JURNAL EMACS
(Engineering, MAthematics and Computer Science) Vol.7 No.1 January 2025: 71-81
e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v7i1.12100

Cyber Security Awareness Simulation for Web Phishing in E-Commerce

Jason Matthew Sutanto[1*], Nadia[2]

[1,2] Cyber Security Program, Computer Science Department, School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480
[1]jason.sutanto.ac.id; [2] nadia002@binus.ac.id

*Correspondence: jason.sutanto@binus.ac.id

Abstract *— The development of information and communication technology has changed people's behavior in conducting transactions for buying and selling goods and services. With e-commerce, people can conduct transactions for buying and selling goods or services digitally. Although e-commerce can provide several positive impacts for society, one of which is through the ease of buying and selling goods digitally, e-commerce also has negative impacts for society, one of which is the risk of cybercrime, such as hacking, theft, and fraud. Therefore, consumers as e-commerce actors need to be protected, guarded, and secured. Protection in cyberspace is not only about strengthening the existing security system, but e-commerce users also need to be given an understanding and knowledge about cybersecurity to prevent data theft and hacking through phishing or other social engineering attacks. This study aims to build an application or feature that can increase security awareness for e-commerce users. The method used is the Waterfall method, as well as SIT (System Integration Testing) and UAT (User Acceptance Testing). Algorithm design involves the Dart programming language and the Flutter framework. The results of the study show that the applications or features created can increase security awareness among users and prevent the risk of cybercrime threats, such as fraud or hacking.*

Keywords: *cybersecurity, e-commerce, security awareness*

I. INTRODUCTION

In the era of digital technology advancement, it has resulted in human daily activities experiencing significant progress (Sukma Ayu et al., 2023). The use of technology itself also changes the way people behave (Djayapranata, n.d.).One example is the use of Internet technology. The internet is a global communications network that can connect computers and computer networks throughout the world. In addition, the internet plays an important role in this digital era (Anik Awalia et al., 2024). One of its main roles is as a provider of various information and communication channels.

However, the use of the internet is not only used to find information and communication, but the internet can also be used to encourage the development of the economic system towards a digital economy that gave birth to e-commerce (Hidayat et al., 2023). E-Commerce (Electronic Commerce) is a trading activity carried out without meeting between sellers and buyers which emphasizes on a system in the form of exchanging goods or services via the internet (Hidayah, 2022). The positive impact of using e-commerce applications, namely wider market reach, more

flexibility, increased income, reduced risk of other costs, maximum service, and reviews from buyers which can be used as business benchmarks (Poeja Kehista et al., 2023).

In addition, buying and selling transactions in e-commerce are also facilitated by the Internet which can help buyers and sellers to conduct virtual transactions on the buying and selling platform used by buyers and sellers (Astuti et al.,2022).

Although e-commerce provides convenience, it also brings security risks, such as the risk of cybercrime (Lisnawati et al., 2023). Cybercrime itself is a crime against computer systems with the intention of stealing data (Daeng et al., 2023). In e-commerce, cybercrime mostly targets personal data belonging to e-commerce users because personal data is one of the most valuable assets (Iharahap et al., 2023).

Personal data such as name, address, telephone number, account number and other personal information are at risk of being stolen or misused by irresponsible parties (Ifan Al Aziz et al., 2024). Security threats to personal data of e-commerce users are quite diverse, such as malware attacks, hacking, fraud, phishing, and many more (Hasya et al., 2024). The risks arising from violations of privacy and security of personal data can harm users financially and reputationally in society. It is important for people to understand the importance of protecting their privacy data when making transactions on e-commerce (Hamim et al., 2023).

However, this is still quite unfortunate because there are still Indonesian people, including users, who still have insufficient knowledge and understanding regarding the world of cybersecurity (Syahputra et al., 2024). This can be proven through the IDADX (Indonesia Anti-Phishing Data Exchange) report which noted that there were 26,675 phishing attacks in the first quarter of 2023. In addition, IDADX said that the industrial sector was the most frequently targeted by phishing attacks in the quarter. I 2023 is social media with a percentage of 45%. This is followed by the financial institutions sector (31%), retail/e-commerce (20%), spam (2%), as well as ISP and cryptocurrency with a percentage of 1% each.

Through this statement, it can be seen that cases of data theft caused by phishing are quite high, where e-commerce is one of the industrial sectors affected by phishing cases.

Phishing itself is one type of cybercrime that often occurs in e-commerce users by tricking victims by sending fake e-mails or websites that look like the original to deceive and obtain the victim's personal data (Rahmadi, 2020). Therefore, it is very important for Indonesians, especially e-commerce users, to have good security awareness to prevent cybercrime, such as fraud, phishing, and spoofing (Nur et al., 2022).

The solution offered to increase security awareness among e-commerce users is by providing cybersecurity education and guidance on using security features in e-commerce applications through implementing the pop up feature as a means or effort to provide cybersecurity education to users and the notification feature as a means to guide them. users to use security features in e-commerce applications. With these two features, users can increase security awareness and prevent the risk of fraud or other cyber attacks. However, without these two features, it is possible that there are e-commerce users who do not realize the importance of having security awareness, so the risk of fraud, identity theft and other cyber attacks will increase.

This pop up and notification feature will be created using a programming language called Dart, and using the Visual Studio Code and Flutter applications as a place to create and test source code for the pop up and notification feature.

II. METHODS

In this section, literature studies and surveys will be used to collect data and information regarding methods for providing cyber security education and guidelines for using security features carried out by Tokopedia, Shopee, and Lazada as a comparison with the proposed method.

Some of the literature studies used in this research include:

1) Analysis of Privacy Data Leaks in Tokopedia E-Commerce.

e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v7i1.12100

2) The Influence of Online Customer Reviews and Trust on Purchase Interest on the Lazada Marketplace.
3) The Role of Security Management in Purchasing Decisions for Shopee Application Users (Security Management Literature Study).

Meanwhile, in a survey or questionnaire there is an explanation of the parts used to collect data or information, including:
1) Participants

In achieving research objectives, access to every e-commerce user is required. Therefore, the survey was conducted in Indonesia using the Google Forms application. This choice was informed because the Google Forms application can help in obtaining responses from many respondents and with a wide reach. The survey will be conducted in 2024 using questions or questionnaires. Based on the existing survey results, it is known that the number of respondents who answered the survey was 73 people with the percentage of students being 9.6%, employees being 80.8%, and the remaining 9.6%.

2) Measures

The questionnaire in this survey is divided into three parts. The first part contains information related to the demographics of e-commerce users, the second part contains testing and evaluation of methods for providing cybersecurity education implemented by Tokopedia, Shopee, Lazada, and the proposed methods, and the third part contains testing and evaluation of methods for guidance on using security features by Tokopedia, Shopee, Lazada, and the proposed method.

After collecting data using literature study and survey methods, data analysis was then carried out using descriptive and comparative methods. The descriptive method will be used to provide an overview of the data that has been obtained in statistical or numerical form, while the comparative method will be used to make comparisons on the data that has been obtained.

To develop the proposed application or feature, the Waterfall method is used so that the application development process can be carried out sequentially and systematically. Meanwhile, in conducting application testing, two methods are applied, including:
1) SIT (System Integration Testing)
In this test, the application that has been designed will be tested independently first to check whether the application or feature created can run correctly and as expected. If the application is running as expected, the next testing step will be carried out.

2) UAT (User Acceptance Testing)
After testing that the designed application can run as expected, the next test will be carried out by the respondent to prove the capabilities of the application that has been designed as a means of increasing security awareness and reducing the risk of leakage of users' personal data.

From the test results that have been obtained, an evaluation will be carried out regarding the efficiency and effectiveness of the methods implemented by Tokopedia, Shopee, Lazada, and the proposed method (the application that has been designed in this research). The evaluation method carried out will use the Usability Evaluation method which can be used to assess the extent to which a system or product can meet user needs.

III. RESULTS AND DISCUSSION

A. Study of Literature
Based on the literature study that has been carried out, it is known that the method applied by Tokopedia, Shopee, and Lazada in providing cybersecurity information and guidance on using security features to users is through the Customer Service feature contained in the application.

B. System and Software Design

The system or application design process (pop up features and notification features) uses the Visual Studio application to assist in creating and developing application source code and the Flutter framework to assist

in creating the UI (User Interface). Meanwhile, the programming language used to create application sources is the Dart language.

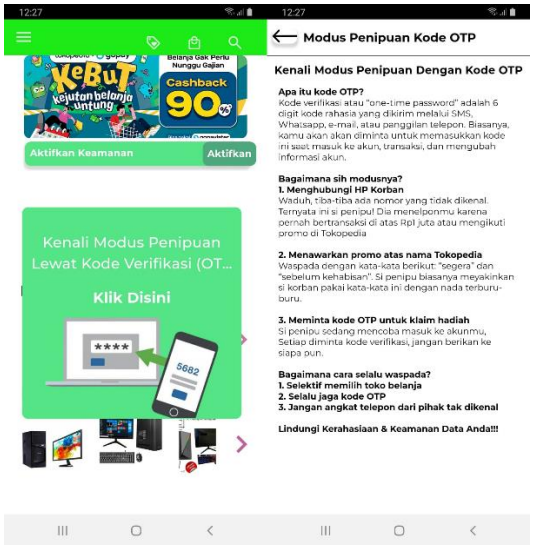

Figure 1. Pop Up Features

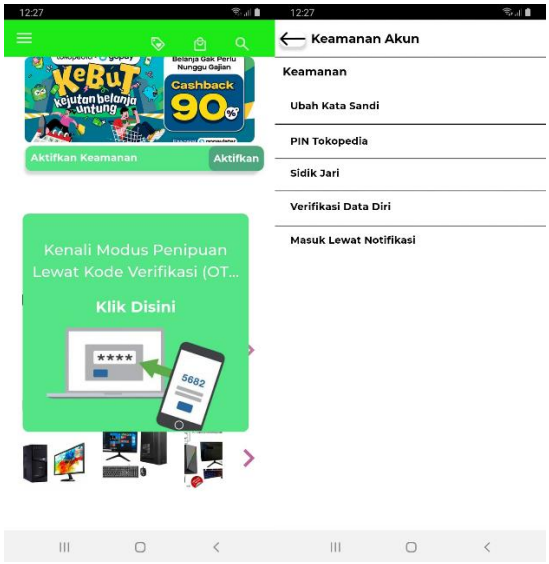

Figure 2. Notification Features

C. System Integration Testing (SIT)

After the application (pop up feature and notification feature) has been designed, independent testing will be carried out to ensure that the system and program can run as expected. Testing will be carried out by simulating a previously designed application.

D. User Acceptance Testing (UAT)

1) Testing and Evaluation Results of Methods for Providing Cybersecurity Education by Tokopedia, Shopee, Lazada, and the Pop Up Feature.

Based on the survey results, the majority of respondents considered that the methods applied by Tokopedia, Shopee, and Lazada in providing cybersecurity education to respondents or users were considered less effective in providing cybersecurity information to users widely and less efficient in reaching users proactively. The results can be seen in figure 5-10.

Meanwhile, regarding the pop up feature, the majority of respondents considered that the method of providing cybersecurity education implemented by the pop up feature was considered quite effective in providing cybersecurity information to users widely and quite efficient in reaching users proactively. The results can be seen in figures 11-12.

2) Testing and Evaluation Results of the Guide Method for Using Security Features by Tokopedia, Shopee, Lazada, and the Notification Feature.

Based on the survey results, the majority of respondents considered that the methods applied by Tokopedia, Shopee, and Lazada in providing cybersecurity education to respondents or users were considered less effective in providing guidance on using security features to users at large and less efficient in reaching users proactively. The results can be seen in figures 13-18.

Meanwhile, regarding the notification feature, the majority of respondents considered that the method of providing cybersecurity education implemented by the notification feature was considered quite effective in providing guidance on the use of security features to users at large and quite efficient in reaching users proactively. The results can be seen in figures 19-20.

3) Survey Results On Google Forms

Based on the results of a survey conducted to carry out User Acceptance Testing (UAT), the following data was produced:

e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v7i1.12100

I) Figures 3 to 4 contain information regarding respondent demographics based on the survey results obtained.

II) Figures 5 to 12 contain the results of testing and evaluating methods for providing cyber security education by Tokopedia, Shopee, Lazada, and the Pop Up Feature.

III) Figures 13 to 20 contain the results of testing and evaluation of the guide method for using security features by Tokopedia, Shopee, Lazada, and the Notification Feature.

4) Figures

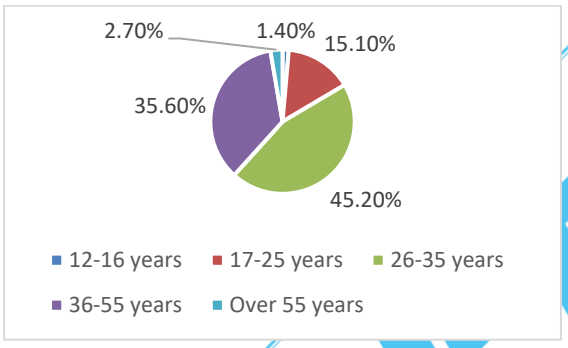

Figure 3. The age of respondents based on a survey on Google Forms.

Figure 3 contains information about the age of respondents based on data obtained from surveys on Google Forms.

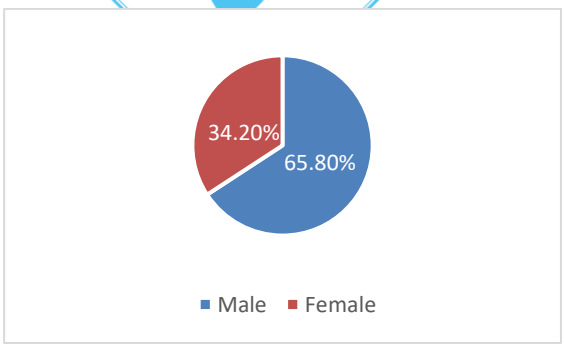

Figure 4. The gender of respondents based on a survey on Google Forms.

Figure 4 contains information about gender on respondents based on data obtained from surveys on Google Forms.

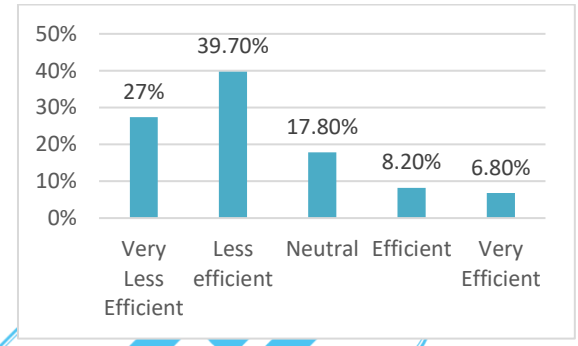

Figure 5. The efficiency of the Tokopedia method.

Figure 5 contains information about the level of efficiency of the Tokopedia method in providing cyber security education according to respondents.

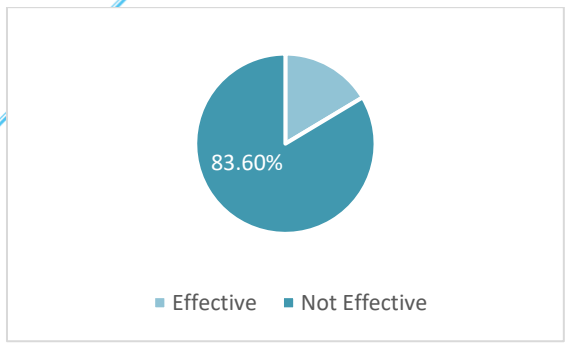

Figure 6. The effectiveness of the Tokopedia method.

Figure 6 contains information about the effectiveness of the Tokopedia method in providing cyber security education according to respondents.

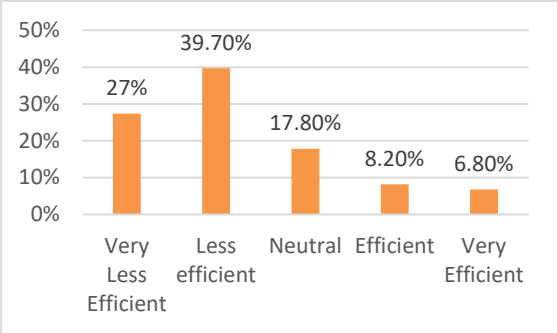

Figure 7. The efficiency of the Shopee method.

Figure 7 contains information about the level of efficiency in Shopee's method of providing cyber security education according to respondents.

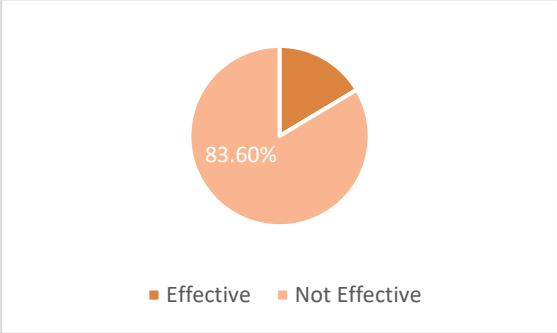

Figure 8. The effectiveness of the Shopee method.

Figure 8 contains information about the effectiveness of Shopee's method of providing cyber security education according to respondents.

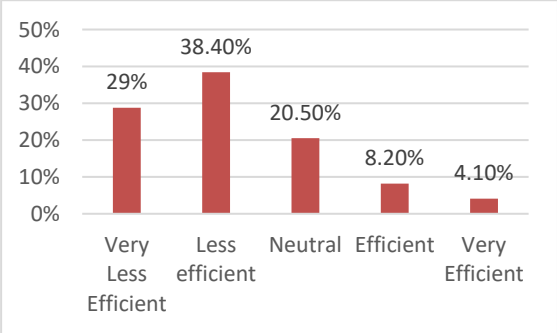

Figure 9. The efficiency of the Lazada method.

Figure 9 contains information about the level of efficiency in Lazada's method of providing cyber security education according to respondents.

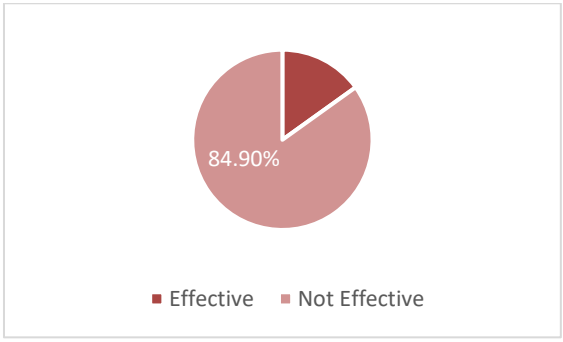

Figure 10. The effectiveness of the Lazada method.

Figure 10 contains information about the effectiveness of Lazada's method of providing cyber security education according to respondents.

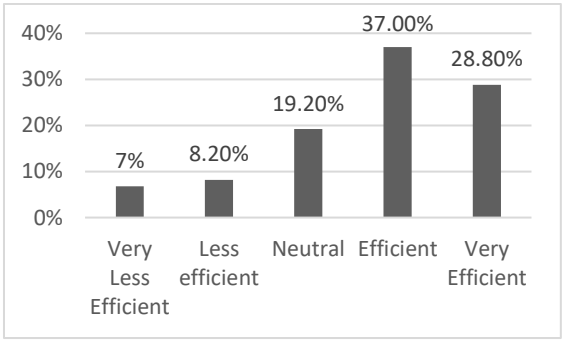

Figure 11. The efficiency of the pop up feature.

Figure 11 contains information about the level of efficiency of the pop up feature in providing cyber security education according to respondents.

e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v7i1.12100

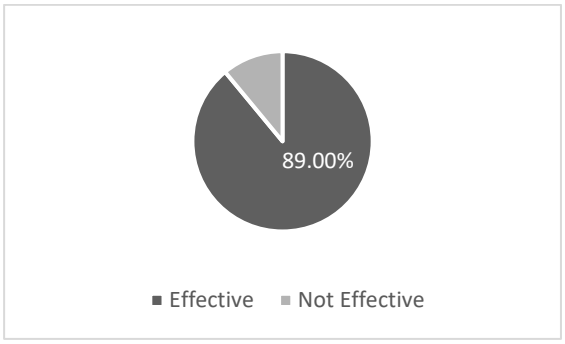

Figure 12. The effectiveness of the pop up feature.

Figure 12 contains information about the effectiveness of the pop up feature in providing cyber security education according to respondents.

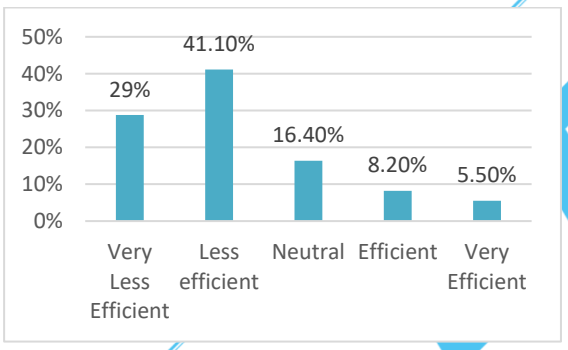

Figure 13. The efficiency of the Tokopedia method.

Figure 13 contains information about the level of efficiency of the Tokopedia method in providing guidance on the use of security features according to respondents.

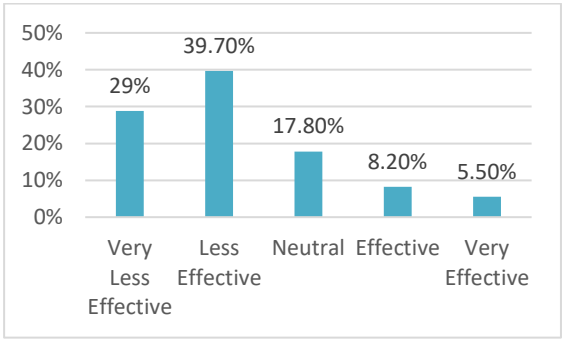

Figure 14. The effectiveness of the Tokopedia method.

Figure 14 contains information about the level of effectiveness of the Tokopedia method in providing guidance on the use of security features according to respondents.

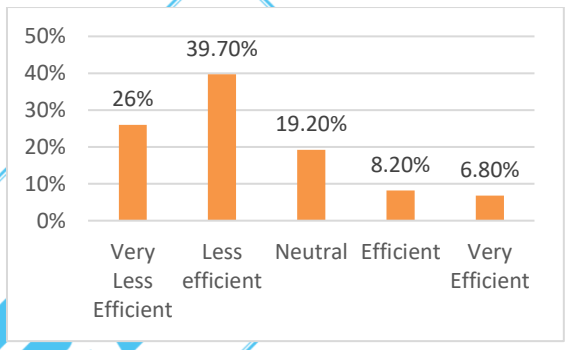

Figure 15. The efficiency of the Shopee method.

Figure 15 contains information about the level of efficiency of the Shopee method in providing guidance on the use of security features according to respondents.

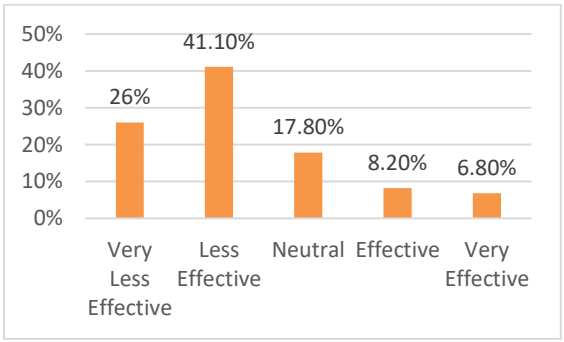

Figure 16. The effectiveness of the Shopee method.

Figure 16 contains information about the level of effectiveness of the Shopee method in providing guidance on the use of security features according to respondents.

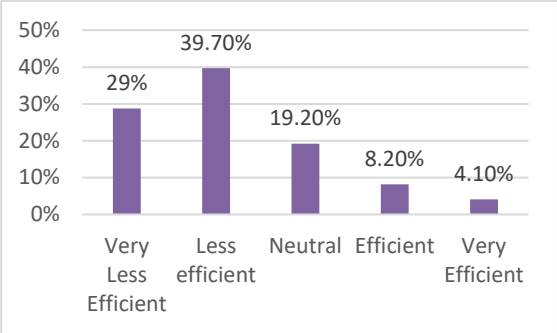

Figure 17. The efficiency of the Lazada method.

Figure 17 contains information about the level of efficiency in Lazada's method of providing guidance on the use of security features according to respondents.

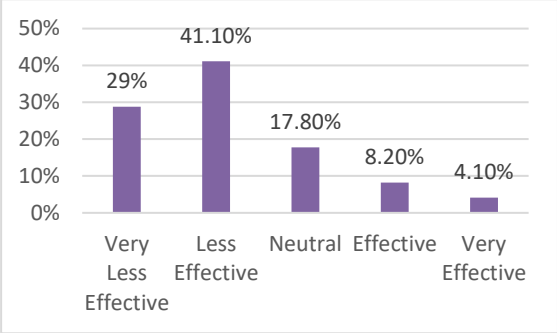

Figure 18. The effectiveness of the Lazada method.

Figure 18 contains information about the level of effectiveness of Lazada's method of providing guidance on the use of security features according to respondents.

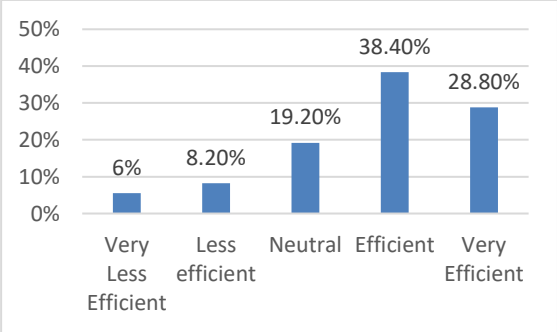

Figure 19. The efficiency of the notification feature.

Figure 19 contains information about the level of efficiency of the notification feature in providing guidance on the use of security features according to respondents.

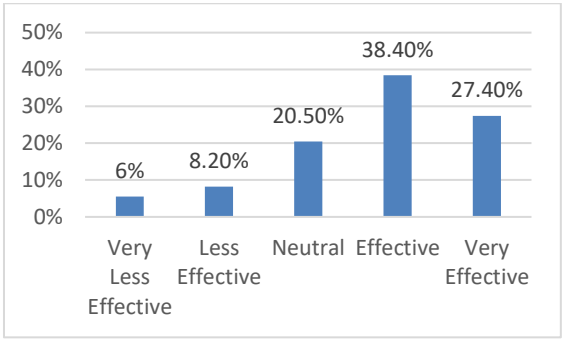

Figure 20. The effectiveness of the notification feature.

Figure 20 contains information about the level of effectiveness of the notification feature in providing guidance on the use of security features according to respondents.

5) Evaluation

From the results of tests and surveys that have been carried out, it can be concluded that the pop up and notification features have advantages in providing cybersecurity education and guidance on using security features compared to the Tokopedia, Shopee and Lazada methods, both in terms of effectiveness and efficiency.

In terms of efficiency, the proposed pop up feature can reach e-commerce users efficiently because the appearance of a pop up on the main page (home screen) can make users aware of information about the threat of cyber attacks, such as fraud modes that can threaten the security of user accounts. Meanwhile, the notification feature can also reach users efficiently because it can reach users widely and remind users to use the available security features.

In terms of effectiveness, the proposed pop up feature can appear at strategic times so that many users can obtain cybersecurity information and education. Meanwhile, the notification feature can provide direct access and remind users to use the available security features.

e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v7i1.12100

The following is a comparison table of test evaluations.

Aspect	E-Commerce Method (Tokopedia, Shopee, and Lazada)	Proposed Method (Pop Up and Notification Feature)
Tools	Customer service features	Pop up and notification features
Ways of Working	*Customer service will provide information about cyber security and information on how to use security features only when the user asks for it*	The pop-up feature will redirect to a page containing cybersecurity information when the pop up is clicked, while the notification feature will direct to a page containing security features when the "Activate" button is clicked
Efficiency	Less efficient in reaching users proactively	Quite efficient in reaching users proactively
Effectiveness	Less effective in providing information and guidance to users at large	Quite effective in providing information and guidance to users at large

IV. CONCLUSION

Based on the results of the research, the pop-up and notification features can be effectively utilized to increase security awareness and prevent the risk of fraud and other cyber threats among e-commerce users. However, several considerations should be addressed to maximize the benefits of these features:

1) Providing Comprehensive Cybersecurity Information:
The pop-up and notification features must deliver clear and actionable cybersecurity information and guidance on using security features. This will help users understand the importance of cybersecurity and how to protect themselves against phishing attacks and other cyber threats. By receiving timely cybersecurity information directly within e-commerce applications, users can enhance their knowledge and awareness, leading to a reduction in the risk of cyber incidents.

2) Ensuring Simplicity and Ease of Implementation:
It is crucial that the pop-up and notification features remain simple and user-friendly. The features should be easily integrable into existing e-commerce systems without causing significant disruptions. The simulations conducted during this research indicate that these features can be implemented effectively with minor adjustments, ensuring the features are accessible and beneficial to users.

To ensure the long-term effectiveness of these features, continuous monitoring and updates based on user feedback and evolving cyber threats are necessary. Implementing these suggestions will contribute to a safer e-commerce environment, ultimately protecting users from fraud and other cyber risks.

For future researchers, it is recommended to explore additional methods for enhancing cybersecurity awareness. Investigating the impact of various educational tools, such as video tutorials, interactive quizzes, and real-time threat simulations, can provide deeper insights into effective strategies for user education. Longitudinal studies assessing the sustained impact of these educational interventions on user behavior and overall security posture will be invaluable.

REFERENCES

Ayu, S. S., & Nasution, M. I. P. (2023). Analysis of Privacy Data Leaks in E-Commerce Tokopedia. JUEB: Journal of Economics and Business, 2(3), 21-24.

Astuti, N. K., & Atmojo, R. N. P. (2022). CONSUMER PROTECTION OF INFORMATION SECURITY RISKS

IN E-COMMERCE TRANSACTIONS. Honeste Vivere, 32(2), 98-107.

Awalia, S. A., Arhansyah, R. J., Nugroho, F. R. A., & Thapsuandji, A. A. (2024). Legal Protection for Consumers in Shopee E-commerce Transactions. Potential Journal, 3(1), 56-67.

Al Aziz, M. I., NB, M. R. A., Alauddin, M. F., & Neyman, S. N. (2024). Simulation and Cyber Security Education Efforts Using Phishing Websites. TEKTONIK: Journal of Engineering Science, 1(4), 74-80.

Djayapranata, G. F. (2023). The Influence of E-Commerce Site Service Provider Ethics on Satisfaction and Loyalty. INOBIS: Indonesian Journal of Business and Management Innovation, 6(4), 458-467.

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., ... & Virgio, V. (2023). Analysis of the Implementation of Cyber Security Systems Against Cybercrime in Indonesia. Innovative: Journal Of Social Science Research, 3(6), 1135-1145.

Hidayat, T., Likadja, J. A. C., & Derozari, P. E. (2023). Legal Protection of Consumer Personal Data in Electronic Commerce. Journal of Comprehensive Science (JCS), 2(5), 1087-1103.

Harahap, W. I., Daulay, A. R. R., Alfisyahri, P. N., & Silalahi, P. R. (2023). Analysis of PT Tokopedia's Market Place Image in Increasing Consumer Trust After User Data Leaks. CEMERLANG: Journal of Management and Business Economics, 3(1), 29-41.

Hamim, N., & Nasution, M. I. P. (2023). Analysis of Legal Protection for Privacy Data Security on the Shopee Market Place. IJM: Indonesian Journal of Multidisciplinary, 1(4), 1235-1242.

Hidayah, A. R. (2022). SANCTIONS AGAINST E-COMMERCE ORGANIZERS IF THEY FAIL TO PROTECT USER'S PERSONAL DATA. Bureaucracy Journal: Indonesian Journal of Law and Social-Political Governance, 2(2), 397-410.

Hasya, D. K., Safitri, D., Putra, D. R., Maulana, F. B. G., & Rakhmawati, N. A. (2024). Ethical Implications in Online Fraud Profiles and Strategies in E-Commerce Transactions in the Realm of Cybercrime. Journal of Innovation Research Management, 2(1), 236-247.

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Security Analysis of Personal Data on E-Commerce Users: Threats, Risks, Security Strategies (Literature Review). Journal of Applied Management Science, 4(5), 625-632.

Lisnawati, T., Hussaen, S., Nuridah, S., Pramanik, N. D., Warella, S. Y., & Bahtiar, M. Y. (2023). Risk Management in E-commerce Business: Identifying, Measuring, and Managing Associated Risks. Tambusai Education Journal, 7(2), 8252-8529.

Rohmah, R. N. (2022). Efforts to Build Cyber Security Awareness among E-commerce Consumers in Indonesia. Commerce Scholar, 6(1), 1-11.

Rahmadi, G. (2020). Analysis of Cyber Security Awareness among E-Commerce Players in Indonesia.

Syahputra, R. A., Maliza, N. O., Kasmawati, K., & Putri, C. W. A. (2024). Strategy for Increasing Public Data and Information Awareness in the Digital

e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v7i1.12100

Era. Indonesian Journal of Community Service, 5(3), 3164-3171.