SOSHUM *Jurnal Sosial dan Humaniora*
[Journal of Social Sciences and Humanities]

Volume 14, Number 3, 2024 p-ISSN. 2088-2262 e-ISSN. 2580-5622
ojs.pnb.ac.id/index.php/SOSHUM/

The Importance of Security Awareness in Combating Phishing Attacks: A Case Study of Bank Rakyat Indonesia

Dwi Wina Adani[1]✉, Ida Nurhayati[2], and R. Elly Mirati[3]

[1,2,3]Politeknik Negeri Jakarta
✉Jl. Prof. Dr. G.A. Siwabessy, Universitas Indonesia, Depok, 16425, Indonesia
✉ida.nurhayati@akuntansi.pnj.ac.id

Article Info

Article History
Received:
Aug 2024
Accepted:
Oct 2024
Published:
Nov 2024

Keywords:
Urgency, Security Awareness, Phishing Attacks

ABSTRACT

The advent of the digital world does not always have positive impacts, it often poses serious attacks that can be highly detrimental to its users, one of which is phishing. Phishing attacks are among the attacks that have been continuously rising in the digital world. With its various forms, phishing stands out as a significant attack, particularly harmful to housewives. Therefore, cultivating security awareness is of paramount importance in preventing customers from becoming victims of phishing attacks. This research aims to explain the importance of security awareness in preventing phishing and to describe the forms of security awareness in combating phishing attacks. The methodology used in this research is quantitative and qualitative methods with simple linear regression analysis, using SPSS 29.0. The sample consists of 80 respondents who are housewives using BRI mobile banking in RT.003, West Tanjung Village, Jagakarsa District, South Jakarta. Primary data collection was conducted through an interview with a BRI informant. The results of the study show that security awareness has a significant impact on reducing phishing attacks. Therefore, enhancing security awareness to prevent phishing is crucial for both individuals and banks to protect information security and avoid becoming victims of digital crimes such as phishing.

INTRODUCTION

The presence of the digital world does not always have a positive impact, it often poses serious attacks that can be detrimental to its users, one of which is phishing. The term phishing is derived from the word fishing, which means to lure. Phishing is a method in which the perpetrator sends a message containing a fake link or attachment (BCA, 2022). The targeted data includes personal information (name, age, address), account data (username and password), and financial data (credit card or bank account information) (Shaid & Jamal, 2022). Phishing encompasses various types, including scam phishing, blind phishing, spear phishing, clone phishing, whaling, vishing, pharming, and smishing (Wijoyo, Saputra, Aditia, Pratama, & Rahman, 2023).

Urgency refers to a necessity or interest that, if not addressed promptly, can lead to the disruption of other activities, necessitating immediate action (Bukhari Is, 2021). Security awareness is a field of security science that is closely related to human factors concerning the protection of information assets (Luvia Friska Narulita, 2019). The knowledge and understanding of users about the risks associated with the use of information technology can reduce the potential for phishing attacks. Therefore, possessing security awareness is essential.

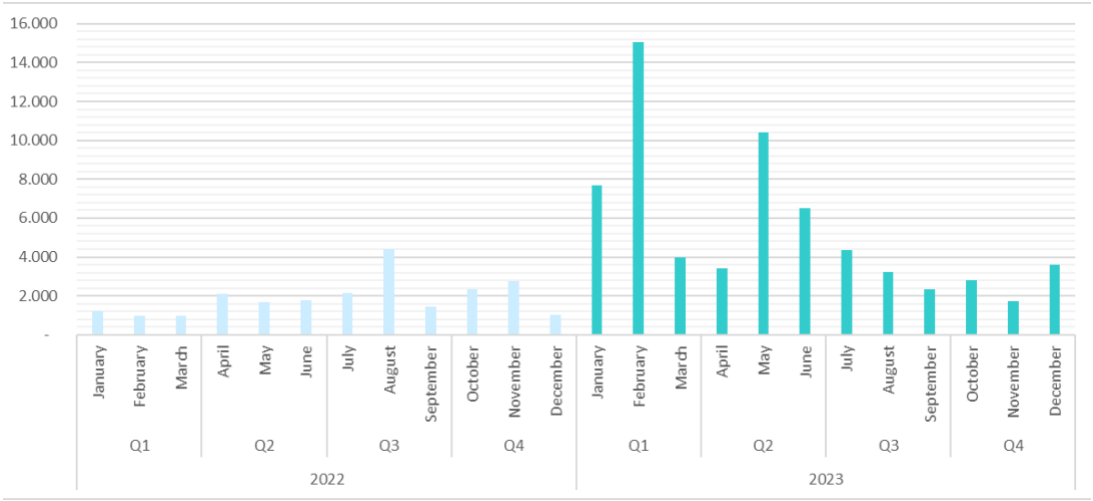

Chart 1: Phishing Attacks in 2022 and 2023
Indonesia Anti-Phishing Data Exchange (IDADX) [source]

In Chart 1 for the year 2022, the Indonesia Anti-Phishing Data Exchange (IDADX) observed that there were 4.410 phishing attacks the highest occurring in the third quarter in August. However, in 2023 phishing attacks increased in every quarter compared to the previous year. The largest increase in 2023 was in the first quarter in February with 15.050 phishing attacks, which set a new record and was the worst quarter for phishing ever observed by IDAX.

From both the banking system side and the customer side, factors contributing to breaches of customer data or phishing attacks include negligence on the part of the customers themselves, particularly in safeguarding personal data such as identity, passbooks, PIN and other personal information (Busthomi, 2023).

Bank Rakyat Indonesia (BRI) is a State Owned Enterprise (SOE) with a type of Persero. BRI launched its mobile banking service to expand its reach and make it easier for customers to conduct transactions. BRI hold the top position with the highest number of mobile banking applications, with 33,5 million users recorded in the first quarter of 2024 (CNBC Indonesia, 2024).

Ratna Aprianingsih a resident of South Sumatra who manages her husband's business finances is a customer of BRI mobile banking. Ratna fell victim to phishing losing IDR 1.4 billion when the perpetrator sent a wedding invitation file via WhatsApp, when Ratna clicked the file her data was immediately accessed by the attacker (Kompas, 2023). The case involving a housewife who is active on her Facebook account also experienced phishing. The case began when the housewife attempted to collect a savings group payment, and upon investigation, it was found that the housewife had previously clicked on a link that required her to enter her data (Kompasiana, 2024).

These phishing cases serve as a reminder to be more vigilant in safeguarding personal data, account data, and financial data at all times. Therefore, the importance of further research on security awareness to minimize and prevent phishing attacks is crucial.

Based on the background above, the author is interested and intends to conduct research titled “The Urgency of Security Awareness on Phishing Attacks (Case Study at Bank Rakyat Indonesia)”.

METHODS

The study was conducted using both quantitative and qualitative methods, analyzed with SPSS version 29.0, and supplemented with interviews with the BRI web developer team. Data was collected through a questionnaire administered to 80 respondents, who use BRI mobile banking in RT.003, Tanjung Barat Village, Jagakarsa Subdistrict, South Jakarta. The questionnaire was distributed directly to respondents, allowing for immediate clarification of each question, which facilitated understanding. This method was chosen because housewives in RT.003 often gather for community events such as religious gatherings and savings clubs, making it easier to reach them. The study utilized a

non-probability sampling technique with an incidental sampling type to select participants. The data was classified based on age, the highest level of education, and whether the respondents had occupations other than being housewives. The study included validity testing, reliability testing, normality testing, simple linear regression analysis, and t-test (partial). The research framework of this study is:

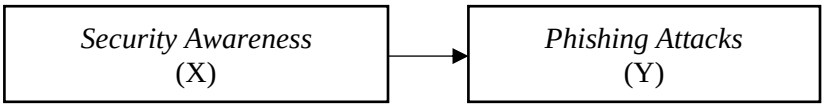

Chart 2: Framework of thought

RESULTS AND DISCUSSION

This study was conducted using both quantitative and qualitative methods, analyzed with SPSS version 29.0 and supplemented with interviews with interviews with the bank's web developer. The data was collected through a questionnaire administered to housewives using BRI mobile banking in RT.003, Tanjung Barat Village, Jagakarsa Subdistrict, South Jakarta. The data was classified based on age, highest level of education, and whether the respondents had occupations other than being housewives.

No.	Age	Amount	Percentage
1	21 - 30 Year	15	19%
2	31 - 40 Year	15	19%
3	41 - 50 Year	30	37%
4	≥ 50 Year	20	25%
	Total	80	100%

Table 1: Respondent Characteristics based on Age
Data processed, 2024 [source]

No.	Highest Level of Education	Amount	Persentase
1	SMP	8	10%
2	SMA/SMK	39	49%
3	Diploma	19	24%
4	S1	13	16%
5.	S2	1	1%
	Total	80	100%

Table 2: Respondent Characteristics Based on Highest Level of Education
Data processed, 2024 [source]

No.	Occupation	Amount	Persentase
1	Yes	42	52%
2	No	38	48%
	Total	80	100%

Table 3: Respondent Characteristics Based on Occupation
Data processed, 2024 [source]

Based on the age characteristics, the largest group of respondents was between 41 and 50 years old, generally, it can be stated that individuals in this age group are still capable of using BRI mobile banking which is a digital product for managing their finances. Regarding the highest level of education, the majority of respondents had completed high school or vocational school (SMA/SMK). Educational background indeed has a significant impact on an individual's awareness of digital security. However, as times have progressed society has increasingly connected with the digital world. Therefore, both high and low-educated housewives are capable of using BRI mobile banking. Thus, the respondents understand each item in the questionnaire. Regarding whether the respondents had occupations other than

being housewives, the most common result was that 42 respondents had jobs in addition to their role as housewives. Housewives with jobs have different needs when using BRI mobile banking, such as requiring quick access, ease of use, and 24-hour availability to assist them in conducting financial transactions.

The author uses an independent variable namely security awareness and a dependent variable namely phishing. Security awareness refers to an individual's knowledge, attitude, and behaviour aimed at protecting personal information after choosing to use mobile banking. Security awareness has three important dimensions knowledge, attitude, and behavior.

Statements	Answers				Total	Empirical Score	Maximum Score	Achievement
	STS	TS	ST	SS				
Security Awareness (X)								
								Knowledge
X.1	0	10	36	34	80	264	320	82,5 %
X.2	0	4	27	49	80	285	320	89,1 %
X.3	0	3	38	39	80	276	320	86,3 %
X.4	0	0	28	52	80	292	320	91,3 %
X.5	0	4	35	41	80	277	320	86,6 %
								Attitude
X.6	0	0	33	47	80	287	320	89,7 %
X.7	1	0	30	49	80	287	320	89,7 %
X.8	1	0	27	52	80	290	320	90,6 %
X.9	1	0	28	51	80	289	320	90,3 %
								Behaviour
X.10	1	3	35	41	80	276	320	86,3 %
X.11	0	1	32	47	80	286	320	89,4 %
X.12	2	1	25	52	80	287	320	89,7 %
X.13	1	0	28	51	80	289	320	90,3 %
X.14	1	1	28	50	80	287	320	89,7 %
X.15	1	0	31	48	80	286	320	89,4 %

Table 4: Distribution of Each Question on the Security Awareness Variable (X)
Data processed, 2024 [source]

Statements	Answers				Total	Empirical Score	Maximum Score	Achievement
	STS	TS	ST	SS				
Phishing (Y)								
Y.1	1	3	48	28	80	263	320	82,2 %
Y.2	1	6	44	29	80	261	320	81,6 %
Y.3	3	21	29	27	80	240	320	75,0 %
Y.4	2	3	33	42	80	275	320	85,9 %
Y.5	3	1	39	37	80	270	320	84,4 %
Y.6	2	3	37	38	80	271	320	84,7 %
Y.7	1	13	38	28	80	253	320	79,1 %
Y.8	0	16	32	32	80	256	320	80,0 %
Y.9	0	0	34	46	80	286	320	89,4 %

Table 5: Distribution of Each Question on the Phishing Variable (Y)
Data processed, 2024 [source]

Based on the result of the highest achievement index in the distribution of each statement for the security awareness variable, it is found that 91,3% of respondents in the knowledge dimension are aware of the importance of updating mobile banking applications for security. In the attitude dimension, 90,6% of respondents feel the need to continuously

learn the latest ways to maintain security related to the mobile banking they use. In the behavior dimension 90,3% of respondents have used unique passwords to protect their mobile banking they use. In the behaviour dimension, 90,3% of respondents have used unique passwords to protect their mobile banking accounts. Meanwhile, based on the results of the highest achievement index in the distribution of each statement for the phishing variable, 89,4% of respondents believe that more education is needed to combat phishing attacks targeting mobile banking users.

Based on the results of the questionnaire distribution for the phishing variable, it was found that 28 housewives using BRI mobile banking strongly agreed they had received suspicious links or files, 29 respondents strongly agreed they had received suspicious emails, 27 respondents strongly agreed they had visited websites that appeared legitimate but were fake, 42 respondents strongly agreed they had received suspicious phone calls, 37 respondents strongly agreed they had received urgent emails requesting payments, 38 respondents strongly agreed they had received SMS messages claiming to award prizes, and 32 respondents strongly agreed they had avoided scams claiming to be from a bank. These results indicate that phishing among housewives occurs relatively frequently, which can pose significant risks for respondents who lack good security awareness.

Nevertheless, these results indicate that BRI mobile banking users understand the importance of safeguarding against phishing attacks. These findings are consistent with research conducted by (Suprio & Farid, 2022), which found that 70% of respondents were aware of the importance of information security against phishing. Additionally, the study (Dafid & Dorie, 2020) found that respondents had an awareness level of 71%. These findings are also supported by research conducted by (Nasution & Santoso, 2021), which found that 60,15% of respondents were aware of phishing. However, this differs from the study by (Sari, Hariyadi, & Sahtyawan, 2022), which found a lack of awareness among respondents on phishing. Additionally, earlier research (Vadila & Pratama, 2021) also found that respondents were not yet aware of phishing attacks. Moreover, the study by (Luvia Friska Narulita, 2019) also found that respondents' awareness of security was still low. These differences are due to the specific demographic and educational backgrounds of the respondents in this research, as well as the differences in methodologies employed in the studies.

The observed differences in awareness levels across various studies highlight the importance of ongoing education and outreach, particularly in the context of respondents who are housewives. This suggests that while certain groups may be more informed, other groups, such as housewives with diverse educational backgrounds and ages, remain vulnerable to phishing risks. This underscores a critical area for future research and intervention. These differences also indicate the necessity for tailored educational programs that take into account the unique characteristics of housewives, including factors such as education, age, and employment status. Therefore, understanding these disparities not only informs future studies but also aids in developing effective strategies to enhance security awareness among all users, especially within the housewife demographic.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	10,643	4,576		2,326	,023
	X	,358	,086	,427	4,175	<,001

a. Dependent Variable: Y

Table 6: Simple Linear Regression Analysis Results and t-Test (Partial) Results
The data were processed using SPSS version 29.0, 2024 [source]

Based on the results of the simple linear regression test, the regression coefficient for X is 0,358, indicating that for every 1 unit increase in security awareness, the phishing value increases by 0,358. Thus, it can be said that the direction of the effect of variable X on Y is positive. Additionally, the t-test results show that the probability (sig) is 0,001 which is less than 0,05 and the calculated t value is 4,175 which is greater than the t table value of 1,990. Therefore it can be concluded that the alternative hypothesis (Ha) is accepted, which states that “there is an urgency of security awareness on phishing attacks at Bank Rakyat Indonesia (BRI).” This means that increased security awareness has a significant

effect on detecting preventing and reporting more phishing incidents. Enhanced security awareness will prevent potential victims or targets of phishing from being caught or falling victim to digital crimes such as phishing.

Awareness of security is a very urgent context for preventing BRI customers from becoming future victims of phishing. According to an interview with Mr Hans Evan Tatipatta from the Web Developer department at Bank Rakyat Indonesia (BRI), BRI has implemented various measures to increase customers' knowledge about phishing attacks, including routine education through email, SMS, and social media, conducting campaigns such as webinars and seminars, and enhancing the security features of the mobile banking application. Phishing attacks also pose a challenge for BRI in its operations, reflecting the need for adjustments in behaviour to handle security incidents.

Question	Answare
1. What actions does Bank Rakyat Indonesia take to maintain security awareness among its customers regarding phishing attacks?	1. Conducting regular education through email, SMS, and social media about phishing tactics. 2. Organizing security awareness campaigns such as webinars and seminars. 3. Enhancing security features in the mobile banking application.
2. Based on the phishing threats, are there any operational obstacles faced by Bank Rakyat Indonesia?	Yes, banking services can be disrupted when handling phishing incidents, leading to decreased customer trust and potential financial losses. Therefore, additional resources are needed for rapid response and recovery.
3. Are there many customers who become victims of phishing?	Not too many.
4. What types of phishing are frequently experienced by Bank Rakyat Indonesia customers?	Email phishing, smishing, vishing, fake websites, and phishing through social media...
5. What steps does Bank Rakyat Indonesia take if a customer becomes a victim of phishing?	1. Access Termination Disabling access to the affected customer's account to prevent further unauthorized access. 2. Identity Verification Verifying the customer's identity to ensure the authenticity of the report and for further security measures. 3. Account Recovery Assisting the customer in recovering access to their account by resetting passwords and implementing other security measures. 4. In-Depth Investigation Investigating to determine the source and methods of the phishing attack and its impact on the customer. 5. Refund Processing If there is a financial loss, processing refunds after necessary verification and validation. 6. Education and Security Advice

		Providing the customer with education on how to avoid future phishing attacks and offering security advice.
6.	How long does Bank Rakyat Indonesia take to resolve phishing incidents affecting its customers?	From several days to several weeks, depending on the complexity of the case and the procedures required to ensure full security and recovery for the customer.
7.	Does the time taken to resolve phishing attacks on customers disrupt Bank Rakyat Indonesia's operations?	Yes, it does cause disruption.

Table 7: Interview Results
Primary data, 2024 [source]

Services at BRI can be disrupted when handling phishing incidents, leading to reduced customer trust and potential financial losses, reflecting changes in attitude caused by a lack of awareness about phishing attacks. Therefore, additional resources are needed for rapid response and recovery. Although not many customers have become victims of phishing, the attitude towards potential attacks still needs attention. Types of phishing frequently experienced by BRI customers, such as phishing emails, smishing, vishing, fake websites, and phishing through social media, highlight the need for improved knowledge regarding digital security.

There are several steps that BRI will take if a customer becomes a victim of phishing. First, access will be terminated by disabling access to the affected customer's account to prevent further unauthorized access, reflecting a rapid response. Second, identity verification will be conducted to ensure the authenticity of the report, account recovery, and other security measures, reflecting technical knowledge of security procedures. Third, a thorough investigation will be carried out to determine the source and methods of the attacks and their impact on BRI customers, with refunds issued if there are financial losses, and the refund process conducted after necessary verification and validation, demonstrating knowledge to understand and address phishing attacks. Fourth, education and security advice will be provided, giving BRI customers knowledge on how to avoid future phishing attacks and offering security recommendations through in-depth investigation to understand the sources and methods of phishing attacks and their impact on BRI customers.

The resolution of phishing crimes affecting BRI customers requires a time frame of several days to several weeks, depending on the complexity of the case and the procedures involved, indicating that response behaviour affects BRI operations. The time spent resolving phishing attacks impacting BRI customers disrupts operations, reflecting the need for adjustments in behaviour to handle security incidents. Therefore, increasing awareness to prevent phishing is crucial for both individuals and BRI to maintain information security. The findings of this study support the awareness theory proposed by (Mitnick & Simon, 2002) (Amin, 2014) that humans are the primary and crucial factor in information security, in addition to advanced technology systems, as humans are the weakest link in the security chain.

CONCLUSION

This study demonstrates that security awareness plays a crucial role in preventing phishing at Bank Rakyat Indonesia (BRI). Data analysis results identify that respondents have a high level of security awareness regarding the importance of safeguarding mobile banking applications. The strength of this research lies in identifying a significant relationship between increased security awareness and phishing prevention. However, this study is limited to general types of phishing, indicating that there is still room for exploration of other phishing types such as spear phishing and whaling.

The practical application of this research suggests that BRI should continue to conduct routine security education for its customers, including disseminating information about recent phishing cases. On the other hand, mobile banking users, particularly housewives, are encouraged to maintain and enhance their security awareness.

ACKNOWLEDGEMENT

The author expresses gratitude to Mrs. Dr. Ida Nurhayati, S.H., M.H., the undergraduate thesis supervisor in the Finance and Banking program at the State Polytechnic of Jakarta, for the support and assistance in providing input for this writing.

REFERENCES

Amin, M. (2014). Pengukuran Tingkat Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MCDA). *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Vol. 5 No. 1*, 2.

BCA. (2022, 03 02). *bca.co.id*. Diambil kembali dari BCA: https://www.bca.co.id/id/informasi/awas-modus/2022/03/02/04/12/awas-modus-phising-yang-bisa-membahayakan-akun-perbankan

Bukhari Is, P. R. (2021). Urgensi Pengkajian dan Penelitisn Bagi Insan Akademik. *Tarbiyatul Bukhary, Jurnal Pendidikan, Agama dan Sains*, 4.

Busthomi. (2023, Maret 18). *Kasus Cyber Crime, Literasi Keuangan Rendah Pemicu Nasabah Rugikan Diri Sendiri*. Diambil kembali dari TopBusiness: https://www.topbusiness.id/74917/kasus-cyber-crime-literasi-keuangan-rendah-pemicu-nasabah-rugikan-diri-sendiri.html

CNBC Indonesia. (2024, June 10). *Cashless Makin Digemari, Ini 5 Digital Banking Pilihan Warga RI*. Diambil kembali dari CNBC Indonesia: https://www.cnbcindonesia.com/research/20240610063016-128-545113/cashless-makin-digemari-ini-5-digital-banking-pilihan-warga-ri#:~:text=Total%20pengguna%20mobile%20banking%20bank,sebesar%2025%2C7%20juta%20pengguna.

Dafid, & Dorie. (2020). Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa. *Jurnal Teknik Informatika dan Sistem Informasi*, 3.

Indonesia Anti-Phishing Data Exchange. (2022). *Phishing Activity Trends Reports Periode Quarter 1 - Quarter 4*. Diambil kembali dari idadx.id: https://idadx.id/report-all

Indonesia Anti-Phishing Data Exchange. (2023). *Phishing Activity Trends Reports*. Diambil kembali dari idadx.id: https://idadx.id/report-all

Kompas. (2023, October 31). *Pelaku "Phishing" Kuras Tabungan Ratna*. Diambil kembali dari Kompas.com: https://regional.kompas.com/read/2023/10/31/204000478/pelaku-phishing-kuras-tabungan-ratna-uang-rp-1-4-m-hasil-dagang-mendadak?page=all

Kompasiana, S. A. (2024, Februari 16). *Seorang Ibu Rumah Tangga Terkena Aksi Phishing yang Merugikan: Media Sosial Facebook*. Diambil kembali dari Kompasiana: https://www.kompasiana.com/shaktyadjie5385/65ce62f3c57afb28091a1f33/seorang-ibu-rumah-tangga-terkena-aksi-phishing-yang-merugikan-media-sosial-facebook#google_vignette

Luvia Friska Narulita, A. K. (2019). Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Ibu Rumah Tangga dan Remaja di Desa Jrebeng, Kecamatan Dukun, Kabupaten Gresik. *SNHRP-II : Seminar Nasional Hasil Riset dan Pengabdian, Ke-II, 2019*, 4.

Mitnick, K. D., & Simon, W. L. (2002). *The Art Of Deception.* Robert Ipsen.

Nasution, M. A., & Santoso, J. D. (2021). Analysis of Community Awareness Against Threats to Personal Data Security Through Phishing Websites. *The IJICS (International Journal of Informatics and Computer Science)*.

Sari, I. D., Hariyadi, D., & Sahtyawan, R. (2022). Analisis Tingkat Security Awareness-Personal Threat Terhadap Ancaman Phishing Dengan Metode Technology Threat Avoidance Theory (TTAT). *Teknomatika Unjaya*.

Shaid, & Jamal, N. (2022, 11 25). *Apa Itu Phising: Definisi, Cara Kerja, Ciri-ciri, dan Cara Mencegahnya*. Diambil kembali dari Kompas.com: https://money.kompas.com/read/2022/06/16/183024326/apa-itu-phising-definisi-cara-kerja-ciri-ciri-dan-cara-mencegahnya?page=all

Suprio , Y. A., & Farid, M. (2022). Pengelompokan Tingkat Kesadaran Masyarakat Tentang Pentingnya Keamanan Informasi Data Pribadi Berdasarkan Clusterisasi K-Means Menggunakan Euclidien Distance. *Jurnal Informatika, Manajemen dan Komputer*.

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Universitas Islam Indonesia.*

Wijoyo, A., Saputra, A., Aditia, Pratama, M. R., & Rahman, R. (2023). Analisis Serangan Phising dan Strategi Deteksinya. *JRIIN: Jurnal Riset Informatika dan Inovasi*, 2-3.