Risk Analysis of Computer Network Security Focusing on Phishing Attacks in Fintech Platform

Zahra Kharisma Sangha[1*], Heni Sulistiani[2]

[1,2,]*Information Technology, Universitas Teknokrat Indonesia, Bandar Lampung, Indonesia*

Article Information

Received: 21-11-2024
Revised: 28-11-2024
Published: 05-12-2024

Keywords
Fintech Platform; Phising; Network Security

****Correspondence Email:***
zahra_kharisma_sangha@teknokrat.ac.id

Abstract

The advancement of Science and Technology, particularly in Information Technology such as the internet, has significantly facilitated individuals in achieving their life goals quickly, either through legal or illegal means. One prominent threat is phishing, which employs social engineering techniques to deceive users by impersonating authoritative entities. Phishing targets various industries, with the fintech platform sector being one of the primary targets. The main factors contributing to phishing in fintech platform services include users' lack of knowledge, psychological factors, and insufficient privacy protection on social networks. Therefore, computer network security is a critical measure to prevent phishing attacks on fintech platform services. This research employs a qualitative method with a descriptive approach.

1. Introduction

Computer network technology is currently advancing in nearly every part of the world. Along with the rapid development of the internet as an information provider, a second world has emerged, often referred to as cyberspace. Thanks to this network, all kinds of information around the globe can be accessed 24/7. However, the advancement of information technology today is seen as a double-edged sword, as it not only contributes to progress, welfare, and human civilization but also brings potential challenges and risks.

Information technology has become a critical enabler for individuals to achieve their objectives rapidly, whether through legitimate or illegitimate means, often sidelining ethical considerations in pursuit of material or intangible benefits. The global advancement of information and communication technology (ICT) has provided immense value to various sectors, including industry, banking, and small and medium enterprises (SMEs). These sectors reap benefits such as improved efficiency, streamlined operations, and enhanced user experiences. However, this technological progress has also introduced new challenges, particularly with the emergence of cybercrimes that exploit system vulnerabilities and the limited awareness of users about information security.

As ICT continues to evolve, the complexity of information security threats increases. Cybercrimes such as hacking, phishing, and malware attacks have become more prevalent, posing significant risks to data integrity and user privacy. Among the most targeted sectors is online banking, fintech platform, or other payment sector, where sensitive personal data and financial transactions are particularly vulnerable. Despite these growing threats, user awareness and understanding of the importance of data protection remain insufficient. This gap

presents a major challenge in mitigating risks and safeguarding information. A comprehensive approach is therefore essential, involving user education and the implementation of advanced security measures like encryption, two-factor authentication, and continuous monitoring to detect and address potential threats proactively.

Phishing attacks remain a significant threat, particularly to the financial services sector, which is a primary target for cybercriminals aiming to exploit system vulnerabilities. According to a recent cybersecurity report, phishing continues to be the preferred method for gaining unauthorized access to sensitive information, particularly in industries like banking and payment services. The financial sector, especially, has witnessed a dramatic increase in phishing attempts, with attackers often impersonating well-known brands like Microsoft and American Express. These fraudulent activities can lead to identity theft, account abuse, and unauthorized financial transactions.

Additionally, the rise of digital services and APIs has expanded the attack surface, making financial institutions more vulnerable to cyber threats. Web application and API attacks targeting the sector have surged, with phishing websites and brand impersonation schemes now accounting for a large proportion of cyberattacks. The prevalence of these tactics highlights the need for financial institutions to enhance their defenses through better user awareness and advanced cybersecurity measures.

In recent years, phishing attacks targeting many fintech platform and other sectors have been on the rise in Indonesia. For example, in early 2023, Indonesia experienced a significant increase in phishing cases, with over 26,000 incidents reported in the first quarter alone. This was a dramatic rise compared to the 6,000 cases reported at the end of 2022. The financial and social media sectors were particularly targeted, with 31% of phishing attacks aimed at financial institutions and 45% directed at social media platforms.

One notable case involved Kredivo, is an Indonesian-based fintech platform that provides buy now, pay later (BNPL) services, as well as offering credit financing options for online shopping. It operates in a similar space in terms of providing digital payment solutions, where scammers exploited a data breach to carry out phishing attacks. These incidents have become a major concern for users and service providers alike, highlighting the need for increased awareness and vigilance regarding the security of personal data and online transactions.

The rapid advancement of science and technology, particularly information technology (IT) such as the internet, significantly aids individuals in achieving their goals quickly, whether through legal or illegal means. Unfortunately, some people exploit this progress by resorting to unethical methods to gain material or intangible benefits. These individuals seek shortcuts to acquire wealth swiftly, using the internet as a tool to learn practices that would otherwise be inappropriate or harmful to others. This creates an opportunity for irresponsible actions, often leading to negative consequences for society as a whole. The internet serves both as a resource for legitimate purposes and a platform for those seeking to engage in activities that can harm others.

1.1 Literature Review

The rapid advancement of information and communication technology (ICT) has brought profound changes in how individuals and organizations operate across the globe. As ICT continues to develop, particularly with the expansion of the internet, it has created a digital landscape referred to as cyberspace, where information is readily available at any time. This connectivity has enabled progress in various sectors, including banking, industry, and small-medium enterprises (SMEs), contributing to improved operational efficiency and user experience. However, the very same technological progress has also presented new challenges, notably the rise of cybercrimes, which exploit vulnerabilities within digital systems.

Phishing, a cybercrime technique where attackers impersonate legitimate organizations to trick individuals into disclosing personal information, has become a prominent issue. This technique, along with others such as malware and social engineering, has escalated due to the increasing digitization of financial transactions. A study by Griffiths (2023) highlights that phishing remains one of the primary methods cybercriminals use to

infiltrate online banking systems, resulting in identity theft, financial fraud, and significant reputational damage for both individuals and institutions. In recent years, phishing attempts have risen dramatically, especially in the financial sector, where sensitive information like account details and credit card numbers are highly targeted

The impact of phishing is not just financial but also reputational, as these attacks undermine trust in digital banking systems. A report by Kompas Cyber Media (2015) emphasized the surge in phishing incidents in Indonesia, especially affecting online banking services. The rising prevalence of phishing in sectors such as finance and social media in Indonesia is alarming. According to recent statistics, there was a noticeable spike in phishing incidents in the first quarter of 2023, with over 26,000 cases reported, a significant increase compared to previous years. The financial sector, particularly online banking, remains a prime target for cybercriminals seeking to exploit system vulnerabilities.

These attacks are often facilitated by phishing websites and brand impersonation tactics, which have been on the rise as more businesses migrate their services to the digital domain. As highlighted by the rise of API-based attacks, financial institutions in Indonesia have had to bolster their cybersecurity measures to combat these threats. Moreover, the Kredivo case, where a data breach allowed scammers to carry out phishing attacks, underscores the urgent need for both individuals and organizations to enhance their awareness and defense against such security threats (Griffiths, 2023; PT Kompas Cyber Media, 2015).

The consequences of phishing attacks are vast, from direct financial loss to the erosion of consumer confidence in online systems. In Indonesia, increased media coverage and official reports point to a clear need for improved public awareness and stricter security measures to prevent these attacks from escalating further. The internet, while providing vast opportunities, also serves as a tool for cybercriminals seeking to exploit users for personal gain, which stresses the importance of responsible internet use and the need for robust cybersecurity frameworks.

2. Research Methods

In the research methodology refers to the approach used to address the research problem throughout the course of the study. In this article, the researcher employs a qualitative research methodology. Qualitative research emphasizes understanding the qualities or key aspects of an object or phenomenon. The most critical element in studying social events or phenomena is the meaning behind these occurrences, which can serve as valuable lessons for theoretical development (Creswell, 2014). Qualitative research aims to explore and explain social phenomena in depth, thereby providing a clearer understanding of the factors at play.

The research conducted here is descriptive in nature, focusing on detailing and analyzing the existing conditions and the factors involved. In this case, the study uses a library research method, involving the collection and analysis of secondary data from sources such as books, articles, papers, and previous research findings. This approach is particularly useful for deepening understanding of a topic, such as the issue of phishing threats in fintech platform.

For data analysis, the researcher follows the steps outlined by Miles and Huberman (1984), which involve three key stages: data reduction, data display, and inference or validation. Data reduction involves selecting relevant information and discarding unnecessary data. Data display refers to the systematic organization and presentation of data, while inference or validation is the process of drawing conclusions and verifying the findings. These steps are essential in building a deeper and more accurate understanding of phishing threats in online banking. Through this approach, the article aims to provide a comprehensive insight into the challenges faced by computer network security, particularly regarding phishing attacks.

3. Result and Discussion

Phishing was first introduced in 1995. According to James (2005), the initial method used by phishers involved employing algorithms to generate random credit card numbers. These randomly generated numbers were then used to create AOL accounts, which were subsequently exploited to send spam to other users, among other purposes. To simplify the process, special programs like AOHell were used. This practice was halted by AOL in 1995 when the company implemented security measures to prevent the successful use of random credit card numbers.

Phishing, also known as "Brand Spoofing" or "Carding," is a form of deception where attackers claim that a user's data is legitimate and secure. Felten et al. (1997) define spoofing as "a technique used to gain unauthorized access to computers or information, where the attacker communicates with the user pretending to be a trusted host." Phishing in online banking is a threat that uses social engineering methods to deceive users (customers). Attackers lure users through emails, text messages, or phone calls, pretending to be bank officials, convincing customers to provide sensitive data related to their bank accounts. The primary factors contributing to phishing attacks in online banking or other payment sector like fintech platform include the lack of user awareness, psychology, and privacy concerns associated with the use of social networking services.

3.1 How Phishing Works

Phishing operates as a deceptive method designed to trick individuals into disclosing sensitive personal information. Phishers exploit users' lack of vigilance, often creating fake emails or websites that resemble legitimate entities. The primary goal is to deceive users into providing information like login credentials, credit card numbers, or other private details. The process begins when phishers send fraudulent emails, pop-ups, or banner ads, directing users to counterfeit websites that look like trusted institutions. Once on these sites, users are encouraged to input their sensitive data.

Several techniques are employed in phishing to manipulate victims:

1. **Link Manipulation**: Phishers use deceptive links to make fraudulent websites appear legitimate. They may create links that resemble official addresses, but slight alterations in the URL (e.g., “goggle.com” instead of “google.com”) are designed to mislead users.
2. **Filter Evasion**: To bypass phishing filters, attackers may use images instead of text in emails. This makes it harder for security systems to detect phishing attempts.
3. **Fake Pop-ups**: Phishers may also employ pop-ups that mimic real security alerts, urging users to disclose sensitive data under the guise of needing to verify their accounts.

These deceptive tactics exploit the vulnerabilities of users' awareness and complacency, making them more susceptible to attacks.

3.2 Phishing Techniques

Phishers employ a variety of methods to execute attacks and deceive their victims:

1. **Email Spoofing**: In this technique, attackers send out massive volumes of emails that appear to come from trusted institutions. These emails often contain links asking recipients to input sensitive information like passwords or credit card details.
2. **Man-in-the-Middle (MITM) Attacks**: A sophisticated phishing technique where hackers intercept communications between the victim and legitimate websites. This allows them to steal sensitive data by posing as an intermediary between the victim and the actual website.

3. **Instant Messaging (IM) Phishing**: This method involves attackers sending messages with links that direct users to fraudulent websites. These sites closely resemble the legitimate ones, tricking users into revealing their private information.

4. **Trojan Horse Malware**: In this approach, hackers inject malicious software into users' devices to collect login credentials and other sensitive data. Once the information is gathered, it is sent back to the phishers.

5. **Link Manipulation**: Phishers send links that lead to fraudulent websites. When users click these links, they are redirected to a page designed to capture their personal data.

In the context of fintech platform, phishing attacks are often carried out using social engineering tactics. Cybercriminals pose as bank representatives, urging customers to provide sensitive information through email, SMS, or phone calls. The methods used for phishing in the banking sector include:

1. **Social Engineering**: Phishers exploit users' emotions and trust by sending messages that appear urgent or important, such as requests for donations or fake security alerts.

2. **Link Manipulation**: A common phishing technique where attackers send emails that contain one or more deceptive links leading to fraudulent websites. These links appear legitimate at first glance, but they redirect the user to malicious pages.

3. **Filter Evasion**: Phishers bypass security filters by embedding images into emails, preventing automatic detection of phishing attempts.

4. **Fake Websites**: Attackers create counterfeit websites that mimic the appearance of real banking sites. These websites are designed to deceive users into entering sensitive information, such as usernames and passwords.

5. **Phone Phishing (Vishing)**: Attackers impersonate bank officials over the phone to convince users to disclose account details. These phishing attempts are often masked by seemingly legitimate messages or requests from the bank.

As phishing continues to grow as a significant threat, financial institutions in Indonesia and globally have implemented measures such as token-based systems for e-banking and user education campaigns to prevent these attacks. However, the ultimate responsibility remains with users to be vigilant and cautious when engaging with fintech platform services.

3.3 Phishing Case at Kredivo

In a recent phishing incident involving Kredivo, a few users fell victim to a scam where attackers posed as customer service representatives offering fake promotions or gifts. These phishers contacted Kredivo users via phone, claiming they had won a giveaway or points exchange offer. The users were then tricked into clicking a link that led to a fraudulent website resembling Kredivo's official page.

Once on the phishing site, victims were asked to input their PIN, which enabled the attackers to access their accounts. Additionally, the scammers used an OTP (One-Time Password) to confirm fraudulent transactions. The attackers made purchases on e-commerce platform Bukalapak using the victims' Kredivo accounts, leading to inflated bills.

Kredivo’s VP of Marketing and Communication, Indina Andamari, clarified that phishing incidents affected less than 0.001% of Kredivo's users. The company emphasized the importance of user education on data privacy and reinforced its stance on never requesting sensitive data like PINs or OTPs.

3.4 Phishing Scenario

The phishing scenario at Kredivo typically begins with a call or message from an attacker posing as a representative offering special deals or rewards. The victim is persuaded to click on a link to claim the reward, which redirects them to a counterfeit website. The fake site mimics Kredivo's legitimate platform, where users are prompted to enter their personal data, including their PIN. Once the attackers have this information, they can make unauthorized transactions, often using the compromised accounts for online shopping.

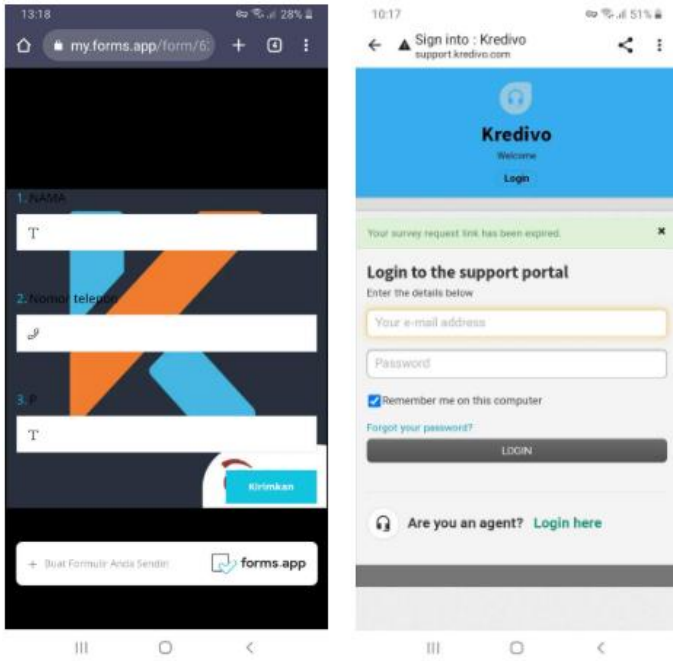

Fig. 1 Example of a phishing website layout sent by the scammer. (source : mediakonsumen.com)

3.5 Impact of Phishing on Kredivo Users

The consequences of the Kredivo phishing incident were significant, although limited to a small group of users. Victims faced financial loss due to fraudulent transactions made on their accounts. While the attackers did not directly steal funds, the compromised information undermined the trust of the affected users and potentially damaged Kredivo's reputation. Kredivo has taken steps to address the issue, including reporting the incident to the authorities and assisting the victims in recovering from the fraud. They also highlighted the need for the entire financial services industry to work together to raise awareness about phishing and improve data protection practices.

4. Conclusions

Phishing remains a significant threat to users of fintech platforms, as demonstrated by the recent case at Kredivo. The attackers employed social engineering tactics to deceive users by posing as customer service representatives offering fake promotions. This method of phishing led to unauthorized access to sensitive data, including PINs and OTPs, which were then used to make fraudulent transactions. Despite the impact being limited to a small percentage of Kredivo's users, the incident highlighted critical vulnerabilities in user awareness and the need for heightened security measures. Kredivo responded by reporting the attack to authorities and reinforcing the importance of user education, emphasizing that sensitive data, such as PINs and OTPs, should never be shared. This case underscores the ongoing challenge faced by fintech platforms in protecting their users from phishing and other cyber threats. Furthermore, it calls for greater collaboration within the financial industry to raise awareness and improve security measures to safeguard users from such attacks in the future.

5. References

Sutabri, T. (2014). Pengantar Teknologi Informasi (1st ed.). Yogyakarta: Andi Offset.

Sutabri, T. (2012). Analisis Sistem Informasi (1st ed.). Yogyakarta: Andi Offset.

Griffiths, R. (2023). Cybercrime in the financial sector: An analysis of phishing attacks. Journal of Cyber Security, 15(2), 233–245. https://doi.org/10.1016/j.jocs.2023.02.002

Kompas Cyber Media. (2015). Penipuan online melalui phishing meningkat di Indonesia. Retrieved from https://www.kompas.com

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.

Miles, M. B., & Huberman, A. M. (1984). Qualitative Data Analysis: A Sourcebook of New Methods. Sage Publications.

Tempo.co. (2022). Puluhan pengguna Kredivo jadi korban phishing, ini deretan modusnya. Retrieved from https://www.tempo.co/ekonomi/puluhan-pengguna-kredivo-jadi-korban-phishing-ini-deretan-modusnya--441352

Media Konsumen. (2022). Penipuan mengatasnamakan Kredivo. Retrieved from https://mediakonsumen.com/2022/08/07/surat-pembaca/penipuan-mengatasnamakan-kredivo-2