form of cybercrime is social engineering with phishing techniques, which involves manipulating users to obtain personal data [7]–[12].

Phishing cases are widespread on e-commerce platforms like Shopee, Lazada, Zalora, and others. Based on the latest data from the Phishing Activity Trends Report reported by the Anti-Phishing Working Group (APWG) in 2024, the number of unique attacks on phishing websites detected reached 877,536 attacks targeting various industry sectors, ranging from e-commerce, social media, payments, and others [13]. In addition, according to the Surfshark report, Indonesia occupies the eighth position and is included in the top 10 countries with the highest number of data leakage cases on the internet globally, including the results of phishing crimes. The data underscores the urgent need to address the vulnerability of e-commerce platforms, which is the main problem in this research.

This study looked into the effects of the impact of e-commerce platform security mechanisms on phishing attacks. While previous studies investigated the impact of phishing attacks on social media platforms [14]–[16], they did not explicitly address their influence on technical authentication methods in systems, thus leaving gaps in understanding the vulnerabilities of e-commerce platforms. Therefore, this study aims to fill this gap by analyzing e-commerce security against the risk of phishing attacks using the social-engineer toolkit (SET) application.

The selection of SET as a testing tool is based on its superior flexibility compared to other phishing tools such as Zphisher, SocialFish, and HiddenEye. Unlike those tools, which are static and limited to the provided social media templates, SET allows syntax/parameter customization and replication of phishing pages that mimic the latest look of the target platform. This flexibility makes SET more effective in conducting phishing attacks, identifying vulnerabilities in e-commerce platforms, and supporting white hat activities in testing platform security through simulated phishing attacks [17]–[22].

Specifically, this research will analyze whether e-commerce platforms can be replicated to trap users into entering their personal information, such as username and password, during the login process. Thus, the results of this research can provide important guidance for platform owners and developers to improve security mechanisms and build a platform to avoid the risk of phishing attacks. In addition, the results of this study are also expected to be a reference for users in choosing a more secure e-commerce platform.

This study contributes to the theoretical understanding of phishing vulnerabilities in e-commerce platforms by providing a comprehensive analysis using SET. Practically, it offers actionable insights for improving e-commerce platform security, which can help reduce the risk of cybercrime. From a management perspective, the findings can guide decision-making processes for implementing robust security measures. Furthermore, the study has societal and sustainability implications by promoting safer digital environments and fostering trust in e-commerce platforms, which are essential for sustainable economic growth.

2. RESEARCH METHOD

The method used in this research is action research. This method was first put forward in 1946 [23]. Kurt Lewin has argued [24] that the action research method is used to test, develop, find, and create new actions so that if these actions are applied in work, the implementation process will be easier and faster and the results will be of higher quality. The process includes five stages: diagnosis, planning, action, evaluation, and learning, which are conducted systematically to be scientifically valid and reliable [25]–[30]. This method was chosen because the stages are structured and relevant to addressing security challenges on e-commerce platforms.

The diagnosis stage begins with the identification of the main problem as the basis for the research, including data collection and sample selection. The data collection technique was conducted through a literature study (documentation) by reviewing relevant literature from scientific journals, books, and academic databases such as Google Scholar. The sample selection used a purposive sampling technique based on the criteria of e-commerce platforms that are active and popular in Indonesia [31]. Then, the number of samples will be determined based on the theory first put forward in 1996 [32]. Higgins and Stens [33] has argued that the ideal sample size in research ranges from 30 to 500 to obtain a distribution of values closer to the normal curve. This research is focused on testing the confidentiality (C) aspect of the confidentiality, integrity, and availability (CIA) triad theory on several e-commerce platforms [34].

The planning stage includes steps that will be taken to overcome the problems that have been previously identified at the diagnosis stage. In this stage, the author will make plans related to the actions to be taken in conducting tests, such as selecting SET as the right tools to conduct tests, types of attacks to be used, measuring the effectiveness of SET applications in conducting tests, and the number of iterations performed during testing. After all the plans are made, it is hoped that the testing process can run well and provide a comprehensive picture of the security of the platform being tested. This is done to identify every aspect of potential vulnerabilities so that the results obtained can be a reference in developing and improving platform security.

The action stage is the implementation stage of the previously developed plan. At this stage, the planned actions will be carried out systematically to test the security of the e-commerce platform from the risk of abuse by cybercrime actors. In this stage, testing will be conducted by the previously determined tools and types of attacks to understand the extent to which cybercrime actors can exploit these vulnerabilities for phishing attacks and steal users' personal information, such as usernames and passwords, during the login process.

The evaluation stage, this stage involves a thorough assessment of the tests conducted to determine the security of the e-commerce platform. Each platform that has been tested will be evaluated based on several key indicators, such as whether the platform can be replicated; unencrypted username and password, and several other indicators, which serve as a reference to classify the platform into high or low security levels. These indicators are systematically listed in Table 1.

Table 1. Platform security level classification

Indicators	Safety level	Platform name
Not replicable; replicable; encrypted password	High	/
Replicable; username and password are not encrypted.	Low	/

To measure effectiveness, we use the theory presented by [35]. Mahmudi [35] describes effectiveness as the relationship between output and input. The greater the contribution of outputs to the achievement of goals, the more effective the organization, program, or activity. To measure the level of effectiveness, we can use the following formula.

$$Effectiveness = \frac{Output}{Input} \times 100\% \quad (1)$$

Output: the number of e-commerce platforms that are successfully replicated. Input: the number of platforms tested. The results will be classified into three (3) categories: high (65-100%), medium (36-64%), and low (0-35%). The last stage in this method is learning. The learning stage aims to document and synthesize the results of the testing that has been done. In this stage, all findings obtained from the security testing of the e-commerce platform will be documented. These findings include successful and unsuccessful attack simulations performed during the testing process. In addition, this stage also formulates actionable solutions to improve the security of platforms that have low security and provides recommendations for future research.

3. RESULTS AND DISCUSSION

The results of this study can serve as a reference for parties aiming to create a platform that is secure from cybercrime actors' abuse for conducting phishing attacks. Moreover, it can offer guidance to users in choosing secure e-commerce platforms and reducing the risk of phishing attacks. Specifically, the study results can assist e-commerce owners in pinpointing issues on their platforms, enabling them to promptly implement corrective measures to uphold the platform's reputation.

3.1. Diagnosis results

At the diagnosis stage, the main problem identified was the increasing number of phishing cases in Indonesia, especially in the e-commerce sector. The APWG report (2024) recorded 877,536 phishing attacks targeting various sectors such as e-commerce, social media, and others. Surfshark also ranked Indonesia as the 8th country with the highest data leakage in the world. In addition, Kaspersky reported a 40% increase in phishing cases in early 2024 compared to the first quarter of 2023. The types of phishing are now increasingly diverse, such as voice, email, web, and QR phishing, mostly targeting e-commerce users such as Shopee, Zalora, Lazada, and others. The data shows the urgency of addressing security issues on e-commerce platforms.

The number of samples in this study was 31. By the theory put forward in 1978 [36]. Rascoe [36] has argued that the ideal sample size ranges from 30-500 to obtain a distribution of values closer to the normal curve. The platform samples include Tokopedia, Shopee, Lazada, Bukalapak, Blibli, Orami, Ralali, Zalora, KlikIndomaret, Sociolla, Matahari, Hijup, Bro.do, Berrybenka, Bobobobo, Tees, Favo, Qoo10, JakartaNotebook, MyHartono, Semuasale, Sephora, Mothercare, OttenCoffee, Alfagift, OLX, Bhinneka, Mapclub, Jamtangan, Plazakamera, and E-catalogue. The selection of the platform sample is also based on the highest number of users and visitors based on data from iPrice group, Similarweb, and Statista (processed by the Indonesian data center and information system, and the Indonesian Ministry of Trade).

3.2. Planning results

The results of this stage include: i) The selection of the SET application for testing the security of e-commerce platforms against the risk of phishing attacks; ii) The type of attack used is Credential Harvesting by utilizing a combination of social engineering attacks, website attack vectors, credential harvester attack methods, and site cloner features. As well as the addition of several syntax/parameters to bypass when testing; and iii) The number of iterations in this study was set at two times. Testing the security of e-commerce platforms by simulating phishing attacks by creating phishing sites using the SET application can only be done by following the combination of these features. Other features in the SET application are designed for different types of attacks, not specifically for phishing site creation. If the attack simulation cannot be performed using these features, some additional syntax/parameters will be added to perform the bypass. If the additional syntax/parameters still fail to create a phishing site, the iteration process will be stopped.

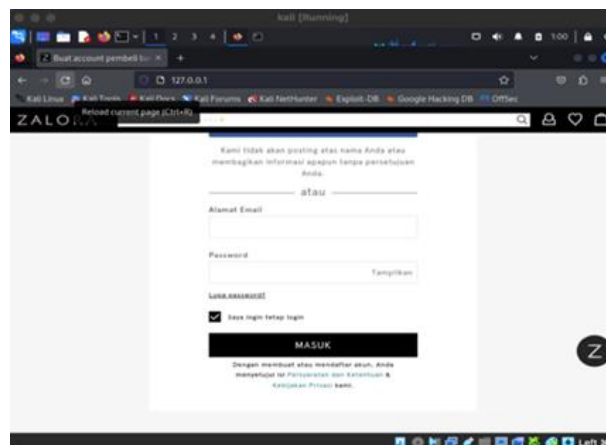
3.3. Action results

At this stage, the implementation of the previously planned actions is carried out. The testing phase of this study was conducted from September to November 2024. The results of the action stage can be seen as follows.

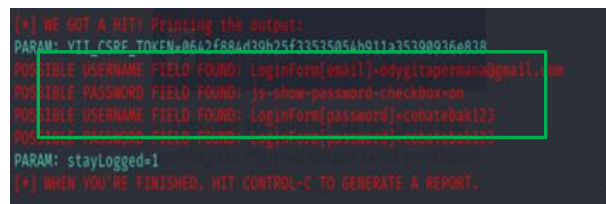
3.3.1. Platform sample testing

Figure 1 shows the results of a successful replication on one of the sample e-commerce platforms. Figure 1(a) shows the replicated login page, which is exactly the same as the original login page of the Zalora platform. Meanwhile, Figure 1(b) shows that the credentials entered by the user (username and password) can be automatically captured at the offender terminal and are not encrypted. This finding indicates that the process of replicating the login page of the Zalora platform using phishing techniques is successful and has the potential to be utilized by cybercriminals to conduct phishing attacks on users.

In addition to testing the Zalora platform, similar tests were also conducted on 30 other e-commerce platforms to determine their level of resilience to the risk of phishing attacks. The results showed that some platforms exhibited vulnerabilities that could be exploited by cybercriminals to conduct phishing attacks and unauthorized theft of user data. On the other hand, some platforms show a high level of security because they cannot be replicated, or the passwords obtained are encrypted, according to the security indicators listed in Table 1.



(a)



(b)

Figure 1. Sample results of e-commerce platforms of (a) platform replication results and (b) successfully captured credentials

3.4. Evaluation results

Based on the test results in the action stage, we found that 22 out of 31 platforms were vulnerable to phishing attacks, correlating strongly with their use of static single-page login designs and a special URL to login. The proposed SET application testing method in this study tended to have an inordinately higher success rate (70.9%) when attacking platforms without dynamic authentication mechanisms. This stage will classify e-commerce platforms based on their security level, platforms with high-security and low-security levels. Platforms with high security are resistant to phishing attacks, while platforms with low security are vulnerable to such attacks. The results of the classification can be seen in Table 2.

Table 2. Result of classifying the security level of the platform

Platform e-commerce	Security level	Assessment indicator
Zalora	Low	Successfully replicated; get plain password
Blibli	Low	Successfully replicated; get plain password
E-Katalog	Low	Successfully replicated; get plain password
Sociolla	Low	Successfully replicated; get plain password
Matahari	Low	Successfully replicated; get plain password
Berrybenka	Low	Successfully replicated; get plain password
Favo	Low	Successfully replicated; get plain password
JakartaNotebook	Low	Successfully replicated; get plain password
MyHatono	Low	Successfully replicated; get plain password
Klikindomaret	Low	Successfully replicated; get plain password
Alfagift	Low	Successfully replicated; get plain password
Semuasale	Low	Successfully replicated; get plain password
Mothercare	Low	Successfully replicated; get plain password
Hijup	Low	Successfully replicated; get plain password
Qoo10	Low	Successfully replicated; get plain password
Jamtangan	Low	Successfully replicated; get plain password
Bro.do	Low	Successfully replicated; get plain password
Tees	Low	Successfully replicated; get plain password
Bobobobo	Low	Successfully replicated; get plain password
Shopee	Low	Successfully replicated; get plain password
Lazada	Low	Successfully replicated; get plain password
Ralali	Low	Successfully replicated; get plain password
Tokopedia	High	Encrypted password
Bukalapak	High	Encrypted password
OttenCoffee	High	Encrypted password
Mapclub	High	Encrypted password
Bhinneka	High	Encrypted password
Sephora	High	Not replicable
OLX	High	Not replicable
Orami	High	Not replicable
Plazakamera	High	Not replicable

The results of measuring the effectiveness of the SET application in conducting tests are as follows: In accordance with the theory of effectiveness conveyed by Mahmudi [35], the percentage of the success rate of the SET application in testing e-commerce platforms can be measured using the (2). This formula provides a quantitative measure of how successful the SET application is in simulating phishing attacks.

$$Effectiveness = \left(\frac{\text{E-Commerce platforms that have been successfully replicated and get plain password}}{\text{Numbers of e-commerce platforms that will be tested}} \right) \times 100\% \quad (2)$$

So,

$$Effectiveness = \left(\frac{22}{31} \right) \times 100\% = 70.9\%$$

Based on these results, the effectiveness of the SET application in conducting testing was recorded at 70.9%. Based on the measurement categories described by [35] in the theory of effectiveness, this percentage is included in the high category. This indicates that the SET application is highly effective in simulating phishing attacks on e-commerce platforms.

This study investigated a comprehensive of 31 e-commerce platforms in Indonesia and their vulnerability against the risk of phishing attacks using the SET application. However, additional and in-depth research may be required to confirm this finding. Particularly regarding platforms employing emerging authentication technologies like biometrics and others.

3.5. Learning results

Based on the results of several stages that have been carried out, 22 of 31 samples of e-commerce platforms selected to be tested for security were found to be insecure. Meanwhile, 9 other e-commerce platforms have been proven safe and free from the risk of misuse by cybercrime actors to conduct phishing attacks. This shows that a significant portion of e-commerce platforms still lack adequate security measures to protect against phishing attacks.

The recommendations that can be given based on the test results that have been carried out are: i) apply step-wise authentication on the login page so that applications such as SET and so on cannot replicate, ii) implement embedded login. Integrating the login page into the homepage to prevent URL-based phishing attempts, and iii) implementing multi-factor authentication can strengthen user authentication to minimize unauthorized access.

3.6. Discussion

This study investigates the security of 31 e-commerce platforms in Indonesia, categorizing them into two groups based on their vulnerability to phishing attacks: i) high-security platforms and ii) low-security platforms. Nine platforms, including Tokopedia, Bhinneka, Sephora, and others, were classified as high-security platforms due to the implementation of advanced security measures like step-wise authentication and embedded login. In user interface (UI) design theory, this method is categorized as progressive disclosure, where information is presented gradually to reduce cognitive load and enhance user information security [37].

Step-wise authentication breaks down the login process into multiple steps, typically requiring the user to input a username before entering a password. This approach utilizes asynchronous JavaScript and XML (AJAX) techniques to interact with the server dynamically and offer real-time feedback to the user without page reloading. Platforms like Tokopedia, Bhinneka, and others employ this method to enhance security, as it can hinder cybercriminals from duplicating the login page. Utilizing AJAX techniques ensures that sensitive information, such as passwords is encrypted before transmission to the server, thereby decreasing the risk of misuse by cybercriminals to conduct phishing attacks.

Embedded login utilized by platforms like Sephora, OLX, and others, integrates the login page directly into the main page without redirecting users to a separate URL. This approach depends on dynamic elements powered by JavaScript, making it challenging for cybercriminals to replicate the login process using phishing applications like SET and others. By removing the necessity for a dedicated login URL, an embedded login can decrease potential attacks and enhance security. These methods effectively thwart phishing attacks by encrypting user passwords and integrating the login process into the main page.

Conversely, 22 platforms like Zalora, Shopee, Lazada, and others were identified as vulnerable to phishing attacks due to their dependence on single-page login and custom login URLs, which are simpler to replicate. The Single Page login method merges the username and password forms on a single page, facilitating attackers to duplicate the login page due to its static nature. In contrast, the login-only URL is a web or application address officially provided to access the login page of the website or application. Although single-page login and login-only URLs provide convenience to users and are equipped with the HTTPS protocol, which offers additional security through data encryption when users enter credentials, their static nature makes them highly vulnerable to phishing attacks. Cybercriminals can easily create fake login pages that mimic the appearance of legitimate platforms and deceive users into entering their credentials.

In previous studies, most of them only focused on phishing vulnerabilities on social media platforms [38]–[40]. These studies only go as far as testing whether these platforms can be replicated to perform phishing attacks on users and provide tips/mitigations to prevent phishing attacks but do not further analyze the specific security mechanisms that make replication impossible. For example, while some studies reveal that certain platforms are secure against the risk of phishing attacks, they do not analyze the underlying authentication methods (such as step-wise authentication or embedded login) that play an important role in the security of these platforms. Our findings indicate that higher implementation of step-wise authentication and embedded login is not associated with poor user experience in e-commerce platforms. The proposed method may benefit from combining technical vulnerability assessments with user behavior studies without negatively affecting platform usability. This contrasts with single-page login and special URLs for login methods, despite their convenience, but it is highly vulnerable to replication.

The findings of this study emphasize the significance of implementing robust security measures, like step-wise authentication and embedded login to safeguard e-commerce platforms from potential misuse by cybercriminals for conducting phishing attacks. Platform owners and developers are expected to prioritize the implementation of these methods to protect personal data and maintain user trust. Our research shows that step-wise authentication and embedded login are more resilient than traditional single-page login and special URL for login methods. Future research may look into hybrid modern authentication (HMA) models and

practical methods for implementing these solutions across different e-commerce or platform architectures, especially for small to medium platforms.

4. CONCLUSION

This research examines the security of e-commerce platforms in Indonesia concerning the threat of phishing attacks utilizing the SET. Recent observations indicate that the persistent vulnerability of Indonesian e-commerce platforms to phishing attacks continues despite widespread security awareness programs. Our findings offer definitive proof that this phenomenon is linked to authentication interface design alteration (step-wise authentication and embedded login vs. single-page login and special URL for login methods), rather than being caused by increased quantities of phishing attempts or user education gaps. The 22:9 vulnerability ratio and SET 70.9% effectiveness rate conclusively demonstrate that technical solutions outperform awareness-based defenses.

ACKNOWLEDGMENTS

We would like to express gratitude to Ir. I Made Edy Listartha, S.Kom., M.Kom. and Bagus Gede Krishna Yudistira, M.Kom., for their input and suggestions during the preparation of this work. Their feedback was helpful in the development process. This acknowledgment is made with their full consent, in recognition of their personal assistance.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Gede Arna Jude Saskara	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓
Made Ody Gita Permana		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
I Made Gede Sunarya		✓		✓		✓				✓			✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study. All participants were adequately informed about the objectives, procedures, potential risks, and their rights, before providing written consent to participate.

DATA AVAILABILITY

The data supporting the findings of this study are available from the corresponding author upon reasonable request. All relevant data used and analyzed during the research were obtained from credible sources and have been appropriately documented to ensure transparency and reproducibility:

- The data that support the findings of this study are openly available in Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report, 2nd Quarter 2024," Aug. 2024. Accessed: Nov. 24, 2024. [Online]. Available: <http://www.apwg.org/>
- I. I. Karinda, "The effect of perceived quality, perceived usefulness, and perceived ease of use on Shopee e-commerce customer satisfaction in Surabaya City (in Indonesian: *Pengaruh perceived quality, perceived usefulness, dan perceived ease of use terhadap kepuasan pelanggan e-commerce Shopee di Kota Surabaya*)", Doctoral dissertation, UPN Veteran Jawa Timur, 2024. [Online]. Available: [https://repository.upnjatim.ac.id/20779/2/20042010063_Bab 1.pdf](https://repository.upnjatim.ac.id/20779/2/20042010063_Bab%201.pdf)




REFERENCES

- [1] L. D. Williams, "Concepts of digital economy and industry 4.0 in intelligent and information systems," *International Journal of Intelligent Networks*, vol. 2, pp. 122–129, 2021, doi: 10.1016/j.ijin.2021.09.002.
- [2] H. K. Sunyoto, C. A. Gunawan, and P. Shrinithy, "The measurement of consumers' purchase intention in e-commerce by electronic service quality: mediation test of e-satisfaction and e-trust," *Abhigyan*, Oct. 2024, doi: 10.1177/09702385241282386.
- [3] A. Prasetyo, N. A. Witasaryah, and Indrawati, "The effect of e-wom on purchase intention in e-commerce in Indonesia through the expansion of the information adoption model," *International Journal of Data and Network Science*, vol. 8, no. 3, pp. 1959–1968, 2024, doi: 10.5267/j.ijdns.2024.1.017.
- [4] A. A. Sudjatmoko, A. A. Susanto, J. A. Jayaseputra, E. S. Purwanto, and A. C. Sari, "The influence of consumer interest on the use of UI and UX in the e-commerce application," *2022 4th International Conference on Cybernetics and Intelligent System, ICORIS 2022*, 2022, doi: 10.1109/ICORIS56080.2022.10031397.
- [5] M. Astuti, Ganefri, and A. Yulastri, "Literature review: the influence of demographics, user experience and e-commerce platforms in the digital business world," *Indonesian Journal of Computer Science*, vol. 12, no. 5, 2023, doi: 10.33022/ijcs.v12i5.3444.
- [6] K. Ariansyah, E. R. E. Sirait, B. A. Nugroho, and M. Suryanegara, "Drivers of and barriers to e-commerce adoption in Indonesia: individuals' perspectives and the implications," *Telecommunications Policy*, vol. 45, no. 8, 2021, doi: 10.1016/j.telpol.2021.102219.
- [7] M. Button, D. Shepherd, D. Blackburn, L. Sugiura, R. Kapend, and V. Wang, "Assessing the seriousness of cybercrime: the case of computer misuse crime in the United Kingdom and the victims' perspective," *Criminology and Criminal Justice*, 2022, doi: 10.1177/17488958221128128.
- [8] Sakshi, A. Vashishth, and Teena, "An analysis of cyber crime with special reference to cyber stalking," *Journal of Positive School Psychology*, vol. 6, no. 4, pp. 1279–1287, 2022.
- [9] P. Y. Leonov, A. V. Vorobyev, A. A. Ezhova, O. S. Kotelyanets, A. K. Zavalishina, and N. V. Morozov, "The main social engineering techniques aimed at hacking information systems," *Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBREIT 2021*, pp. 471–473, 2021, doi: 10.1109/USBREIT51232.2021.9455031.
- [10] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions," *IEEE Access*, vol. 9, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.
- [11] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social engineering attacks prevention: a systematic literature review," *IEEE Access*, vol. 10, pp. 39325–39343, 2022, doi: 10.1109/ACCESS.2022.3162594.
- [12] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies," *Journal of Applied Security Research*, 2024, doi: 10.1080/19361610.2024.2372986.
- [13] G. Varshney, R. Kumawat, V. Varadharajan, U. Tupakula, and C. Gupta, "Anti-phishing: a comprehensive perspective," *Expert Systems with Applications*, vol. 238, 2024, doi: 10.1016/j.eswa.2023.122199.
- [14] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021, doi: 10.1109/ACCESS.2021.3066383.
- [15] A. Jafar, A. Yeboah-Ofori, T. Abisogun, I. Hilton, O. Oguntuyinbo, and O. Oyetunji, "The impact of social engineering attacks on the metaverse platform," *Proceedings - 2024 11th International Conference on Future Internet of Things and Cloud, FiCloud 2024*, pp. 201–208, 2024, doi: 10.1109/FiCloud62933.2024.00038.
- [16] J. N. P. Soon, R. Q. Chan, Q. H. Lee, D. En Loke, S. L. H. Chun, and P. K. Yuen, "User perceptions of artificial intelligence powered phishing attacks on facebook's resilient infrastructure," *International Journal of Advances in Applied Sciences*, vol. 13, no. 4, pp. 878–886, 2024, doi: 10.11591/ijaas.v13i4.pp878-886.
- [17] M. Kulkarni et al., "Mitigating email phishing: analytical framework, simulation models, and preventive measures," *Proceedings of the 2024 10th International Conference on Communication and Signal Processing, ICCSP 2024*, pp. 1459–1464, 2024, doi: 10.1109/ICCSP60870.2024.10543325.
- [18] R. Sahay, W. Meng, and W. Li, "A comparative analysis of phishing tools: features and countermeasures," *Lecture Notes in Computer Science*, vol. 15053 LNCS, pp. 365–382, 2025, doi: 10.1007/978-981-97-9053-1_21.
- [19] R. P. K. Kollepalli, M. J. S. Reddy, B. L. Sai, A. Natarajan, S. Mathi, and V. Ramalingam, "An experimental study on detecting and mitigating vulnerabilities in web applications," *International Journal of Safety and Security Engineering*, vol. 14, no. 2, pp. 523–532, 2024, doi: 10.18280/ijssse.140219.
- [20] D. Arnaldy and R. P. Theyser, "Analysis of apiloy.id email domain security status using dmarc (domain-based message authentication, reporting, and conformance)," *Proceedings - 2023 6th International Conference on Computer and Informatics Engineering: AI Trust, Risk and Security Management (AI Trism), IC2IE 2023*, pp. 125–130, 2023, doi: 10.1109/IC2IE60547.2023.10331296.
- [21] V. A. H. Krupalin, G. V. Sriramakrishnan, and T. Daniya, "A survey and taxonomy of anti-phishing techniques for detecting fake websites," *4th International Conference on Inventive Research in Computing Applications, ICIRCA 2022 - Proceedings*, pp. 601–604, 2022, doi: 10.1109/ICIRCA54612.2022.9985744.
- [22] S. Merugula, K. S. Kumar, S. Muppidi, and C. Vidyadhari, "Stop phishing : master anti-phishing techniques," *2022 IEEE North Karnataka Subsection Flagship International Conference, NKCon 2022*, 2022, doi: 10.1109/NKCon56289.2022.10126569.
- [23] C. Adelman, "Kurt Lewin and the origins of action research," *Educational Action Research*, vol. 1, no. 1, pp. 7–24, 1993, doi: 10.1080/0965079930010102.
- [24] P. C. Endrejat and B. Burnes, "Kurt Lewin's ideas are alive! but why doesn't anybody recognize them?," *Theory and Psychology*, vol. 32, no. 6, pp. 931–952, 2022, doi: 10.1177/09593543221118652.
- [25] C. Wohlin and P. Runeson, "Guiding the selection of research methodology in industry-academia collaboration in software engineering," *Information and Software Technology*, vol. 140, 2021, doi: 10.1016/j.infsof.2021.106678.
- [26] N. Ong et al., "Patient safety and quality care for children with intellectual disability: an action research study," *Journal of Intellectual Disabilities*, vol. 27, no. 4, pp. 885–911, 2023, doi: 10.1177/17446295221104619.
- [27] D. López-García et al., "Building agroecology with people. challenges of participatory methods to deepen on the agroecological transition in different contexts," *Journal of Rural Studies*, vol. 83, pp. 257–267, 2021, doi: 10.1016/j.jrurstud.2021.02.003.
- [28] I. Bleijenbergh, F. van Mierlo, and T. Bondarouk, "Closing the gap between scholarly knowledge and practice: guidelines for HRM action research," *Human Resource Management Review*, vol. 31, no. 2, 2021, doi: 10.1016/j.hrmr.2020.100764.




- [29] B. Sundarakani, A. Ajaykumar, and A. Gunasekaran, "Big data driven supply chain design and applications for blockchain: an action research using case study approach," *Omega (United Kingdom)*, vol. 102, 2021, doi: 10.1016/j.omega.2021.102452.
- [30] M. Strumińska-Kutra and C. Scholl, "Taking power seriously: towards a power-sensitive approach for transdisciplinary action research," *Futures*, vol. 135, 2022, doi: 10.1016/j.futures.2021.102881.
- [31] S. Campbell *et al.*, "Purposive sampling: complex or simple? research case examples," *Journal of Research in Nursing*, vol. 25, no. 8, pp. 652–661, 2020, doi: 10.1177/1744987120927206.
- [32] J. R. Higgins, *Sampling theory in fourier and signal analysis: foundations*. Clarendon Press, 1996. doi: 10.1093/oso/9780198596998.001.0001.
- [33] J. R. Higgins and R. L. Stens, *Sampling theory in fourier and signal analysis: advanced topics*. Oxford University Press, 1999. doi: 10.1093/oso/9780198534969.001.0001.
- [34] J. Hariharan, A. T. Sheik, C. Maple, N. Beech, and U. I. Atmaca, "Customers' perception of cybersecurity risks in e-commerce websites," *IET Conference Proceedings*, vol. 2023, no. 14, pp. 53–60, 2023, doi: 10.1049/icp.2023.2565.
- [35] Mahmudi, *Public sector performance management: second edition (in Indonesian: manajemen kinerja sektor publik: edisi kedua)*. UPP STIM YKPN, 2013.
- [36] D. L. Rascoe, "A search for a new phonon detector," *University of Illinois at Urbana-Champaign*, 1978.
- [37] M. Chromik and A. Butz, "Human-xai interaction: a review and design principles for explanation user interfaces," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2021, pp. 619–640. doi: 10.1007/978-3-030-85616-8_36.
- [38] S. Gupta, M. Pritwani, A. Shrivastava, Mohana, M. Moharir, and A. R. Ashok Kumar, "A comprehensive analysis of social engineering attacks: from phishing to prevention - tools, techniques and strategies," in *2nd International Conference on Intelligent Cyber Physical Systems and Internet of Things, ICoICI 2024 - Proceedings*, 2024, pp. 42–49. doi: 10.1109/ICoICI62503.2024.10696444.
- [39] J. W. James, "Engineering the human mind: social engineering attack using Kali Linux," *SN Computer Science*, vol. 4, no. 6, 2023, doi: 10.1007/s42979-023-02321-y.
- [40] C. Le, R. Nassiri, E. Jebessa, J. Cathcart, and T. K. Mohd, "Social media account hacking using Kali Linux-based tool beef," *Lecture Notes in Networks and Systems*, vol. 665 LNNS, pp. 713–724, 2023, doi: 10.1007/978-981-99-1726-6_55.

BIOGRAPHIES OF AUTHORS






Gede Arna Jude Saskara    is a lecturer member in the Department of Informatics Engineering, Faculty of Engineering and Vocational, Universitas Pendidikan Ganesha. He specializes in computer networks and information systems security, which serve as the primary focus of his research activities. He earned his Master's degree from Institut Teknologi Bandung (ITB) in 2016, specializing in telematics and telecommunication networks. He can be contacted at email: jude.saskara@undiksha.ac.id.



Made Ody Gita Permana    is a graduate student from the Department of Informatics Engineering, Faculty of Engineering and Vocational, Universitas Pendidikan Ganesha. He specializes in computer networks, and information system security, which serve as the primary focus of his research activities. He can be contacted at email: ody@undiksha.ac.id.



I Made Gede Sunarya    is a lecturer member in the Department of Informatics Engineering, Faculty of Engineering and Vocational, Universitas Pendidikan Ganesha. He specializes in computer networks, information systems security, aeromodelling, and digital image processing, which serve as the primary focus of his research activities. He earned his Doctorate from Institut Teknologi Sepuluh Nopember (ITS) in 2020, a Master's degree from Universitas Gadjah Mada (UGM) in 2012, and a Bachelor's degree from Universitas Gadjah Mada (UGM) in 2006. He can be contacted at email: sunarya@undiksha.ac.id.