Cybercrime Awareness Phishing Email Using Secure Socket Layer as an Interpretation of Information Security

Kotim Subandi [1], **Dinar Munggaran A** [2], **Victor Ilyas Sugara** [3], **Adriana Sari Aryani** [4], **Hermawan** [5*]

[1,2,3,4] Department of Computer Science, Faculty of Mathematics and Natural Science, Pakuan University, Bogor, West Java, 16143, Indonesia

Abstract

Email phishing is a fraudulent technique used by cybercriminals to obtain sensitive information through emails that appear legitimate but have malicious purposes. Information security has become a crucial aspect in the increasingly developing digital world, especially along with the increasing threat of cybercrime, such as email phishing. In this context, implementing Secure Socket Layer (SSL) is one solution to increase awareness and mitigate risks against phishing attacks. SSL, which is a security protocol for data encryption, can help protect digital communications by authenticating servers and encrypting data sent, thereby reducing the potential for misuse of personal data sent via email. This research aims to examine the role of SSL in providing protection against email phishing and increasing user awareness regarding the importance of information security in the use of digital technology. Through an information security interpretation approach, this study suggests that SSL can serve as an effective barrier in reducing the risk of phishing attacks and increasing the level of user trust in the emails received. Therefore, it is important for individuals or organizations to understand and apply information security principles such as the use of SSL to maintain the integrity and confidentiality of data exchanged online

Keywords: *Cybercriminal; Email phishing; Information Security; Protocol; SSL*

1. Introduction

Crime in cyberspace has recently become very worrying makes us have to be even more vigilant. There are many forms of crime on social networks occurring at this time of the many attacks is phishing emails. Phishing itself is threat to internet users when they are surfing. If we are in target condition Phishing, there will be a lot of losses for us It's natural if you're not alert to what you're doing crime in cyberspace. For example, act data theft or even fraud material. Challenges that arise in Information technology continues to develop quickly provides opportunities for attackers to get access to various tools and software that can be used for carry out attacks, such as malware, exploit kits, and hacking services sold at black market.

It can even change the economic model and business models in the industrial world. Phishing crimes appear along with many activities on the internet as well as several The main reasons are related to technique deception is so effective because it is weak awareness regarding security systems in social networking. Usually human weakness (Human Error) that this user often ignoring caution or not trained in recognizing the signs of phishing. Fraudsters often take advantage of conditions users by creating a sense of worry, fear, urgency, so without realizing it getting victims to provide information their personality. Phishing mail is a form attacks on email users where the perpetrator trying to deceive a potential target victims via email that has a purpose to steal sensitive information such as words password, credit card number (Credit Card), even personal data such as e-KTP. E-mail Phishing is often created as if like a legitimate email from trusted organizations/companies, such as banks, online services, even companies big. Email phishing activities, perpetrators usually use techniques like Fraudulent identity of the email sent is visible like from an official organization, often by including a logo, format, as well as using very language

Convincing. Fake links received by the user in the email, include link that directs the victim/target clicking through to a fake website that was created looks genuine site, usually the target is requested enter their personal information. Attachments in emails can also include attachments that have been compromised

*Corresponding author. *E-mail address:* kotim.subandi@unpak.ac.id
Received: 5 May 2025, Accepted: 31 July 2025 and available online 31 July 2025
DOI: https://doi.org/10.33751/komputasi.v19i2.5260

by malware, when the attachment is opened, you can installing malware or even viruses on your computer user. Phishing emails frequently include an urgent message as well give the victim fear take immediate action, such as confirm account information or updating important details. Email hacking is a criminal act of someone or usually called hackers trying to gain access to other people's email accounts become a target even without permission. this condition can occur through several methods such as phishing, brute force attacks, using software (software) dangerous, even often exploited weak security in email services

The perpetrator can use the victim's data for various irresponsible actions answer, as an example of fraud as well illegal sale of data. Phishing is is a very serious crime dangerous even done in a way attacking various sectors. Like sectors Financial, technology, retail, and various sectors others.. Information obtained through phishing, such as passwords, card numbers credit, or other personal information, very valuable to the perpetrators because they can be sold buy or use to do not fraud such as online gambling, online loans. Look at the urgency of frequent phishing emails sometimes creates a sense of fear in the victim for example, the threat of an account being blocked make the recipient immediately do and act quickly without thinking about the impact that will appear. In an effort to overcome and provide solutions to actions email phishing, the author uses the method and techniques to apply either by individuals, organizations and companies for the sake of creating security and preventing phishing attacks. By applying Secure Socket Layer (SSL) or Transport Layer Security (TLS) to encrypt email communication between the sending server and recipient. With SSL/TLS, data transmitted via email will be encrypted, making it more difficult for phishers to steal sensitive information.

2. Methods (10 pt, bold)

In this research, it will be presented steps to be taken by study . here are the steps like collecting data, preprocessing data, making classification models to scenarios trials to be carried out in this research.

2.1 General Description

Methodology in this research depicted in the diagram as below This

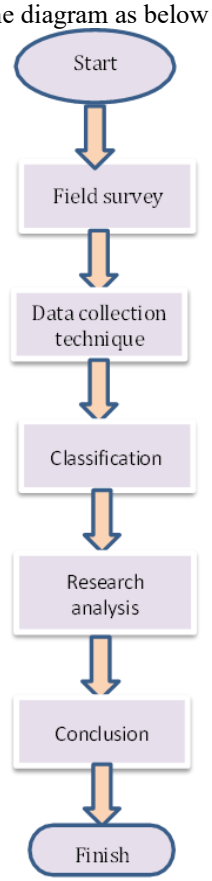

Figure 1. Research Stages

2.2 Data Collection Techniques

This method is used for collect all the information necessary for conducting research as well analysis. Tools to help in collecting data through a series of written questions answered by the respondent. After that is done observations then record the behavior or events directly in the field without intervention. Data obtained such as reports, articles, or historical notes will be in document not to continue. Below this is an example of a case study of the characteristics of phishing The email that was successfully obtained is as follows, password

experation, mailbox full, password leaking

2.3 Classification

Classification method for detection phishing emails by checking the URL structure to find a pattern of keywords which is often used by phishers. To ensure several criteria in help identify later grouping considered emails suspicious

2.4 Classification of Phishing Emails

Table 1. Classification of phishing emails

Types of Phishing	Content Characteristics	Visual Aspect	Sender Source	Expected action
Spear Phising	Dangerous link	Spelling and grammar errors	Suspicious sender address	Anxiety or urgency
Whaling	Dangerous attachments	Inconsistent design	Unusual sending patterns	Unreasonable offer
Clone Phising Agler Phising	Sensitive request			

3. Result and Discussion

3.1 Researcher's Analysis

The research conducted analysis on users who often receive emails that don't known. The following are some of the incidents experienced when the user is active using e-mail. There is a notification via email regarding password changes then it will ask for the old password and new password, the purpose of the website is not to change the password, but more towards obtain the user's password as seen in figure 2.

Figure 2. Mail Phishing Password Expiration

The next report is an email information about the mailbox, the sender's manipulating the recipient to reveal sensitive information or clicking on links that leads to malicious websites seen on figure 3

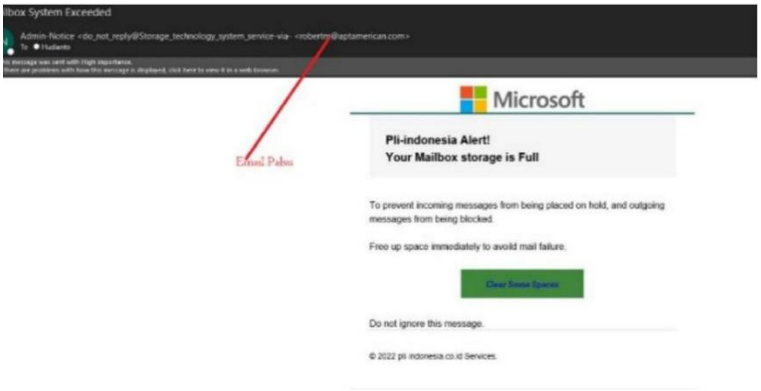

Figure 3. Mail Phishing Mailbox Full

Analysis and research findings below Email password leaked real email from Rere email is connected from email previously. If you notice there are any irregularities in this email s, namely the sender requested The email recipient opens the attachment with use the password listed on the body This email is included in the characteristics category content as in figure 4

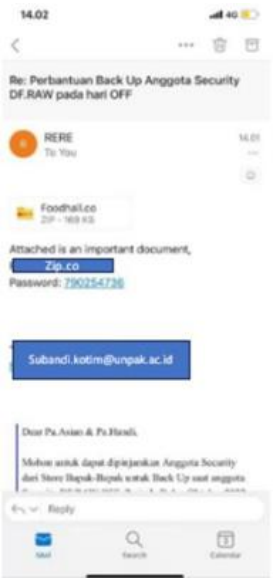

Figure 4. Password Leaked

Given these problems, then the author identifies as well analyze and then delve deeper into scheme used by para cybercrime in carrying out actions phishing. To avoid various phishing threat researchers tried implement Secure Socket Layer (SSL) and provide policies for users as an effort to create interpretation information security. Social media such as Email, Facebook, Instagram, and Twitter have billions active users. this means giving a big opportunity for hackers to reach and manipulate many potential victims with one attack. Many social media accounts, especially those have many followers or be connected to online shop, can be used as a source financial gain if successfully hacked. Additionally, hacked accounts can be sold back on the black market or used for financial fraud. On social media, hackers can create fake accounts that resemble official account or account of someone close to the victim.

With techniques such as cloning or impersonation, they can be convincing users to share personal information or clicking on dangerous links. Social media is also used for spreading malware or ransomware. Malicious links camouflaged as videos, interesting articles, or promotions can deploys easily and has high level of interaction on social media. Many users share information personal information on their profile, such as date of birth, email addresses, phone numbers, and even location. This data can be used for more personalized attacks, such as phishing and spear phishing, or use for steal someone's identity.

3.2 Solutions to Dealing with Phishing

In this case the researcher provides protection on websites with certificates SSL/TLS will have a starting URL with "https://" indicating that secure connection. Users should only entering sensitive information on sites with secure connection. Secure DNS and secure email has protection such as DMARC, SPF, and DKIM can help organizations prevent Fake emails claim to come from the domain themselves, which is a common tactic in phishing. Email will be equipped with SSL protection (Secure Sockets Layer) or TLS (Transport

Layer Security) to make email more secure rather than emails that do not have protection the. Because SSL/TLS helps secure data sent via email by encrypting the connection between email server and client (user) or between two email servers. With this encryption, data sent becomes difficult to access or read by unauthorized third parties, including hackers who try to eavesdrop data on the network. SSL/TLS only protects current data is being transmitted (data in transit), ie as long as the email is sent from the sender to recipient. As soon as the email arrives at the server recipient or accessed by the user, encryption this no longer applies. SSL/TLS protection on email does increase security and protect data during the transmission process, but not a guarantee of full security. Users still need to be careful with email received, especially against attacks phishing, ensure the server used safe, and avoid networks that are not secure or public to access email as seen in the image below.

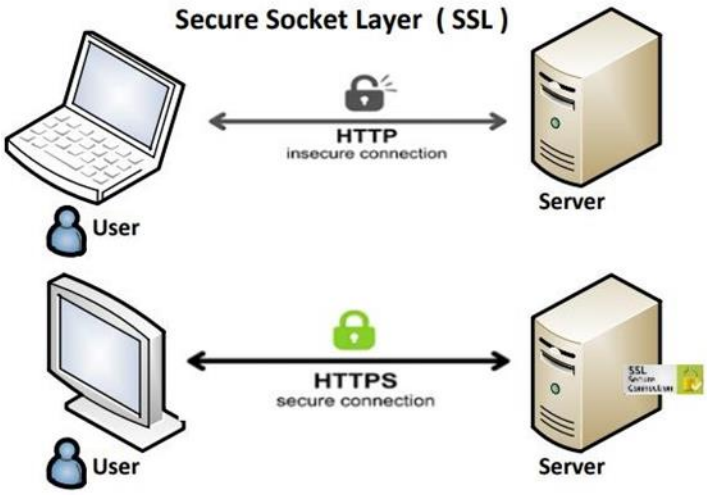

Figure 5. SSL diagram

Secure Socket Layer (SSL) configuration a reliable one involves several steps and best practices to ensure security Data communication is carried out via email This is truly the era of security. Although SSL has been largely replaced by TLS (Transport Layer Security), SSL term still frequently used today. Use a valid, issued certificate by a trusted Certificate Authority (CA). As an additional security setting enable HSTS to ensure the browser always use HTTPS. For security if using email, implement it MTA-STS to ensure usage

TLS in email sending. The following is the SSL/TLS configuration for web server uses Nginx and Apache. This configuration includes basic settings to enable SSL/TLS using valid certificate.

```
server {
    listen 443 ssl;
    server_name example.com www.unpak.ac.id;
    ssl_certificate /path/to/your/certificate.crt; # Sertifikat SSL
    ssl_certificate_key /path/to/your/private.key; # Kunci pribadi

    # Pengaturan SSL/TLS
    ssl_protocols TLSv1.2 TLSv1.3; # Hanya gunakan versi terbaru
    ssl_ciphers 'ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256'; # Cipher suites yang aman
    ssl_prefer_server_ciphers on; # Prioritaskan cipher server

    # HSTS
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
    location / {
        # Pengaturan lokasi
        try_files $uri $uri/ =404;
    }
}
```

Figure 6. SSL configuration with Nginx

```
<VirtualHost *:443>
    ServerName example.com
    ServerAlias www.unpak.ac.id

    SSLEngine on
    SSLCertificateFile /path/to/your/certificate.crt # Sertifikat SSL
    SSLCertificateKeyFile /path/to/your/private.key # Kunci pribadi
    SSLCertificateChainFile /path/to/your/chainfile.pem # Rantai sertifikat (jika diperlukan)

    # Pengaturan SSL/TLS
    SSLProtocol -all +TLSv1.2 +TLSv1.3 # Hanya gunakan versi terbaru
    SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256 # Cipher suites yang aman
    SSLHonorCipherOrder on # Prioritaskan cipher server

    # HSTS
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    DocumentRoot /var/www/html
    <Directory /var/www/html>
        AllowOverride All
    </Directory>
</VirtualHost>
```

Figure 7. SSL configuration with Apache

3.3 Security Interpretation With SSL

Focuses on providing layers protection for transmitted data between the client (such as a browser) and the server. SSL encrypt all data to be sent, so that sensitive information such as passwords, credit card numbers and personal data cannot be read by third parties possibly intercept communications. This encryption ensure that only recipients are has the right and legal right to decrypt and access information.

By using a digital certificate, SSL helps verify the server's identity. When a user connects to a website using SSL, they can be sure that they are connected to the correct server and not to a fake server. It protects users from attacks such as man-in-the middle. SSL ensures that data is shipped cannot be modified or stolen without being detected during the transmission process. If data is changed, the connection will be lost, and the user will be notified. SSL helps protect data from various attacks, including preventing parties third listen to communication, protect from attackers trying to position self between client and server, avoid attacks in which data is captured reused by the attacker

3.4 Information Security Education

One way to protect information on various threats, risks and destructive attacks, confidentiality, integrity and availability or commonly called with CIA (Confidential, Integrity Availability). With the aim of increase awareness and skills of each individuals/users and even organizations within maintain data and information system security valuable. In understanding the various types threats, such as malware, phishing, ransomware, and other cyber attacks. Providing training and education regarding basic principles such as use of strong passwords such as capital letters, numbers, symbols, minimal characters used, then update the software regularly, and appropriate access management, understanding and implement policies and procedures existing security in the organization or company in an effort to protect sensitive data, including encryption, data backup, and management of access rights.

This procedure applied to handle and respond security incidents if there is a breach or attacks into information systems owned. Cyber and technology continues to develop, education. training must be continuous so that knowledge and understanding are also up-to-date with developing trends or latest. Understand and comply with regulations and relevant standards, such as GDPR, HIPAA, or ISO 27001 is very important, depending on the industry, company as well location.To achieve information security The powerful write implements Filtering spam and device configuration for automatic phishing detection in emails detect and block emails suspicious, users must also be regular check and update filter settings used.

Using the device software for analyzing email traffic and detect indicating anomalies potential phishing attacks, such as patterns unusual delivery or volume of emails high in a short time. Apply two-factor authentication (2FA) method for accounts email and other important services. 2FA requires the user to enter additional information besides the password (for example, a code sent via SMS or authentication application) before you can access the account.

4. Conclusion

Awareness of the threat of crime cyber, especially email phishing attacks, is a very important thing in efforts to maintain information security. Phishing email is often the method that used by cybercriminals to deceive victims and obtain sensitive data, such as passwords, personal information, or data finance. In this context, Secure Socket Layer (SSL) and related security protocols such as Transport Layer Security (TLS) comes into play a very vital role as a tool for improve communications security and protect data from potential attacks.

Through use of SSL/TLS, data transmission via Email can be encrypted, which is not only ensure that the data sent is consistent safe, but also reduces the possibility theft of sensitive information. SSL/TLS assist in verifying the identity of the sender, which reduces the risk of fraud in form of phishing. Therefore, SSL can be considered as an important component in building an information security system effective and reliable. Additionally, implementation other techniques such as email authentication MFA, spam and phishing filters, and education Users also have no less role important in dealing with threats phishing.

By increasing awareness users against signs of phishing and the importance of data protection, the risk of attacks can be minimized. Overall, comprehensive approach and use of technologies such as SSL in secure email communications, combined with strict policies and ongoing education, will be significantly reduces the impact of an attack email phishing and improve resilience information security system at level individuals and organizations. Remove phishing emails from your inbox and from the trash or archive folder if any. This can reduces the risk if accidentally exposed again, immediately change the password (password) accounts that may be impacted. Use a strong and unique password for each email account.

References

[1] SADIQ, A., ANWAR, M., BUTT, R. A., MASUD,F., SHAHZAD, M. K., NASEEM, S., & YOUNAS, M. (2021). A review of phishing attacks and countermeasures for internet of thingsbased smart business applications in industry 4.0. Human Behavior and Emerging Technologies, 3(5), 854–864. https://doi.org/10.1002/hbe2.301

[2] OTO, I. (2021). IJRS: International JournalReglement & Society Cyber CrimeAccording to… Cyber

Crime According tothe ITE Law. August, 103– 110.
[3] MISHRA, A., & FANCY. (2021). Efficient Detection of Phising Hyperlinks using Machineearning. International Journal on Cybernetics & Informatics, 10(2), 23–33.https://doi.org/10.5121/ijci.2021.10020
[4] IRAWAN, D. (2020). Mencuri Informasi PentingDengan Mengambil Alih Akun Facebook Dengan Metode Phising. JIKI (Jurnal LlmuKomputer & Lnformatika), 1(1), 43–46 https://doi.org/10.24127/jiki.v1i1.671
[5] MUSLIM, N., SENJAYA, O., HUKUM, F., & KARAWANG, U. S. (2022).Pertanggung jawaban Hukum PlatformMedia Sosial Terhadap Korban PhisingMelalui Mass Tagging. 9(2), 955–963
[6] MOORTHY, R. S., & PABITHA, P. (2020). OptimalDetection of Phising Attack using SCA based K-NN. Procedia Computer Science,171(2019), 1716 1725.
[7] RAMADHAN, A., ALHAFIDH, M. A., &FIRMANSYAH, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud Terhadap Mahasiswa UNINUS. Kampret Journal,1(1), 11–15.https://doi.org/10.35335/kampret.v1i1.9.
[8] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," Springer Sci. Media, 2020
[9] M. K. Sharma and M. J. Nene, "Two-factor authentication using biometric based quantum operations," Secur. Priv., vol. 3, no. 3, 2020, doi: 10.1002/spy2.102.
[10] C. Z. Acemyan, P. Kortum, J. Xiong, and D. S. Wallach, "2FA might be secure, but it's not usable: A summative usability assessment of Google's two_factor authentication (2FA) methods," Proc. Hum. Factors Ergon. Soc., vol. 2, pp. 1141–1145, 2018, doi: 10.1177/1541931218621262
[11] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur., no. May, pp. 475–486, 2016, doi: 10.1145/2897845.2897916.
[12] R. S. Pressman and B. R. Maxim, Software Engineering A PRACTITIONER'S APPROACH. McGraw-Hill, 2020
[13] D. E. Kurniawan, M. Iqbal, J. Friadi, F. Hidayat, and R. D. Permatasari, "Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance," J. Phys. Conf. Ser., vol. 1783, no. 1, 2021, doi: 10.1088/1742-6596/1783/1/012041.
[14] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-Factor Authentication," IEEE Access, vol. 6, pp. 32677–32686, 2018, doi: 10.1109/ACCESS.2018.2844548
[15] N. Karapanos et al., "Sound-Proof : Usable Two-Factor Authentication Based on Ambient Sound This paper is included in the Proceedings of the," Usenix Secur., 2015.
[16] N. Morze, O. Buinytska, and L. Varchenko-Trotsenko, "Use of Bot_Technologies for Educational Communication At the University," Eff. Dev. Teach. Ski. Area Ict E-Learning, vol. 9, pp. 239–248, 2017, [Online]. Available: https://depot.ceon.pl/handle/123456789/15492
[17] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudary, "New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles," 2020 IEEE Asia_Pacific Conf. Comput. Sci. Data Eng. CSDE 2020, no. April 2021, 2020, doi: 10.1109/CSDE50874.2020.9411569.
[18] C. Adams, G. V. Jourdan, J. P. Levac, and F. Prevost, "Lightweight protection against brute force login attacks on web applications," PST 2010 2010 8th Int. Conf. Privacy, Secur. Trust, pp. 181–188, 2010, doi: 10.1109/PST.2010.5593241
[19] CASCAVILLA, G., TAMBURRI, D. A., & VAN DEN HEUVEL, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers and Security, 105, 102258.
[20] GULO, A. S., LASMADI, S., & NAWAWI, K. (2021). Cyber Crime dalam Bentuk PhisingBerdasarkan Undang- Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of crimimal Law 1(2) ,68-81 https/doi.org/10.22437/ pampas.v1i2.9574Criminal Law, 1(2), 68–81. https://doi.org/10.22437/pampas.v1i]