Phishing and Basic Digital Security for Students and the General Public

Rasya Dika Pratama[1], Wahid Satrio Aji[2], Muhammad Mizanul Faiq[3], Rachmadiaz Vebriansyah Aflah Islami[4], Raffi Aditiya Saputra[5]

dikagilang2007@gmail.com[1], wahidsatrioaji29@gmail.com[2], mizanulfaiq3@gmail.com[3], rachmadiaz07@gmail.com[4], aezakhmi3@gmail.com[5]

Telkom University

Abstract: Although cyber hygiene practices are increasingly promoted, phishing attacks remain high both globally and in Indonesia, affecting university communities as well as the general public. This study aims to map recent phishing trends, identify key factors contributing to user vulnerability, and formulate essential digital security measures relevant to students and broader society. The research employed a literature review of authoritative reports and studies, complemented by interviews with students and community members around the campus. APWG data recorded 1,270,883 attacks in Q3-2022 and 1,003,924 attacks in Q1-2025, indicating that phishing risks continue to persist. Google's research shows that its SMS code verification system can block 100% of automated bots, 96% of mass phishing attempts, and 76% of targeted attacks, highlighting the urgency of activating MFA. Training approaches such as PhishGuru have been shown to significantly reduce phishing clicks in field studies, and recent systematic reviews confirm that repeated education provides meaningful protective effects. Overall, the combination of layered technical controls and continuous digital security education demonstrates the strongest potential for reducing phishing risks among students and the general public.

Keywords : *cyber hygiene, Cybersecurity education and training, social engineering, Otentikasi multi-faktor (MFA)*

Abstrak: Meski praktik dari cyber hygiene makin disosialisasikan, Tetapi serangan phishing ini masih tetap tinggi secara global maupun di indonesia dan berdampak pada komunitas kampus. Bagaimana cara kita meminimalkan kerentanan terkenanya phishing bagi masyarakat umum dan Mahasiswa, Tujuan penelitian ini dibuat yaitu untuk memetakan tren dan banyaknya modus phishing itu bagaimana, mengidentifikasi faktor yang membuat masih banyaknya yang terkena modus phishing ini, dan merumuskan langkah keamanan digital dasar yang relevan untuk mahasiswa dan masyarakat umum. Metode penelitian ini dibuat menggunakan studi literatur terhadap laporan atau riset otoritatif dilengkapi wawancara dengan mahasiswa dan masyarakat umum di sekitar kampus. Hasil dari riset tren global masih tinggi dari data APWG mencatat 1.270.883 serangan pada Q3-2022 dan 1.003.924 serangan pada Q1-2025, menandai hal tersebut beban resiko masih berkelanjutan kedepannya. riset dari google sistem kode SMS dari google mampu memblokir 100% bot otomatis, 96% phishing massal, dan 76% serangan yang tertarget, google mengukuhkan urgensi aktivasi MFA di akun itu sangat penting. pelatihan ala PhishGuru secara nyata menurunkan klik phishing dalam studi lapangan, dan tinjauan sistematis terbaru menegaskan pelatihan berulang memberi efek protektif bermakna. Secara keseluruhan, kombinasi kontrol teknis berlapis dan edukasi berkelanjutan menunjukkan potensi terbaik untuk menurunkan risiko phishing pada populasi mahasiswa dan masyarakat umum.
Kata kunci: *Keamanan digital, Edukasi dan pelatihan keamanan siber, Rekayasa sosial, Otentikasi multi-faktor (MFA)*

Introduction

In today's digital age, phishing attacks have become a very common and dangerous cybersecurity threat. Anti-phishing Working Group (APWG) reports show an increase in the number of phishing incidents over the past few years (APWG, 2022; APWG, 2025). In the third quarter of 2022, the APWG recorded 1,270,883 phishing attacks worldwide—the highest number at that time, a more than fivefold increase compared to early 2020 (APWG, 2022). This trend continued, and in the first quarter of 2025, the number of global phishing attacks reached 1,003,924 in three months, the highest number since late 2023 (APWG, 2025). In Indonesia, phishing is also the most prevalent type of cybercrime. Studies show that phishing was the most common cybercrime in Indonesia between 2017 and 2022 (Nurhayati et al., 2022). The National Cyber and Crypto Agency (BSSN) also confirmed this. According to the Deputy of BSSN, phishing is one of the most common forms of cyberattacks because the perpetrators' methods are relatively simple (BSSN, 2025). With the increasing number of phishing cases, internet users from all walks of life are potentially victims.

Phishing typically exploits the ignorance and inattention of internet users. Phishing attacks employ social media tactics to create a false sense of trust and urgency. Kaspersky reports that cybercriminals are increasingly adept at pretending to be known or trusted individuals, such as colleagues, banks, or government agencies, so that victims do not pay attention and follow the phishing perpetrators' instructions (Kaspersky Resource Center, n.d.; Kaspersky, 2024). Simply by clicking on a fake link, users can be trapped and unknowingly provide confidential information. Consequently, it's not surprising that 83% of organizations have experienced at least one successful phishing attack in the past year (AAG IT, 2025). In the education sector, students and academics are also targets of phishing, such as the case of a fake university login page used to steal student usernames and passwords (Antaranews Jatim, n.d.).

The threat of phishing is increasingly dangerous because many people still lack understanding of digital security. Many people take phishing lightly and feel it's easy to recognize how it works. However, survey results show that not everyone is confident in recognizing phishing and malware attacks. For example, one study found that only around 40% of respondents felt confident in recognizing these attacks, while the rest were unsure (BSSN, 2025). This low level of confidence and understanding indicates the need for increased education about cybersecurity. Phishing is no longer limited to easily detected fake emails; it takes various forms and continues to evolve. Therefore, raising awareness and implementing basic security practices is crucial, especially in higher education environments where many people use technology but may not necessarily have sufficient knowledge about cyber threats.

This research aims to explain the phenomenon of phishing and basic digital security measures that are important for students and the general public to know.

The first section will discuss the definition of phishing, its modus operandi, and examples of potential impacts. The second section will discuss the role of humans and their level of awareness in dealing with phishing attacks. The third section will provide some basic digital security recommendations to prevent phishing and other cyber threats. Finally, the importance of education and training in fostering digital security awareness and culture is emphasized. With sufficient understanding, readers will hopefully be more cautious and protected from phishing threats in their daily digital lives.

Research Methods

The research method used was a descriptive mixed-methods approach with a predominantly qualitative approach to address the issues of trends, vulnerability factors, and cyber hygiene practices related to phishing. Data was obtained through a literature review of authoritative journals and reports from APWG, Google, PhishGuru, and academic research from 2019–2025. Data were also collected through semi-structured interviews with students and the community around campus using a purposive sampling technique (Palinkas et al., 2015). Data collection was conducted both in person and online. Interviews were transcribed and anonymized, while literature was selected based on relevance and credibility. Data analysis was conducted using thematic analysis to interpret key patterns such as urgency, impersonation of trusted entities, and obstacles to MFA implementation. Descriptive statistics from secondary data were used to support the context of trend figures. Validity was maintained through source triangulation between literature and interviews. This research was ethically sound, with informed consent, respondent anonymization, and secure data storage.

Definition and Threats of Phishing

Phishing is a cybercrime method in which the perpetrator attempts to lure the victim into taking an action that gives them access to their information or systems. Typically, the perpetrator impersonates a trusted person or company or organization, tricking the victim into voluntarily providing sensitive information. Phishing is often carried out through fraudulent emails that appear to be from a trusted source, such as a company, bank, or official institution. The email often directs a link to a fake website that looks similar to the legitimate one. When the victim clicks on the link and enters credentials, such as a username and password, the perpetrator can steal their confidential information. After entering their data, they are often redirected to the legitimate website, preventing them from immediately realizing they have been deceived.

Phishing is a social engineering-based crime, meaning it focuses on manipulating people, not breaching technical systems. Trust and a sense of urgency are the primary weapons of phishing. The perpetrator attempts to manipulate the victim's emotions—for example, with messages like "Your account is blocked,

verify immediately!" or "Congratulations, you've won the lottery, click this link now!" In a state of panic or excitement and emotional turmoil, victims tend to be less thorough and follow instructions without verification. Other tactics include time-sensitive or pressure tactics, and false narratives (posing as a boss and asking for a money transfer). All of these tactics are designed to make victims act impulsively and not think critically.

Phishing isn't limited to email. Perpetrators also utilize various other communication channels: for example, fake websites that appear in search results, SMS (known as smishing), automated or direct phone calls (vishing), and messages on messaging apps and social media. Recent reports even show a trend of using QR codes in phishing emails—users are lured into scanning QR codes that actually lead to phishing sites or malware. Phishing is also commonly found on social media, for example, fake links spread through Facebook, Instagram, or WhatsApp messages. According to statistics, 90% of message-based phishing occurs on WhatsApp, with the remainder via other social media platforms like Telegram.

Phishing is particularly dangerous due to its versatility and difficulty in identifying. Even alert users can still fall for phishing because the email or website looks convincing.

Lack of Awareness and Training

Many users who are uneducated about phishing schemes are more easily fooled. Cybercriminals actively exploit this knowledge gap. Alkhalil et al. (2021) noted that attackers typically target users with low awareness or who are untrained in digital security. Without understanding the characteristics of phishing emails or messages, users tend to easily believe emails that appear important or urgent. Conversely, users who have received anti-phishing training tend to be more vigilant. Several studies have shown that after receiving brief training, the percentage of employees who click on phishing emails decreases. For example, the PhishingGuru training program at CMU successfully reduced the phishing click index by more than half within a week of training. Globally, reports have even found that phishing click rates can drop by up to 85% (from 29.8% to 4.1%) after 12 months of regular user phishing simulations and education. This demonstrates the crucial role education plays in increasing user awareness of the threat of phishing.

Interestingly, phishing victims don't always come from less tech-savvy backgrounds. Sometimes, users who perceive themselves as tech-savvy are actually more careless. Overconfidence, believing "I can definitely recognize a fake email," can lead someone to be less thorough in checking email details.

Research into the influence of age and gender on phishing vulnerability has yielded mixed results. Several studies indicate that older users tend to be more susceptible to phishing than younger generations. This is related to decreased cognitive abilities and a lack of digital experience (digital natives vs. digital immigrants). Oliveira et al. (2017) reported that older users, especially older

women, are most vulnerable because they are less likely to recognize fraudulent behavior and are more likely to believe the promise of financial gain in phishing emails.

However, other data suggests that young people also frequently fall victim. Statistics in the UK show that 18-40 year olds are less likely to fall for phishing (23% of respondents) than 41-55 year olds (19%). This may be because young people are more active in the digital world and are more frequently exposed to various forms of phishing. Everyone, from children and teenagers to adults and seniors, now uses digital devices, and their contact information, such as email addresses, mobile phone numbers, and social media accounts, is easily accessible to the public.

Several personal characteristics also influence susceptibility to phishing. Research conducted by Workman (2008) states that greed is a common weakness. Furthermore, being hasty or impulsive is also risky, as impatient users tend to click on links without considering the risks. Conversely, skepticism and thoroughness are natural safeguards; individuals who are always cautious of suspicious messages are safer.

Phishing perpetrators also exploit emotional states. When someone is panicked, tired, or rushed, their critical thinking skills are impaired. Therefore, attacks often occur during vulnerable times, such as peak work hours or holidays, when users are less vigilant. Kaspersky notes that fraudsters often exploit the holiday season by posing as fake travel tickets or tour packages to trap unsuspecting victims.

From the points above, it can be concluded that humans are a crucial factor in phishing incidents. Even sophisticated security technology will be ineffective if users make mistakes (human error), such as clicking on malicious links or carelessly providing personal information. Therefore, building human defense by increasing awareness in digital literacy is very important.

Basic Digital Security Practices (Cyber Hygiene)

No system is 100% secure, but most cyberattacks (including phishing) can be prevented or their impact minimized by consistently implementing basic security practices. Therefore, every user, whether students, lecturers, or the general public, should make "cyber hygiene" a daily habit. The US Cybersecurity Agency (CISA) emphasizes that simple steps such as using strong passwords, regularly updating software, thinking twice before clicking links, and enabling multifactor authentication can drastically improve our online security. Some recommended basic digital security practices are as follows:

Create/Use Strong and Unique Passwords

Also, ensure each of your online accounts has a strong password (a combination of uppercase and lowercase letters, numbers, or symbols) that is different for each service. And when creating passwords, avoid using easily guessed

passwords (such as your birth date or "password123"). Create unique passwords; if one of your accounts is compromised, your others won't be compromised. Use a password manager if necessary to help you store more complex passwords. This practice is also important because many attacks exploit leaked credentials; criminals try the same passwords across multiple sites (credential stuffing). Strong and unique passwords can prevent this domino effect.

Enable Multi-Factor Authentication (MFA)

Two-factor authentication (2FA), or MFA, adds an extra layer of verification (e.g., SMS OTP code, authenticator app, fingerprint, etc.) in addition to your password. This is one of the best defenses against phishing. Even if an attacker does manage to steal your password, they'll have a hard time logging in without the second factor. Google research has shown that with SMS-to-phone 2FA, 100% of automated bots, 96% of mass phishing, and 70% of targeted attacks can be thwarted. Using a stronger 2FA method (such as an authenticator app or security key) can prevent 99% of mass phishing attacks and 90% of targeted attacks. Essentially, enable MFA on every account that supports it (email, social media, internet banking, etc.). This simple step significantly improves account security.

Be Aware of Suspicious Emails or Messages

Cultivate skepticism of unexpected digital communications. If you receive an email asking you to click a link or download an attachment, verify its authenticity. Verify the sender - do the sender's email address and domain match? Phishers often use similar addresses (e.g., support@paypai.com instead of paypal.com). Check the spelling of the URL before clicking; scammers often use typosquatting techniques (e.g., the letter "rn" resembles a "principle" or "principle"). "m", the number "1" as "l"). Don't easily believe emails that pressure you to act quickly (e.g., "your account will be closed today if you don't click the link"). When in doubt, don't click links directly from emails. Instead, manually open the official website via a browser or confirm with an authorized contact. This kind of vigilance is the strongest defense against falling victim to phishing schemes.

The Importance of Digital Security Education and Literacy

In addition to the technical protections mentioned above, the best investment in combating phishing is investment in knowledge. Digital security education needs to be continuously improved among students and the general public to distinguish between phishing and non-phishing and to foster a strong culture of security awareness. Training and outreach regarding phishing methods can foster vigilance and help recognize signs of digital fraud, such as domain misspellings, urgent language, or requests for personal data (Kaspersky, 2024). When users understand attack patterns, the chance of being phished decreases dramatically. Digital literacy programs also help the public stay updated on threats as new techniques develop, such as the trend of QR code phishing (Geisler et al., 2024). On campus, cybersecurity seminars and training can be held regularly so students

can stay up-to-date on new digital fraud schemes, such as scholarship scams and fake internships that frequently target them (Nur'aini & Simanjuntak, 2025).

Good education doesn't stop at just material, but also includes hands-on practice in the form of phishing simulations. The PhishGuru program developed at Carnegie Mellon University has been shown to effectively reduce phishing click rates after training based on mock emails (Kumaraguru et al., 2009). Other research by Cyberpilot shows that the combination of awareness training and phishing simulations can reduce user errors by up to 60% in just one session.

Conclusion

Based on the results of the literature review and interviews, it can be concluded that phishing remains the most dominant cyber threat both globally and nationally. The Anti-Phishing Working Group (APWG) report shows a significant increase in attacks, reaching over one million cases per quarter (APWG, 2022; APWG, 2025). In Indonesia, phishing also ranks among the top cybercrime cases (BSSN, 2025). These attacks are successful not solely due to technical weaknesses, but also due to human factors such as a lack of digital literacy, overtrust, and poor implementation of basic security measures (Alkhalil et al., 2021; Workman, 2008).

This study found that implementing simple cyber hygiene measures such as using strong passwords, regular software updates, and activating multi-factor authentication (MFA) can significantly reduce the risk of phishing attacks. Google research (2019) supports these findings by demonstrating the effectiveness of MFA in preventing up to 99% of mass phishing attacks. In addition to technical controls, an educational approach is also a key factor in increasing user resilience. Training programs such as PhishGuru (Kumaraguru et al., 2009) and phishing simulations have been shown to reduce user errors by up to 60% (Prümmer et al., 2024). Continuous education at the campus and community levels, such as digital literacy seminars or public campaigns from the National Cyber and Information Technology Agency (BSSN) and the Ministry of Communication and Information Technology (Kominfo), is effective in building a strong cybersecurity culture (security awareness).

Therefore, the combination of layered technical protection and ongoing digital security education is the most effective strategy for reducing the risk of phishing among students and the general public. Governments and educational institutions are advised to strengthen mandatory MFA policies, provide regular simulation-based training, and integrate cybersecurity literacy into non-formal curricula. Future research is recommended to evaluate the long-term effectiveness of digital literacy programs on changing user security behaviors. Building a culture of digital security awareness not only protects individuals but also strengthens the resilience of the national cyber ecosystem.

References

AAG IT. (2025, June). *The latest phishing statistics (updated June 2025)*.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

Anti-Phishing Working Group. (2022, December). *Phishing Activity Trends Report, 3rd Quarter 2022*.

Anti-Phishing Working Group. (2025, July 2). *Phishing Activity Trends Report, 1st Quarter 2025*. CISA. (n.d.). *Securing your home network*. Cybersecurity & Infrastructure Security Agency.

Geisler, S., Evers, D., Becker, P., & Smith, M. (2024). *Hooked: A real-world study on QR code phishing*. arXiv.

Google (Thomas, K., & Moscicki, A.). (2019, May 17). *New research: How effective is basic account hygiene at preventing hijacking*. Google Security Blog.

Kaspersky. (2024, March 7). *Kaspersky reports phishing attacks grow by 40 percent in 2023*. Press release.

Kaspersky. (2025, February 19). *Kaspersky reports nearly 900 million phishing attempts in 2024 as cyber threats increase*. Press release.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, A., Acquisti, A., Cranor, L. F., & Hong, J. (2009). Getting users to pay attention to anti-phishing education: Evaluation of embedded training emails. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1–10). ACM.

Nur'aini, R. J., & Simanjuntak, M. (2025). Phishing awareness and security concerns: Analyzing the role of anti-phishing knowledge and Internet experience in online banking users. *Jurnal Ilmu Keluarga & Konsumen, 18*(2), 121–134. (IPB Press)

Workman, M. (2008). Gaining access with social engineering: An empirical study of the threat of information security breaches. In *Proceedings of the 41st Hawaii International Conference on System Sciences (HICSS)*. IEEE.