Ann PUBLISHER
Journal of Engineering Sciences (Improsci)
e-ISSN: 3031-7088
p-ISSN: 3032-3452

Phishing
Cyber Security Threats

Muhammad Nana Trisolvena [1*], Nana Handre Saputra [2]
[1*]Indsutryal Engineering, University of Muhammadiyah Cirebon, Indonesia. Email nana.trisolvena@umc.ac.id
[2]Informatics Engineering, University of Muhammadiyah Cirebon, Indonesia. Email nanaggmu@gmail.com
***Corresponding Author. Email nana.trisolvena@umc.ac.id**

Abstract. Phishing is a growing threat in the realm of cybersecurity, where cybercriminals use various phishing techniques to steal sensitive information from individuals and organizations. In practice, phishing aims to obtain personal, account, and financial data by impersonating trusted parties through fake emails, websites, text messages, or social media. The term "phishing" comes from the word "fishing" which describes an attempt to lure prey with fake bait. The most common types of phishing include web phishing, email phishing, smishing phishing, scam phishing, blind phishing, whaling phishing, and angler phishing, each with different approaches and targets. Phishing causes losses to individual victims and significantly impacts the information and communication technology profession, including loss of data, reputation, security, time, cost, quality, and trust. An in-depth understanding of the types of phishing, their impacts, and their prevention and countermeasures is essential to protect yourself and your organization from phishing attacks. Therefore, awareness and education about phishing are key in building resilience to this cyber threat. As such, further research and proactive actions are needed to tackle phishing effectively in the ever-evolving digital age.

Keywords: Phishing, Cybersecurity, Sensitive Data, Fake Websites

INTRODUCTION

In the increasingly evolving digital era, threats to cyber security are also increasingly complex and diverse. One of the threats that has become a significant concern is phishing attacks. Phishing is a fraudulent practice carried out online, where cybercriminals use various phishing strategies to steal sensitive information from individuals, organizations, or even government agencies.

Phishing is the act of impersonating a trusted entity, such as a financial institution, technology company, or authority, to obtain personal, account, or financial data from the victim. In practice, the techniques used in phishing are highly sophisticated and often challenging to recognize by less vigilant users.

Understanding the phenomenon of phishing and its prevention efforts cannot be

DOI 10.62885/improsci.v2i1.440

ignored. Phishing attacks not only result in financial losses for victims, but they can also damage reputations, lose trust, and even compromise the security of individuals and organizations. Therefore, research on phishing is very important to identify attack patterns, analyze their impact, and develop effective prevention strategies.

In this context, this journal aims to provide an in-depth understanding of the phenomenon of phishing, including the types of attacks, the methods used, their impact, and the preventive measures that individuals and organizations can take. Thus, it is hoped that this journal can make a meaningful contribution to efforts to build resilience to phishing threats in the ever-evolving digital era.

METHOD

The methods in manuscript this literature review are :

Literature Study: The first step in this study is to conduct a literature study to understand phishing in depth. This involves searching and analyzing scientific articles, books, research reports, and other trusted sources that have studied the topic before.

Case Study Analysis: The research will involve case study analysis of phishing attacks that have occurred before. This will help in understanding how it works

the practice of phishing in authentic contexts and the factors that influence its success.

Surveys and Interviews: Online surveys and interviews with relevant respondents will be conducted to collect primary data. The survey will include questions about respondents' understanding of phishing, their experiences dealing with phishing attacks, and the cybersecurity practices they have implemented.

Data Analysis: Data collected from literature studies, case studies, surveys, and interviews will be analyzed qualitatively and quantitatively, depending on the data type obtained. This analysis will help explore important patterns, trends, and findings related to phishing.

Recommendations and Conclusions: Based on the study's findings, recommendations will be compiled for individuals, companies, and other related parties to reduce the risk of falling victim to phishing attacks. The study's conclusion will illustrate the core of the findings obtained and their practical implications in the context of cybersecurity.

DISCUSSION

Definition of Phishing

Phishing is an attempt to obtain someone's data information using phishing techniques. The data targeted by phishing are personal data (name, age, address), account data (username and password), and financial data (credit card information, bank account).

DOI 10.62885/improsci.v2i1.440

The official term for phishing is "phishing," which comes from the word "fishing." Phishing activities do aim to lure people to voluntarily provide personal information without realizing it. Phishing perpetrators usually appear as authorized parties or institutions, using fake websites or emails that look convincing so that many people are successfully deceived. The information obtained from phishing data can be used to deceive victims or sold to other parties to commit irresponsible acts such as account misuse.

Phishing is done by faking official websites to deceive victims, which can be punished under the ITE Law and the Criminal Code. Various phishing techniques have been developed, such as phishing scams that send links or files modified or contain malware and blind phishing sent via bulk email without any strategy. In professional ethics, phishing is a cybercrime that can significantly harm victims. Therefore, it is imperative to understand the ways of phishing and avoid such attacks by monitoring accounts, not giving out personal data to anyone, and not clicking on suspicious links.

Phishing has a significant impact on the information and communication technology profession. Here are some of the effects that can be identified:

1. Data Loss: Phishing can lead to significant data loss, including personal information, passwords, and financial data. Phishing victims can become victims of fraud and other online crimes.
2. Reputational Loss: Phishing can damage the reputation of information and communication technology professionals, as phishing victims can become victims of fraud and other online crimes. This impact can continue at the organizational and industry levels.
3. Security Losses: Phishing can disrupt the security of information technology systems and applications, leading to significant losses for organizations and individuals. These impacts can be in the form of financial, data, and reputational losses.
4. Time Loss: Phishing can cause significant time losses for technicians and information technology professionals, as they have to spend time dealing with phishing attacks and repairing the resulting damage.
5. Cost Loss: Phishing can cause significant costs for organizations and individuals, as they must spend money to address phishing attacks, repair damage, and maintain system security.
6. Quality Loss: Phishing can lead to a loss of quality for information technology professionals, as phishing victims can become victims of fraud and other online crimes. This impact can continue at the organizational and industry levels.

DOI 10.62885/improsci.v2i1.440

7. Loss of Trust: Phishing can lead to a loss of trust in information technology professionals, as phishing victims can become victims of fraud and other online crimes. This impact can continue at the organizational and industry levels.

The impact of phishing on the information and communication technology profession is significant and can continue at the organizational and industry levels. Therefore, technicians and information technology professionals need to understand the ways of phishing and avoid such attacks by monitoring accounts, not giving personal data to anyone, and not clicking on suspicious links.

Types of phishing

1. Web Phishing is phishing that uses fake websites to trick victims. Phishing websites are designed to appear similar to legitimate websites and often use similar domain names.
2. Email Phishing is a type of phishing that uses email to trick victims. The fake emails may contain links or files modified to trick the victim.
3. Smishing Phishing: A type of phishing that uses SMS and phone calls to trick victims.
4. Phishing Scam: This is a type of phishing scam in which links or files that are modified or contain malware are sent to trick victims and obtain personal information.
5. Blind Phishing: Phishing sent via bulk email without a strategy.
6. Whaling: A type of phishing that targets influential individuals or high-ranking officials to obtain sensitive information.
7. Angler Phishing: A type of phishing that targets social media users through private messages (DMs) or malware notifications.

By understanding the types of phishing, you can be more vigilant and protected from phishing attacks.

Loss

Phishing is a cybercrime that provokes victims to voluntarily provide personal data without realizing it. The losses from phishing are significant and can have an impact on financial losses, data losses, and reputational losses. Here are some examples of the disadvantages of phishing:

1. Financial Losses: Phishing can lead to significant financial losses, such as fraud, data theft, or illegal data sales. Phishing victims can become victims of fraud and other online crimes.
2. Data Loss: Phishing can cause significant data loss, such as loss of personal data, account data, and financial data. Data obtained from phishing victims can be used for criminal purposes, such as fraud, theft, or illegal data sales.
3. Reputational Loss: Phishing can damage the reputation of information and

DOI 10.62885/improsci.v2i1.440

communication technology professionals, as phishing victims can become victims of fraud and other online crimes. This impact can continue at the organizational and industry levels.

4. Time Loss: Phishing can cause significant time losses for technicians and information technology professionals, as they have to spend time dealing with phishing attacks and repairing the resulting damage.
5. Cost Loss: Phishing can cause significant cost losses for organizations and individuals, as they must spend money to address phishing attacks, repair damage, and maintain system security.
6. Quality Loss: Phishing can lead to a loss of quality for information technology professionals, as phishing victims can become victims of fraud and other online crimes. This impact can continue at the organizational and industry levels.
7. Loss of Trust: Phishing can lead to a loss of trust in information technology professionals, as phishing victims can become victims of fraud and other online crimes. This impact can continue at the organizational and industry levels.
8. Privacy Loss: Phishing can lead to significant privacy losses, such as personal data loss and online security loss. Phishing victims can become victims of fraud and other online crimes.
9. Security Losses: Phishing can lead to significant security losses, such as security system and sensitive data losses. Phishing victims can become victims of fraud and other online crimes.
10. Business Losses: Phishing can lead to significant business losses, such as lost sales and reputational losses. Phishing victims can become victims of fraud and other online crimes.

Thus, phishing losses are very significant and can impact financial losses, data losses, reputational losses, time losses, cost losses, quality losses, trust losses, privacy losses, security losses, and business losses. Therefore, phishing victims need to understand how phishing works and avoid such attacks by monitoring accounts, not giving out personal data to anyone, and not clicking on suspicious links.

Examples of Phishing Cases

Here are examples of phishing cases that are complex and require victim awareness to avoid such attacks:

1. **Case 1**: Phishing with Fake Emails. The phishers send a fake email that looks like an

DOI 10.62885/improsci.v2i1.440

official email from XYZ Bank. The email contains a link to a fake website similar to the original website of XYZ Bank. Victims who click on the link are directed to a fake website and asked to enter a username and password to "verify" the information.

2. **Case 2**: Phishing with Fake Websites. Phishing perpetrators create duplicate websites from a trusted institution, such as financial institutions. This fake website is similar to the real website, so the victim does not realize that they are being deceived. Victim
3. Those who access the fake website will be asked to enter personal data, such as name, address, and credit card number.
4. **Case 3**: Phishing with Fake SMS. The phisher sends a fake SMS that looks like an official SMS from XYZ bank. The SMS contains a message asking the victim to enter sensitive information, such as username and password, to "verify" the information.
5. **Case 4**: Phishing with Bulk Emails. Phishing perpetrators send bulk emails that appear to be official emails from trusted organizations. The email contains a link to a fake website similar to the organization's original website. Victims who click on the link are redirected to the fake website and asked to enter personal data.
6. **Case 5**: Phishing with WhatsApp Chats. The phishing perpetrator sent a fake WhatsApp chat that looked like an official chat from XYZ bank. The chat contains a message asking the victim to enter sensitive information, such as username and password, to "verify" the information.
7. **Case 6**: Phishing with Zoom. The phisher sends a fake email that looks like an official email from Zoom. The email contains a link to a fake website similar to Zoom's original website. Victims who click on the link are redirected to the fake website and asked to enter personal data.

Thus, the phishing case above shows that the perpetrator uses various techniques to trap the victim and obtain personal information. Therefore, it is essential for victims to understand how phishing works and avoid such attacks by monitoring accounts, not giving out personal data to anyone, and not clicking on suspicious links.

How to Overcome Phishing

Dealing with phishing is a complex strategy and requires victim awareness to avoid such attacks. Here are some steps you can take to address phishing:

1. Antivirus: An antivirus is a program that detects and removes viruses that enter a computer system. It can also help stop phishing attacks and protect victims' data.
2. Firewall: A firewall is a program that controls the traffic of data that enters a computer

DOI 10.62885/improsci.v2i1.440

system. It can help stop phishing attacks and protect victims' data.

3. Security System: A security system is a program that detects and removes viruses that enter a computer system. It can help stop phishing attacks and protect victims' data.
4. VPN: A VPN is a program that protects a victim's data when they access the Internet. It can help stop phishing attacks and protect victims' data.
5. Cloud Security Solution: A cloud security solution is a program that can protect victims' data by storing it on secure servers. It can help stop phishing attacks and protect victims' data.

How to Overcome Phishing by Using Strong Passwords

Phishing is a form of cybercrime that provokes victims to voluntarily provide personal data without realizing it. To overcome phishing, victims can use strong passwords. Here are some examples of how to create strong passwords:

1. Creating a Unique Password: The victim must create a password that is unique and not used by anyone else. Unique passwords can help stop phishing attacks and protect victims' data.
2. Creating a Strong Password: The victim must create a password that is strong and not easy to guess. Strong passwords can help stop phishing attacks and protect victims' data.
3. Creating a Long Password: The victim must create a password that is long and not easy to guess. Long passwords can help stop phishing attacks and protect victims' data.
4. Creating a Password That Uses Special Characters: The victim must create a password that uses special characters, such as symbols and numbers. Passwords that use special characters can help stop phishing attacks and protect victims' data.

How to Overcome Phishing by Using Two-Factor Authentication

Phishing is a cybercrime that provokes victims to voluntarily provide personal data without realizing it. To get around phishing, victims can use two-factor authentication. Here are some examples of how to use two-factor authentication:

1. Using OTP: Victims can use an OTP (One-Time Password) sent to their phone number or email. OTPs can help stop phishing attacks and protect victims' data.
2. Using Biometrics: Victims can use biometrics, such as fingerprints or faces, to authenticate themselves. Biometrics can help stop phishing attacks and protect victims' data.
3. Using Smart Cards: Victims can use smart cards that contain their personal information. Smart cards can help stop phishing attacks and protect victims' data.

DOI 10.62885/improsci.v2i1.440

Thus, dealing with phishing is a complex strategy that requires victim awareness to avoid such attacks. Therefore, phishing victims need to understand how phishing works and avoid such attacks by monitoring accounts, not giving out personal data to anyone, and not clicking on suspicious links.

The steps taken by the Indonesian government to tackle phishing in Indonesia include several strategies and preventive measures. Here are some examples of steps that have been taken:

1. Socialization: The Government of Indonesia, through the Personal Data Protection Law (PDP Law), conducts thorough socialization throughout the region to help the public understand their rights and obligations in dealing with phishing. The purpose of this is to help the public understand how to report illegal data collection by other parties.
2. Establishment of a Rapid Response Team: The Government of Indonesia established an emergency response team to handle cases of alleged public data leaks and other cyberattacks. Thus, the government can be faster and more effective in dealing with cyberattacks.
3. Development of the 'Born to Protect' Program: The government is working to attract talented young people to information technology through the 'Born to Protect' program, which aims to improve the community's ability to deal with cyber attacks.
4. Cooperation with the Police: The Government of Indonesia, through the National Police of the Republic of Indonesia, has taken several steps to combat cybercrime. The National Police's Cybercrime Directorate has tried to address cybercrime, including phishing, by increasing public awareness and improving law enforcement capabilities.
5. Surveillance and Education: The government is increasing public surveillance and education about phishing. For example, the Directorate General of Aptika Kominfo has held a campaign to raise public awareness about phishing and how to deal with cyberattacks.

Thus, the Indonesian government's steps to address phishing include socialization, the formation of a rapid response team, program development, cooperation with the police, and public surveillance and education.

CONCLUSION

In this study, an in-depth analysis has been carried out related to the phenomenon of phishing, an increasingly troubling online fraud practice. Through literature studies, case studies, surveys, and interviews, various aspects related to phishing have been explored. Here are the conclusions that can be drawn:

1. Phishing is a serious threat in cybersecurity, with the potential to financially damage individuals, companies, and other organizations and cause reputational damage.
2. Phishing techniques are constantly evolving and becoming more sophisticated, demanding vigilance and a deep understanding of scammers' tactics.
3. Education and public awareness play a key role in fighting phishing. The better the public understands phishing techniques and risks, the better they can protect themselves and their organizations.
4. Technical efforts such as cyber security training, implementation of robust security solutions, and constant monitoring of suspicious activity are essential in reducing the risk of falling victim to phishing attacks.
5. Collaboration between governments, the private sector, and other cybersecurity agencies is needed to develop effective strategies for dealing with the ever-evolving phishing threat.

With a better understanding of phishing and its prevention efforts, it is hoped that it will reduce the negative impact caused by phishing attacks and create a safer online environment for all users.

BIBLIOGRAPHY

Agustiawan, T. (2020). *Cyber Attacks and Their Prevention: A Case Study in Indonesia.*

CNN Indonesia. (2020, June 15). *Prevent Phishing in These 5 Ways. CNN Indonesia.* Retrieved from https:// www.cnnindonesia.com/teknologi/20200615150918-185-511174/cegah-act-phishing-with-5-ways-this

DetikInet. (2021, November 10). *5 Increasingly Scary Phishing Scam Modes. Detik.com.* Retrieved from https://inet.detik.com/cyberlife/d-5794084/5-modus-penipuan- phishing-which-is-getting scarier

Fikri, A. R., Pratama, A., & Nusa, I. N. S. (2020). *Website Phishing Data Analysis*

https://kominfo.go.id/content/detail/23498/phishing-pengenalan-dan-cara- Avoid it/0/artikel_gpr

Jurnal Abdi, 6(2), 187-193.

Kadir, A. (2018). *Cybercrime: Threats, Actions and Countermeasures*. Jakarta: PT Gramedia Pustaka Utama.

Kartikasari, D. (2020). *Analysis of Social Media Users' Awareness in Avoiding Phishing Attacks.* Journal of Business Information Systems, 9(1), 83-89.

Kominfo. (2021, May 20). *Phishing: Introduction and How to Avoid It. Ministry of Communication and Informatics*. Retrieved from

Maulani, E., Prasetya, Y., & Sofyan, S. (2021). *Detection of Phishing Attacks Using the Random Forest Method on the Instagram Social Media Network*. Cursor Journal, 7(1), 12-18.

Using Decision Tree Algorithm and Naïve Bayes Classifier. Journal of Information Technology and Computer Science Development (J-PTIIK), 4(5), 5186-5194.

Pahlevi, H. (2021). *Detection and Recovery of Phishing Attacks Using Random Forest Methods and K-means Clustering.* National Seminar on Information Technology and Its Applications (SENTIA), 8(1), 35-39.

Phishing detectors use the K-Nearest Neighbor (K-NN) algorithm. Journal of Science and Informatics, 1(1), 12-19.

Rohman, A. A., Darmalaksana, W., & Fathoni, F. M. (2022). *Analysis of the phishing detection system using the Random Forest method*. Journal of Informatics and Information Systems Engineering (JTISI), 8(1), 1-6.

Sarwiji, S., Pranowo, A. H., & Kusumo, B. A. (2020). *Knowledge Influence Analysis,*

Attitudes, and Subjective Norms towards Interest in Using Information Security Technology to Reduce Phishing Actions in the Internet of Things Era. Scientific Journal of Students of the Faculty of Engineering, 5(1), 28-35.

Suryaningsih, E., Wijaya, A., & Nanda, R. (2021). *System Design Analysis*

Usman, A. (2019). *Cyber Security: Threats and Protection. Jakarta*: Prenada Media Publisher.

Wahyuni, S. (2022). *The Need for Internet User Awareness in Phishing Prevention.*

Yogyakarta: CV. Andi Offset.