DOI: https://doi.org/10.70656/ijcse.v2i01.498

Analysis of Phishing Link Attack Threats to User Account Security

Riskha Syofiyana
Department of Informatics
Universitas Islam Negeri K.H. Abdurrahman Wahid
Pekalongan,Indonesia
riskha.syofiyana24076@mhs.uingusdur.ac.id

Indri Oktavia Ramadani
Department of Informatics
Universitas Islam Negeri K.H. Abdurrahman Wahid
Pekalongan,Indonesia
indri.oktavia.ramadani24078@mhs.uingusdur.ac.id

Annisa Larasati
Department of Informatics
Universitas Islam Negeri K.H. Abdurrahman Wahid
Pekalongan,Indonesia
annisa.larasati24086@mhs.uingusdur.ac.id

Aghitsna Yashiva Aulia Ahabbany
Department of Informatics
Universitas Islam Negeri K.H. Abdurrahman Wahid
Pekalongan,Indonesia
aghitsna.yashiva.aulia.ahabbany24090@mhs.uingusdur.ac.id

Dicky Anggriawan Nugroho
Department of Informatics
Universitas Islam Negeri K.H. Abdurrahman Wahid
Pekalongan,Indonesia
dicky.anggriawannugroho@uingusdur.ac.id

Abstract*—This study examines the threat of phishing link attacks to user account security by tracing common attack patterns, user behavior, and system vulnerabilities. The study explains how attackers use fake URLs to trick users into unknowingly providing personal information and login credentials. Through qualitative analysis of several phishing case studies, it was found that low user awareness, weak link verification habits, and lack of protection at the platform level significantly increase the risk of credential theft. This research also emphasizes the importance of implementing multi-factor authentication, URL filtering, and ongoing user education as mitigation efforts to minimize the impact of phishing attacks. The findings of this study provide insight into effective prevention strategies that can improve user account security and support the development of more robust authentication systems.

Keywords- Phishing, link attacks, account security, user behavior, cyber threat analysis

I. INTRODUCTION

The increase in digital activity in Indonesia, ranging from the use of social media and digital banking services to e-commerce, has led to a rise in the number of online accounts used by the public. However, this development has been accompanied by an increase in cases of data theft and account hacking, particularly through phishing link attacks. These attacks use fake links that mimic official websites to steal sensitive information such as usernames, passwords, and OTP codes. Low digital security literacy and the lack of additional security features such as two-factor authentication (2FA) further increase the risk of users becoming victims.

A number of studies show that phishing attacks utilize social engineering and the visual similsrity of fake websites to deceive victims. [1]explains that phishing techniques continue to evolve in line with internet usage trends. [2] found that the habit of users opening links without verification is a major factor in the success of attacks. Furthermore, [3] emphasizes that phishing links are now spread through various channels such as email, instant messaging, and social media, thereby expanding the threat.

Although many studies discuss phishing attack detection and patterns, research on the level of digital security awareness among users in Indonesia, particularly in relation to phishing link attacks, is still limited. This indicates a gap in research on how users understand threats, vulnerability factors, and the most common means of dissemination they encounter.

Therefore, this study aims to analyze the threat of phishing link attacks to user account security by identifying the modus operandi, vulnerability factors, means of dissemination, and user awareness levels regarding digital security. This study is expected to provide a comprehensive overview and more effective prevention recommendations.

II. LITERATURE REVIEW

A. Introduction Literature Review

Phishing is a form of cybercrime that has grown alongside society's increasing dependence on digital services. These attacks use social engineering techniques to convince victims to voluntarily provide sensitive information. This literature review was compiled to comprehensively understand the phenomenon of phishing through an analysis of several journals grouped into six themes: how phishing works, user vulnerability factors, the impact of attacks, methods of dissemination, preventive measures, and user awareness levels. This thematic division aims to provide a structured overview of how attacks occur, why users become victims, what the consequences are, and how these risks can be minimized.

B. How Phishing Works

Phishing works by impersonating a trusted party to lure victims into providing personal information. Perpetrators usually send links, messages, or fake websites that are designed to resemble official sites so that victims do not

realize that the page is not authentic [4]. When victims access these links and enter sensitive data, perpetrators can access devices, collect data, or install malware without the victims' knowledge [4].

In certain methods, perpetrators create fake login sites that resemble the original sites, so that after victims enter their credentials, the data is sent directly to the perpetrators through automatic mechanisms such as the Telegram bot API [5]. Phishing attacks do not directly hack into systems, but rather trick victims into voluntarily providing access. By exploiting user negligence, perpetrators can take over accounts, steal personal information, and carry out further fraud [5].

C. User Vulnerability Factors

User vulnerability to phishing is mainly caused by low awareness and digital literacy, especially in identifying online threats [6]. Many users do not understand the characteristics of malicious messages, compounded by the high intensity of internet use among teenagers who are often exposed to suspicious links [6]. The lack of digital security education further increases the potential for users to fall victim to attacks [7].

Age and region of residence also influence vulnerability levels. Older users have lower security awareness than younger users, while users outside Java tend to have lower digital literacy [7]. Overall, vulnerability arises from a combination of poor digital literacy, limited understanding of technology, lack of security education, and demographic factors [6], [7].

D. The Impact of Phishing Attacks

Phishing has a significant impact in the form of financial losses, identity theft, and personal information leaks [5]. The increase in the number of phishing sites shows that this threat continues to grow. Data such as email addresses and phone numbers can be used to access other services, thereby increasing the risk of loss [5].

One notable case was the hacking of BRI accounts in West Sumatra, where victims lost more than one billion rupiah after entering their personal data on a fake link. In addition to financial losses, phishing attacks also result in privacy violations and data misuse, which can impact various sectors that rely on digital transactions.

E. Phishing Distribution Media

Social media and messaging apps have become the primary means of spreading phishing due to high user activity. Perpetrators use platforms such as WhatsApp to send malicious links, fake PDF files, or APK applications that appear to be official documents. Fake identities such as government agencies or banks are often used to make messages appear credible [8].

Spread also occurs through fake accounts on social media that appear credible in order to spread links to fake login pages designed to steal sensitive data such as email addresses or passwords [9]. In addition, multimedia files or modified applications containing malware are often used to take over victims' accounts. These techniques take advantage of users' negligence in not verifying the authenticity of files or the identity of the sender. The spread of phishing relies heavily on social engineering, identity theft, and message sharing features on digital platforms [8].

F. Phishing Prevention Measures

Preventing phishing requires a comprehensive strategy. User education is the most fundamental step because a good understanding of the signs of phishing helps individuals recognize suspicious messages or links before they cause harm [10]. Users also need to utilize security technologies such as two-factor authentication (2FA), spam filters, and regular software updates to reduce the risk of illegal access to accounts [10]. In addition, device and application security must be maintained by only downloading applications from official sources, checking application permissions, and performing regular system updates to close potential loopholes that could be exploited by perpetrators [10].

Practices such as avoiding the use of public Wi-Fi for sensitive activities and checking the authenticity of messages or links before opening them are also very important [10]. At the platform level, protection is strengthened through encryption (SSL/TLS), threat reporting features, and detection of suspicious activity. Effective prevention requires collaboration between users, digital service providers, governments, and security experts in sharing threat information and mitigation strategies [10]. With consistent implementation of these measures, the chances of users falling victim to phishing can be significantly reduced [10].

G. User Awareness Level Regarding Phishing

Public awareness of phishing remains low to moderate, making many users easy targets for digital fraud. Most social media users do not understand the characteristics and risks of phishing, so warning signs are often ignored [10]. One study shows that only about 35% of users can actually recognize phishing, while the majority still have difficulty distinguishing genuine messages from manipulative attacks that use social engineering techniques [10].

Another study using the K-Means method also found similar patterns. Of the 30 respondents, only 17% were classified as having high awareness, while 57% were at a moderate level and 26% at a low level [11]. These differences in awareness levels were influenced by factors such as education, age, intensity of internet use, and access to security information. Users with low awareness tended to open links without checking them, while those who were more aware were usually more cautious and able to recognize the signs of dangerous links [11].

The two studies confirm that low digital literacy and cybersecurity awareness are the main reasons why phishing remains highly effective. Due to uneven levels of user awareness, more intensive digital security education is urgently needed to reduce the risk of online fraud [10], [11].

H. Literature Review Synthesis

The literature shows that phishing works by exploiting social engineering that targets user negligence. User vulnerability caused by low digital literacy and lack of education makes these attacks very effective. The impact can be financial loss, privacy violations, and account takeover. Widespread dissemination, especially through WhatsApp and social media, accelerates the spread of attacks. Although preventive measures are available, their effectiveness is highly dependent on the level of user awareness. The lack of user knowledge is a major gap in research as to why phishing attacks are still very difficult to contain. Therefore, your

group's research journal is relevant in addressing this gap through phishing threat analysis and digital security enhancement strategies.

No	Journal Title	Platform used
1.	Digital Fraud Through Phishing Links.	Email, WhatsApp, Telegram, Facebook, other digital media.
2.	Instagram Follower Fraud: Analysis of Phishing Attacks and Their Impact on Data Security	Fake Websites, Instagram, Telegram Bots
3.	Analysis of Cybersecurity Awareness among Social Media Users in Indonesia	WhatsApp, Instagram, Twitter (X), Facebook, Line, YouTube
4.	Raising Teenagers' Awareness of Phishing Through Digital Literacy: A Case Study at Darussalam Vocational High School in Makassar	Social Media, Email, Fake Websites
5.	Analysis of Online Fraud Communication Networks Through WhatsApp Messenger Social Media	WhatsApp Messenger
6.	Phishing in the Social Media Era: Identifying and Preventing Threats on Social Platforms	Popular Social Media, Fake Websites
7.	Analysis of Security Awareness Against Phishing Threats	Email, Fake Website
8.	Analysis of Public Awareness of the Dangers of Internet Phishing Using K-Means Clustering	The Internet in General

III. METHOD

This study uses a descriptive approach with a mixed method that combines qualitative and quantitative techniques. This approach was chosen to provide a comprehensive understanding of link-based phishing attack patterns, user vulnerability factors, and user awareness levels regarding digital account security.

A. Data Collection Techniques

Primary data was collected through an online questionnaire using Google Forms distributed to internet users in Indonesia. The questionnaire was designed to explore users' experiences with phishing attacks, their level of knowledge, and their digital security practices.Secondary data was obtained from scientific journals, industry reports, and other relevant literature related to phishing attacks and digital account security.

B. Research Instruments.

The main instrument in this study was a structured questionnaire containing closed and semi-open questions about user experiences, phishing dissemination media, alertness levels, and user responses to these threats.In addition, a literature review was conducted to identify previous research findings related to attack patterns, risk factors, and prevention strategies.

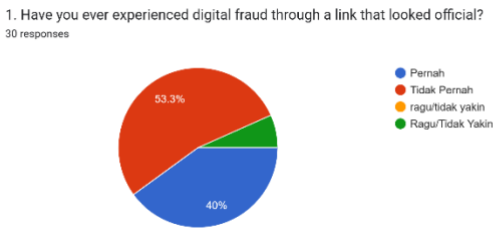
C. Research Techniques

Quantitative data from the questionnaire was analyzed using descriptive statistics to determine users' level of knowledge, experience, and digital security practices. Qualitative data from the literature study was analyzed thematically to identify attack patterns, risk indicators, and prevention methods reported in the literature.The results of both analyses were then synthesized to answer the research questions and provide a comprehensive overview of users' vulnerability to link-based phishing attacks.

IV. RESULTS AND DISCUSSION

This section presents the results obtained from the survey regarding user experiences, perceptions, and awareness related to digital fraud, particularly phishing attacks delivered through malicious links. The findings are analyzed and interpreted in relation to previous studies on cybersecurity and social engineering.Pengalaman Menjadi Korban Penipuan Digital.

A. Experiencee with Digital Fraud



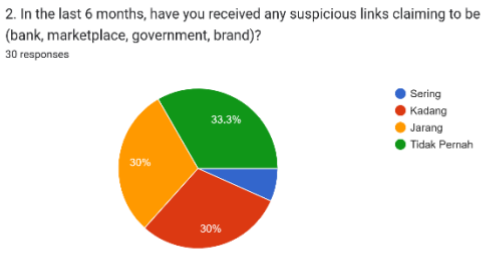
Note: 1"Tidak Pernah" = Never;"Pernah" = Ever;"Ragu/Tidak Yakin" = Unsure.

Survey results indicate that the majority of respondents reported never experiencing digital fraud, although a noteworthy portion stated that they had been victims of such incidents. A number of respondents also selected the unsure option, suggesting that some users may lack sufficient understanding to identify phishing attempts or digital fraud indicators.

This aligns with prior research showing that limited digital literacy contributes to users' difficulty in recognizing whether a link or message is legitimate or malicious.

DOI: https://doi.org/10.70656/ijcse.v2i01.498

B. *Frequency of Receiving Suspicious Links*

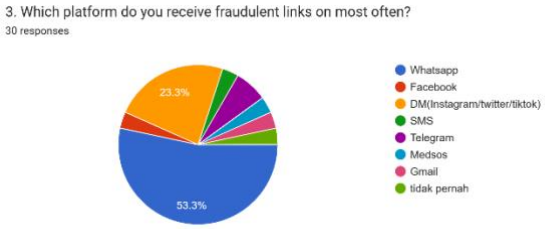


Note: 2 "Tidak Pernah" = Never; "Jarang" = Rarely; "Kadang" = Sometimes; "Sering" = Often.

Over the past six months, most respondents reported rarely or occasionally receiving suspicious links that claimed to originate from official institutions. A smaller portion reported frequent exposure to such links.

These results suggest that phishing remains a persistent threat in users' daily digital activities. The findings are consistent with studies that highlight the increasing prevalence of phishing as a common method of cyberattack.

C. *Platforms Used for Phishing Link*



Note: 3 "WhatsApp" = WhatsApp; "DM Instagram/Twitter/TikTok" = Direct Message (Instagram/Twitter/TikTok); "Gmail" = Gmail; "Facebook" = Facebook; "Telegram" = Telegram; "SMS" =SMS; "Medsos" =Social Media; "Tidak Pernah" =Never

The survey found that WhatsApp is the most commonly used platform for distributing phishing links. The next most frequent platforms include Instagram/Twitter/TikTok direct messages, while a smaller number of respondents reported receiving suspicious links through email, Telegram, or SMS.

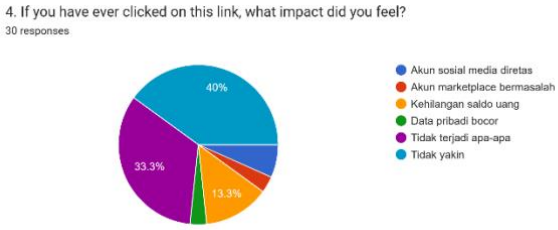
The dominance of WhatsApp suggests that attackers intentionally target platforms with high user engagement, especially personal messaging apps where users may naturally trust the sender.

D. *Impact Experienced After Clicking the Link*

Respondents who had clicked suspicious links reported varying impacts, including:

- no noticeable effect,
- loss of money,
- hacked social media accounts,
- leaked personal data, and
- issues with online marketplace accounts.

Although many users did not experience immediate consequences, the findings confirm the potentially severe risks associated with phishing, consistent with cybersecurity literature indicating financial and privacy-relate harms.



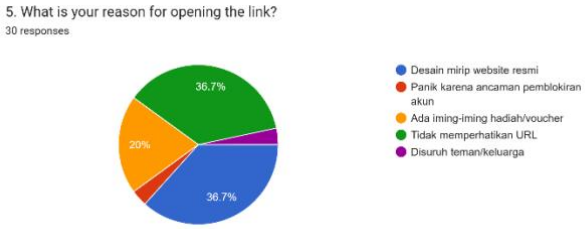
Note: 4 "Tidak Terjadi Apa-Apa" = No impact; "Tidak Yakin" = Unsure; "Kehilangan Saldo Uang" = Lost money, "Akun Sosial Media Diretas" = Social media account hacked; "Akun Marketplace Bermasalah" = Marketplace account compromised; Data Pribadi Bocor" = personal data leaked.

E. *Factors Influencing Users to Open Phishing Links*

Several key factors contributed to respondents clicking suspicious links:

- Webpage design resembling an official site,
- Failure to check the URL,
- Attractive offers or rewards,
- Fear triggered by account-blocking threats,
- Requests from friends or family.

These results show that phishing attacks heavily rely on social engineering, exploiting emotions such as fear, curiosity, excitement, or trust supporting prior studies identifying psychological manipulation as a central phishing strategy.



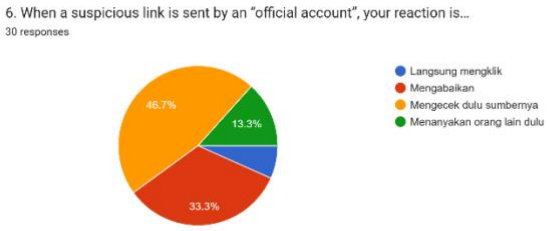
Note: 5"Desain Mirip Website Resmi" = Website design looked official; "Tidak Mempehatikan URL" = Did not check the URL; "Ada Iming-iming Hadiah/Voucher" = Attracted by prize/voucher; "Panik Karena Ancaman Pemblokiran" = Panic due to blocking threat; "Disuruh Teman/Keluarga" = Asked by friend/family.

F. *User Responses When Receiving Links from "Official Accounts"*

When asked how they react to links that appear to be sent from official accounts, most respondents stated that they would:

- verify the source first, or
- ignore suspicious messages.
- ignore suspicious links.

However, some respondents admitted to clicking the link immediately without verification, indicating uneven levels of awareness and ongoing vulnerabilities among users.



Note: 6 "Mengecek Dulu Sumbernya" =Verify the source first; "Mengabaikan" = Ignore; "Menanyakan Orang Lain Dulu" = Ask someone else first; "Langsung Mengklik" =Clik immediately.

G. *Types of Digital Fraud Experienced*

The types of fraud most frequently reported included:

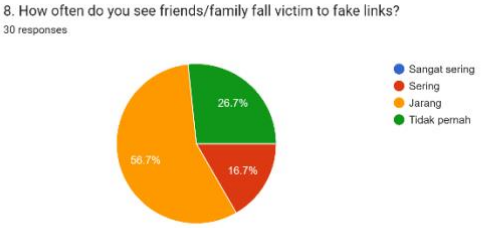
- fake prize or voucher announcements,
- fake discount or promotion offers,
- account update confirmation scams,
- "failed package delivery" notifications,
- theft of one-time passwords (OTP).

Some respondents reported never encountering digital fraud. These patterns demonstrate that phishing campaigns often follow common trends designed to attract or alarm users.

Note: 7 "Hadiah/voucher Palsu" = Fake prize/voucher; "Diskon/Promo Palsu" =Fake discount/promotion;"Konfirmasi Pembaruan Akun" = Account update scam; "OTP Akun" = OTP thef; "Tidak Pernah Mengalami" =Never experienced.

H. *Exposure to Victims Within the Respondents' Social Circles*

While most respondents answered rarely, a considerable number reported frequently seeing friends or family members fall victim to suspicious links. This indicates that phishing is not only an individual issue but also a widespread social



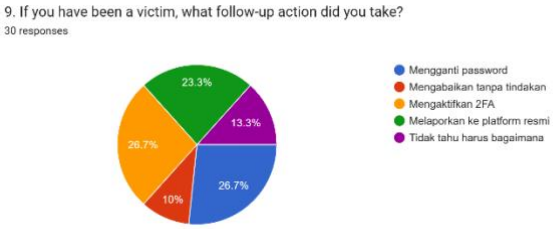
concern affecting many user communities.

Note: 8 "Jarang" = Rarely; "Tidak Pernah" = Never; "Sering" = Often.

I. *User Actions After Becoming a Victim*

Respondents took various actions after becoming victims, including:

- changing their passwords,
- enabling two-factor authentication (2FA),



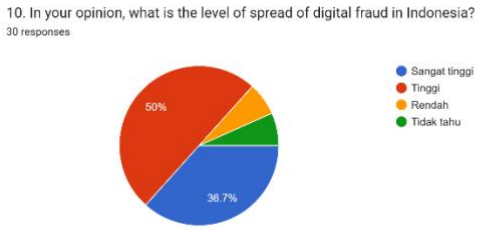
- reporting the incident to official platforms,
- or being unsure about what to do.

A number of respondents took no action, reflecting a lack of knowledge about appropriate incident response steps and highlighting the need for improved digital security education.

Note: 9 "Mengganti Password" = Change password; "Mengaktifkan 2FA"= Enable 2FA; "Melaporkan ke Platform Resmi" =Note sure what to do; "Mengabaikan Tanpa Tindakan" =Ignored / No action taken.

J. *Perceptions of Digital Fraud Prevalence in Indonesia*

Most respondents perceived the prevalence of digital fraud in Indonesia as high or very high, with only a small portion



selecting low or not sure.

This perception is consistent with national reports and academic studies demonstrating that phishing and other cybercrimes are increasing in frequency.

Note: 10 "Rendah" = Low; "Tinggi" = High; "Sangat Tinggi" = Very high; "Tidak Tahu" = Not sure

K. *Sense of Safety When Using Digital Services*

The majority of respondents reported feeling moderately safe when using digital services. However, many respondents also expressed uncertainty, while smaller groups felt very safe or unsafe.

These findings suggest that the overall sense of security among users is mixed and influenced by personal experience and exposure to information about digital fraud cases.

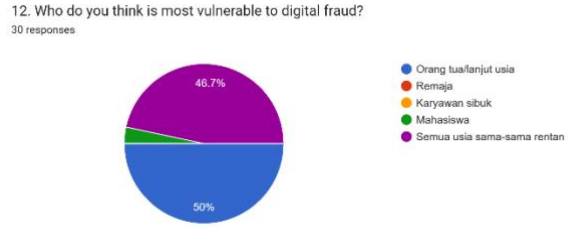
Note: 11"Sangat Aman" = Very safe; "Cukup Aman" = Moderately safe; "Tidak Aman" = Unsafe; "Tidak Yakin" = Not sure1

L. Groups Considered Most Vulnerable to Digital Fraud

Respondents most frequently identified:

- Elderly individuals as the most vulnerable demographic

A significant portion also believed that all age groups are equally vulnerable, which aligns with cybersecurity literature suggesting that phishing can successfully target users regardless of age or digital proficiency.

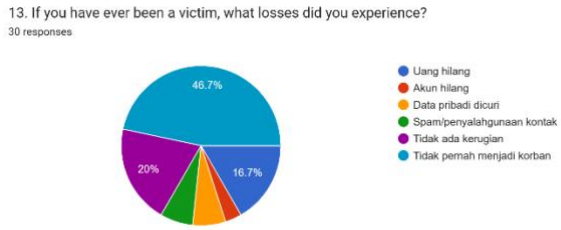


Note: 12 "Orang Tua/Lanjut Usia" = Elderly individuals; "Semua Usia Sama-sama Rentan" = All ages aqually vulnerable; "Mahasiswa" = University students.

M. Types of Losses Experienced

Respondents described several types of losses resulting from phishing, including:

- monetary loss,

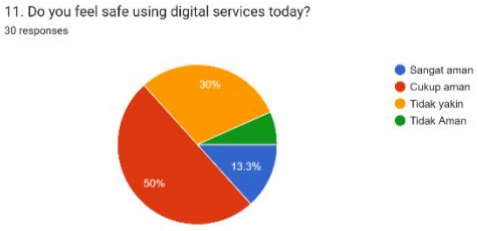


- compromised personal data,
- stolen online accounts,
- misuse of contact information,
- or no loss for those who had not been victims.

These findings reinforce the understanding that phishing can result in both financial and non-financial harm.

N. Reporting Digital Fraud Incidents

Respondents' reporting behavior fell into three categories:



Penyalahgunaan kontak = Spam/contact misuse; "Tidak Ada Kerugian =No loss; "Tidak Pernah Menjadi Korban" = Never been a victim.

- those who reported,
- those who did not report,
- those who planned to report.

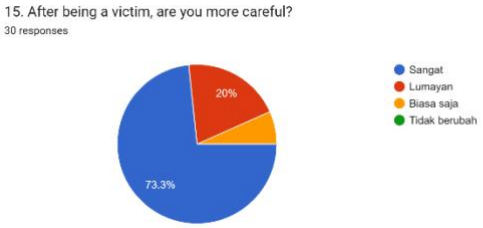
Most respondents did not report the incident, suggesting insufficient awareness of reporting channels or a lack of confidence in available reporting mechanisms.

Note: 14 "Ya" = Yes; "Tidak" = No; "Berencana Melaporkan" = Planning to report.

O. Behavioral Changes After Becoming a Victim

Most respondents reported becoming more cautious, either very cautious or somewhat cautious, after experiencing or witnessing digital fraud. Only a small number indicated no change in behavior.

These results demonstrate that exposure to digital fraud has a positive influence on user vigilance and digital security habits.



Note: 15 "Sangat" = Significant change;"Lumayan" =Moderate change; "Biasa Saja" = No notable change.

V. CONCLUSION

This study successfully answered the main objective, which was to analyze the threat of link-based phishing attacks to the security of users' digital accounts. The results of the study show that phishing attacks utilize social engineering and the similarity of website appearances to deceive victims so that they unknowingly provide sensitive information. Low levels of digital literacy, users' habits of rarely verifying URLs, and the lack of security features such as two-factor authentication have been proven to be factors that increase users' vulnerability to these threats. The survey conducted reinforced these findings, with most respondents still frequently receiving suspicious links but lacking sufficient knowledge to recognize the characteristics of phishing.

The implications of this research show that phishing threats not only result in financial loss, but also have the potential to cause personal data leaks, account takeovers, and a decline in user confidence when engaging in digital activities. This situation indicates the need for systematic improvements in digital security literacy and the

implementation of stronger protection technologies at both the user and platform provider levels. Continuous education is a crucial factor in enabling users to recognize, avoid, and respond to phishing threats more effectively.

Based on these findings, further research is recommended to expand the scope of respondents, develop more in-depth instruments for measuring digital security awareness levels, and explore technology-based approaches such as machine learning to detect phishing patterns in real time. In addition, future research could also examine the effectiveness of digital literacy programs across different age groups and regions in order to develop more targeted and impactful mitigation strategies

REFERENCES

[1] A. Basit, M. Zafar, and Z. Jalil, "A Review of Website Phishing Attack Detection Methods," 2020.

[2] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput Secur*, vol. 105, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[3] A. Ur Rehman *et al.*, "Securing Cyberspace: An Efficient Machine Learning Based Approach To Phishing Attack Detection," *Journal of Mechanics of Continua and Mathematical Sciences*, vol. 19, no. 8, pp. 94–119, Aug. 2024, doi: 10.26782/jmcms.2024.08.00008.

[4] A. Sahfitri and Rosmalinda, "Penipuan Digital Melalui Tautan Phising," *Jurnal Dialektika Hukum*, vol. 6, no. 2, 2024, [Online]. Available: https://bankjombang.co.id/serangan-phishing-di-indonesia-terus

[5] M. A. B. Dewanto, M. Fathurrahman, D. R. Firdaus, and A. Setiawan, "Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, Jun. 2024, doi: 10.47134/pjise.v1i4.2672.

[6] A. A. J. Arsyad, U. Tamrin, J. P. Lande, and N. Umar, "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar," *Jurnal Pengabdian Literasi Digital Indonesia*, vol. 3, no. 2, pp. 60–71, Oct. 2024, doi: 10.57119/abdimas.v3i2.122.

[7] M. R. Ramadhani and A. Raf'ie Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," 2020.

[8] Wahyuddin, L. Firdausiah Ersa, G. Aningsih, T. Hidayat, and A. Febri Sonni, "Analisis Jaringan Komunikasi Penipuan Daring Melalui Media Sosial Whatsapp Messenger," Jan. 2024. [Online]. Available: http://netnografiikom.org/index.php/netnografi

[9] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, "Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, Jun. 2024, doi: 10.47134/pjise.v1i4.2753.

[10] A. Dias Sulistyo, B. Dwi Wicaksono, R. Nur Saputra, and R. Ramadhani, "Strategi Penanggulangan Serangan Phishing di Media Sosial," *Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, pp. 18–2024, Jul. 2024.

[11] I. Ady Saputro, L. Sugiarto, and F. Surya Nugraha, "Analisis Kesadaran Masyarakat Terhadap Bahaya Internet Phising Menggunakan K-Means Clustering," Dec. 2024.