JPPIPA 11(4) (2025)

Jurnal Penelitian Pendidikan IPA

http://jppipa.unram.ac.id/index.php/jppipa/index

Enhancing Email Security Against Phishing Attacks Through User Behavior Analysis and Data Loss Prevention (DLP)

Tamara Sinatrya Yasmin[1*], Tomi Yulianto[2]

[1]Master of Information Technology: Data Science Cyber Security, Swiss German University, Indonesia.
[2]Master of Information Technology: Data Science Business Informatics, Swiss German University, Indonesia.

Received: November 12, 2024
Revised: February 04, 2025
Accepted: April 25, 2025
Published: April 30, 2025

Corresponding Author:
Tamara Sinatrya Yasmin
tamarasy15@gmail.com

DOI: 10.29303/jppipa.v11i4.10781

© 2025 The Authors. This open access article is distributed under a (CC-BY License)

Abstract: This study was conducted and aimed to improve email security against phishing attacks through user behavior analysis and data loss prevention (DLP). Phishing attacks pose a significant threat to the protection of user information and privacy, especially for individuals who are less aware of phishing emails. Their vulnerability to such attacks not only compromises their own security but also poses a great risk to the company. This can result in huge financial losses. Thus, there is an urgent need to improve security measures for users and systems. This study will use the NIST Cybersecurity Framework 2.0. This framework provides a structured approach to identifying and analyzing user behavior. Then an assessment of the phishing simulation is carried out to pay attention to users who are vulnerable to phishing attacks. After assessing the phishing email, the DLP configuration is determined for preventive measures. The following are the core functions of CSF as a framework that will be used: Based on the phishing simulation conducted, the pattern is almost the same, displaying the sender's email domain that is very similar to the original. Employees are usually easily trapped if they do not read the domain carefully and immediately follow the instructions in the email body. Phishing emails typically have a business context and are assumed to be sent by a trusted person, such as a supervisor, a colleague from the same department, or a different department. User behavior analysis is key to identifying vulnerabilities to phishing attacks. Understanding how users interact with emails can help develop effective mitigation strategies. Implementing DLP as a layer of defense can proactively detect and prevent phishing emails from reaching users' inboxes. Proper DLP configuration is critical to a successful implementation. User education and training are critical components to raising awareness of phishing threats. Equipping users with the skills to recognize and avoid phishing attacks can significantly reduce an organization's vulnerability.

Keywords: Attacks; Data Loss Prevention (DLP); Email; Phishing; Security; User behavior

Introduction

Continuous phishing attacks pose a serious threat to information security and user privacy (Alsharnouby et al., 2015). Therefore, it is very important to take effective measures to address the problem of user behavior in response to phishing emails (Shahbaznezhad et al., 2021; Dawkins & Jacobs, 2023). This research proposal aims to improve email security against phishing attacks through user behavior analysis and data loss prevention (DLP) (Liu & Kuhn, 2010; Yadav & Gupta, 2023).

This project has the primary goal of identifying user behavior patterns that indicate vulnerability to phishing attacks through analysis of user behavior and email

How to Cite:
Yasmin, T. S., & Yulianto, T. (2025). Enhancing Email Security Against Phishing Attacks Through User Behavior Analysis and Data Loss Prevention (DLP). *Jurnal Penelitian Pendidikan IPA*, *11*(4), 590–600. https://doi.org/10.29303/jppipa.v11i4.10781

interactions (Shahbaznezhad et al., 2021). Additionally, using DLP policies that act as an important line of defense against malicious emails, it also detects and filters phishing emails before they reach the user's inboxes (Alsharnouby et al., 2015; Steves et al., 2020; Wiranata et al., 2024).

To achieve the goals of this project, a structured approach will be taken to manage and deal with cyber security threats and risks, through the NIST Cybersecurity Framework. This framework has core functions that will guide our discussion and implementation of DLP policies (Mansikka, 2023). It consists of govern, identification, protection, detection, response and recovery (Moore, 2024). This research also includes initiatives in the form of campaigns, education and socialization to target user awareness. So that later it can increase user awareness of phishing attacks and improve the organization's overall security posture (Wang et al., 2020; ISO/IEC, 2018; Li et al., 2019).

In conclusion, this project proposal addresses the critical need for enhancing email security against phishing attacks through user behavior analysis and DLP. By implementing effective measures, organizations can proactively mitigate the risks associated with phishing attempts and improve their overall security posture (Senapati et al., 2023). The objective of this research is to make a contribution to the field of cybersecurity by providing valuable insights complemented by practical solutions to combat phishing attacks (Kapoor, 2024).

Requirements

In this project, the security goals are: Decreased the chance of phishing attacks on email, basically due to vulnerable and unsafe user behavior; Enhance organizational security and ensure compliance with DLP privacy regulations, which are instituted to uphold data security standards; Increased user mindfulness of phishing attacks and the preventive measures to be taken.

In order to achieve the outlined security goals effectively, it is essential to ensure that the necessary requirements are met to support the successful implementation of this project (Wendy, 2024). The requirements are: Phishing Simulation Tools, Tools to conduct phishing simulations and evaluate user responses. The simulations should include various types of phishing attacks to test user vulnerability and measure the effectiveness of the training and DLP policies implemented (Chaganti et al., 2022); Data Loss Prevention Implementation, Implementation of DLP systems to identify, monitor, and protect sensitive data from unauthorized access, transmission, or disclosure. The DLP system must filter and detect phishing emails before they reach user inboxes; User Training Platforms, Platforms for conducting training sessions and awareness programs for users to recognize and avoid phishing attacks (Abid, 2020). Incident Management and Recovery Systems, Systems for managing phishing incidents, including reporting and handling complaints effectively. These systems should also support recovery efforts, such as restoring compromised accounts and evaluating the entire system for security breaches or ongoing threats (Kovaitė et al., 2020; Firdaus et al., 2023).

Problem Statement

Phishing attacks bring significant threats to information protection and user privacy, particularly for individuals lacking awareness of phishing emails. Their susceptibility to such attacks not only harms their own security but also poses substantial risks to the company. This can result in extensive financial losses (Omodara, 2022). Thus, there is a pressing need to enhance security measures for both users and systems (Leo et al., 2019; Saunders et al., 2021).

Method

Framework

This research will use the NIST Cybersecurity Framework 2.0. This framework provides a structured approach to identify and analyze user behavior. Then an assessment of the phishing simulation is carried out to pay attention to users who are vulnerable to phishing attacks (Ahmed et al., 2023). After assessing phishing emails, the DLP configuration is determined for preventive measures (Marcillo-Delgado et al., 2022). The following are the core functions of CSF as a framework that will be used.

The following are the parameters used in implementing the Cybersecurity Framework (Jaeger et al., 2021).

Figure 1. CSF's core function is as a framework

The following are the parameters used in implementing the Cybersecurity Framework.

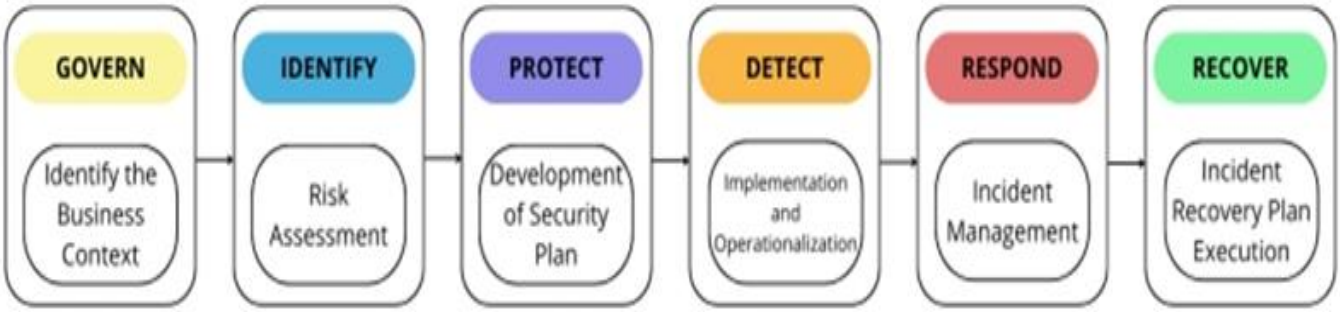

Figure 2. Parameters in the implementation of the Cybersecurity Framework

Identify the Business Context

At this stage, carry out an analysis that phishing attacks are very dangerous. So, it is necessary to increase user awareness about the importance of keeping sensitive data safe from phishing attacks; Collect user behavior data related to email, such as interaction patterns in email, habits in opening or downloading attached files, and tendencies in opening unsafe links; Assess the scoring of phishing simulations conducted to increase user awareness.

Risk Assessment

Analyzing the potential risk of users falling victim to phishing attacks with scoring of phishing email. Successful phishing not only causes great losses to the individual, but also poses a great threat to the entire organization.

Development of Security Plan

Various actions to mitigate phishing attacks can be taken based on the results of the risk assessment in the previous stage, including: User awareness with providing appropriate training and education to employees to recognize and avoid phishing; and Technical control with implementing the necessary DLP configurations to filter and detect phishing attacks on incoming emails.

Implementation and Operationalization

Establishing the DLP configuration as an implemented countermeasure. This DLP serves as an early warning for users; and Evaluate the application of the specified (DLP) configuration.

Incident Management

Incident management is needed when a phishing attack occurs and results in victims, it is mandatory to have a complaint service with the aim of stopping the spread of phishing attacks effectively and efficiently (Shahbaznezhad et al., 2021).

Incident Recovery Plan Execution

At the recovery stage, propose formal efforts to recover the accounts of users affected by phishing, then carry out a thorough evaluation of the entire system to guarantee and ensure that there are no security breaches or potential ongoing threats (Isaura et al., 2020).

Design and Prototype

In the execution of this project, a comprehensive plan for testing is essential. Consequently, this project includes the following design and prototype details (Emenike, 2021).

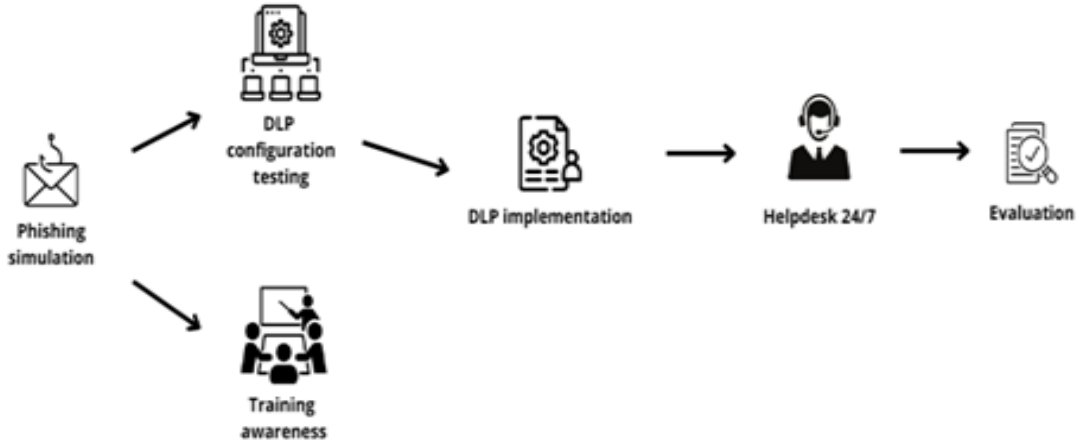

Figure 3. Design and prototype

Phishing Simulation

The purpose of this phishing simulation is to analyze the behavior patterns of users who fall for phishing attacks. The simulation will utilize a variety of phishing emails, each with different types of messages. As part of this project, two rounds of phishing simulations will be conducted, targeting all 14,020 employees (Kintonova et al., 2021).

DLP Configuration Testing

The DLP configuration testing is designed to evaluate the viability of deploying DLP on the office server as a proactive measure against phishing emails targeting employees. This entails configuring filters on a local VPS to serve as criteria for blocking incoming emails (Steves et al., 2020).

Training Awareness

Awareness training will be provided to all employees, with specialized sessions for those who were trapped to phishing simulations. This approach aims to increase overall employee awareness and vigilance against phishing emails (Hassib & Shires, 2024).

DLP Implementation

The implementation of DLP will be carried out in the office environment, adhering to the configurations that were successfully tested earlier (Syarova et al., 2024).

Helpdesk 24/7

The help desk is established to provide a dedicated complaint service for employees who trapped to phishing attacks. It operates 24/7, ensuring prompt assistance and effective mitigation measures to address phishing incidents (Beyer, 2023).

Evaluation

The evaluation phase involves regular monitoring and assessment of DLP performance, along with monthly reviews of employee awareness levels. This ongoing process aims to continually improve security performance and ensure high-quality outcomes (Liesnaia & Malakhov, 2023).

Timeline

This project adheres to a carefully structured timeline for its execution. Following discussions with key stakeholders within the office, the timeline has been refined and updated as follows.

Table 1. Timeline

Activity	March			April				May				June				July			
	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4
Identify the business context																			
Risk assessment																			
Development of a security plan																			
Implementation and operationalization																			
Incident management																			
Incident recovery plan execution																			

Result and Discussion

Risk Assessment

Before conducting the testing, a self-risk assessment is performed to determine the magnitude of risks associated with this project (Domnik & Holland, 2024).

Threat Identification

The main threat identified in this project is phishing attacks, which can result in the leakage of sensitive data, vulnerability to malware attacks, and financial losses. These threats can occur due to user behaviors that are vulnerable to phishing attacks and a lack of effective security measures (Adeyeri & Abroshan, 2024).

Risk Analysis

Table 2. Impact score table

Score	Definition
1	Minimal financial impact, no operational disruptions.
2	Minor financial impact, minor operational disruptions.
3	Moderate financial impact, minor reputational damage, and manageable operational disruptions.
4	Significant financial impact, serious reputational damage and major operational disruptions.
5	Major financial impact, severe reputational damage and total operational failure.

Table 3. Likelihood score table

Score	Definition
1	Once every year
2	Once every semester
3	Once every quarter
4	Once every month
5	Twice every month

Table 2 shows the impact score, and Table 3 shows likelihood score, and Figure 4 shows risk score to determine the level of risk indicators presents in this project. These indicators are determined based on the methods outlined in ISO 27005 (ISO/IEC, 2018).

Likelihood							
	High	5	5	10	15	20	25
	Moderate to High	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Low to Moderate	2	2	4	6	8	10
	Low	1	1	2	3	4	5
			1	2	3	4	5
			Low	Low to Moderate	Moderate	Moderate to High	High
			Impact				

Indicator	Value
High	> 20
Moderate to High	11 to 20
Moderate	8 to 10
Low to Moderate	4 to 7
Low	< 4

Figure 4. Risk score

After determining the scores for the risk assessment, here is a list of potential risks and the evaluations, along with a treatment plan to mitigate risky actions and the expected reduction in risk levels (Khanna, 2024).

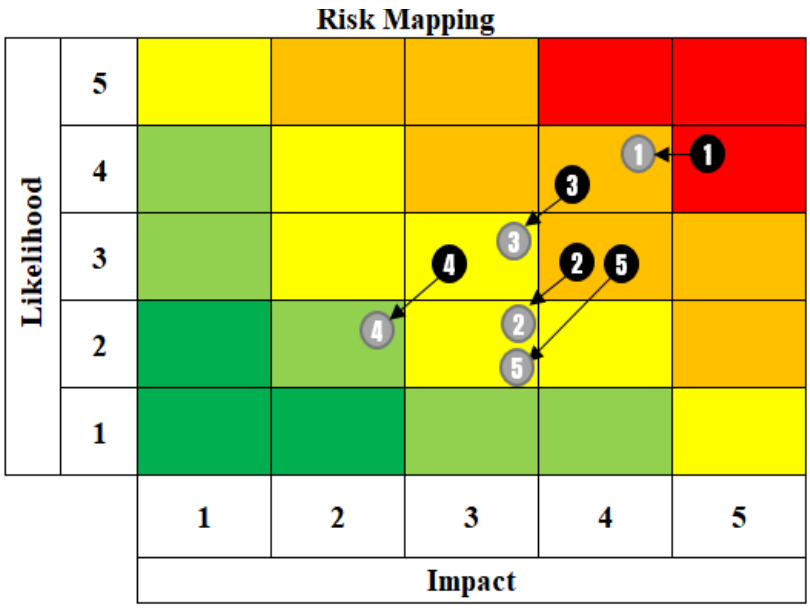

Figure 5. Risk mapping current and expected

Table 4. Risk analysis and treatment plan

	Activity	Risk	Impact	Likelihood	Impact score	Likelihood score	Inherent risk	Risk score	Treatment plan	Expected risk level
People	Using tools to conduct phishing simulations and evaluate user responses.	Users are unable to recognize phishing emails.	Data breach and financial loss.	High, especially if users are not well-trained.	5	4	20	High	Increase the frequency of phishing simulations.	Moderate to high
	Conducting training and awareness campaigns to recognize and avoid phishing attacks.	Users remain unaware of phishing despite being trained.	An unauthorized access	Moderate, if training is ineffective or not ongoing.	4	3	12	Moderate to high	Provide feedback and monitor employee performanc e during training.	Moderate
Process	Monitoring and detection process of cyber attacks.	Failure to detect phishing attacks.	Undetected intrusion into the company's system, resulting in significant data loss.	Moderate, depending on the effectiveness of the monitoring and response system in place.	4	4	16	Moderate to high	Implement automatic detection systems.	Moderate to high
	Testing the configuration of DLP (Data Loss Prevention).	Configuration failure.	Failure of email filtration allowing phishing emails into the inbox.	Moderate, depending on the volume of incoming emails.	3	3	9	Moderate	Test the latest and most updated DLP (Data Loss Prevention) scenarios.	Low to moderate
Technology	Implementing DLP system to detect and protect sensitive data.	DLP failure to detect phishing emails.	Malware spread and unauthorized access.	Moderate, depending on the configuration and monitoring implemented .	4	3	12	Moderate to high	Regularly updated, monitor, and maintain installed systems.	Moderate

Scoring Phishing Simulation

Prior to conducting a phishing simulation to evaluate its difficulty level, a scoring system is applied to the emails that will be sent to all employees (Adeyeri & Abroshan, 2024). The phishing scoring involves several stages, which are outlined below.

Flowchart Scoring Phishing Simulation Framework 1From the above flowchart, several stages can be conducted as: Identification of Suspected Emails, Collect the emails containing phishing attempts for scoring purposes; Phishing Indicator List, Analyzed the key performance metrics detailed in the email against the relevant industry standards outlined in the NIST guidelines; Choose the Premise Alignment Element, This section will provide a detailed examination of the key premise elements referenced in the NIST standards and how these assessments can be adapted and implemented effectively in an office environment; Assessment and Categorization, Conduct phishing simulation assessments based on pre-defined parameters; Interpreting Results, Compile the findings from the phishing simulation assessment.

The scoring of this phishing simulation is conducted in the sequence described in the diagram above. Next, the phishing scoring is carried out using the following defined parameters (Nayak et al., 2024). The assessment of phishing attacks in this research is carried out by applying the scoring method to phishing simulations. The scoring process is carried out on each phishing email using Phish Scale parameters (Steves et al., 2020). For example, the assessment of visual branding indicators is seen from the presence or absence of an official logo and format consistency that can be measured for format suitability (Omotunde & Ahmed, 2023). Content analysis is also carried out to assess several aspects such as sentence structure, quality of message content, and persuasive tricks (Nayak et al., 2024). Assessment is also done on sender information based on the validity of the

email address and display name. Links and URLs are assessed based on their consistency and validity. Meanwhile, attachments are assessed based on context relevance and potential risk of phishing attacks (Dawkins & Jacobs, 2023). The following assessment parameters can be measured numerically according to the specified cues (Khan et al., 2024).

Table 5. The following questions are answered with "yes" or "no". If “yes” then it has a value of 1 and “no” has a value of 0

Cues Type	Question
Technical Indicators	Is the sender's name not associated with the sender's email address, including the address of the "reply-to"?
	Is the domain name applied in the sender's email address similar to a recognizable entity domain?
Visual Presentation Indicators	Are there any branding elements (texts or logos) missing?
	Does the design and format of the email look unprofessional?
Language and Content	Does the email lack common greetings, either formal or informal greetings?
	Does the email lack any kind of personalization?
	Does the message lack details about the sender, such as sender or contact information?
Common Tactics	Does the message look like a work- or business-related process?
	Does the message appear to come from a friend, colleague, boss, other authority entity, or other reputable entity of authority?

Part 2: Count the Total Number of Times the Following Appear in the Email:

Errors

1. How many spelling mistakes are there in the email?
2. How many grammatical errors are there in the email, including inappropriate plurals?
3. How many contradictions or inconsistencies are there in the email?

Technical Indicators

1. How many potentially malicious attachments are included in the email?
2. How many times does the text hide the actual URL through a hyperlink?
3. How many links have a domain name similar to the domain name of a recognizable entity?

Language and Content

1. How many times is legal language used within the message, such as copyright information, disclaimers, or tax information?
2. How many unnecessary aspects of detail are present in the message?
3. How many requests for sensitive information in the email, including personally identifiable information or credentials?
4. How many times does the email reveal time pressure, including implied?
5. How many threats are included in the message, including implied threats?

Common Tactics

1. How many requests does the email make to help others?
2. How many times has the email offered something too good to be true, such as winning a contest, sweepstakes, free holiday, and so on?
3. Does it offer something personalized and unexpected just for you?
4. How many times did the email offer something for a limited time?

Following the completion of responses to determined cues, where participants answer either "yes" or "no," it becomes possible to calculate the quantity of "yes" answers received (Dawkins & Jacobs, 2023). This count of "yes" responses can serve as a determinant for the phish scale, utilizing the specified parameters below (Prince et al., 2024).

To determine its value, it is necessary to first define the premise of the assessment within the email simulation (Montano et al., 2024). This premise includes the content in the email that will be used for phishing (Steves et al., 2020). Here is the premise that will be utilized in the assessment of phishing emails for this research:

1. Imitate workplace processes or practices: this element tries to capture the alignment of the premise with a process or practice in the workplace for the target audience.
2. Has relevance to the workplace: this element tries to reflect the suitability of the premise to the target audience.
3. Aligns with other situations or events, including those outside the workplace gives the message a sense of familiarity.
4. Raises concerns about the consequences of NOT clicking: a stimulus that has the potential to cause harm by not clicking increases the likelihood of clicking.
5. Has been the subject of targeted training, specialized warnings or other exposure: this element is intended to reflect the effects of targeted training that would lead to detection of the premise.

Once the available premise questions have been answered, the corresponding ratings will be categorized according to the following classifications (Steves et al., 2020).

Table 6. Phishing simulation scoring results

Title	Total Cues	Cues Category	Premise Alignment	Premise Alignment Category	Overall Scoring
Simulation 1	12	Some	26	Strong	Very Difficult
Simulation 2	16	Many	28	Strong	Very Difficult
Simulation 3	14	Some	20	Strong	Very Difficult
Simulation 4	12	Some	22	Strong	Very Difficult
Simulation 5	13	Some	14	Medium	Moderately Difficult

After scoring the types of emails to be used in the simulation, the phishing simulations were conducted for 14,020 employees over two periods. A total of 119 employees fell for the phishing attempts twice in a row.

DLP Testing

In this DLP testing phase, a local VPS is utilized to assess the delivery of phishing emails and to evaluate the configurations designed to filter incoming phishing emails (Aziz et al., 2022). In this testing, it will implement several word filters and restrictions on documents with specific extensions, such as .html, .exe, and .apk (Marques, 2024). The word filters to be applied are as follows: The results of the testing phase are as follows: the simulation emails were promptly blocked as SPAM.

```
body    LOCAL_RULE1    /password/i
score   LOCAL_RULE1    40.0
body    LOCAL_RULE2    /form/i
score   LOCAL_RULE2    40.0
body    LOCAL_RULE3    /email/i
score   LOCAL_RULE3    40.0
body    LOCAL_RULE4    /dokumen/i
score   LOCAL_RULE4    40.0
body    LOCAL_RULE5    /document/i
score   LOCAL_RULE5    40.0
body    LOCAL_RULE6    /credit card/i
score   LOCAL_RULE6    40.0
body    LOCAL_RULE7    /creditcard/i
score   LOCAL_RULE7    40.0
body    LOCAL_RULE8    /nomor hp/i
score   LOCAL_RULE8    40.0
body    LOCAL_RULE9    /nomorhp/i
score   LOCAL_RULE9    40.0
body    LOCAL_RULE10    /handphone/i
score   LOCAL_RULE10    40.0
body    LOCAL_RULE11    /data diri/i
score   LOCAL_RULE11    40.0
body    LOCAL_RULE12    /datadiri/i
score   LOCAL_RULE12    40.0
body    LOCAL_RULE13    /formulir/i
score   LOCAL_RULE13    40.0
body    LOCAL_RULE14    /kode/i
score   LOCAL_RULE14    40.0
body    LOCAL_RULE15    /kode keamanan/i
score   LOCAL_RULE15    40.0
body    LOCAL_RULE16    /keamanan/i
score   LOCAL_RULE16    40.0
body    LOCAL_RULE17    /tautan/i
score   LOCAL_RULE17    40.0
body    LOCAL_RULE18    /aturan/i
score   LOCAL_RULE18    40.0
```

Figure 6. Simulation 1

Figure 7. Simulation 2

Figure 8. Simulation 3

Figure 9. Simulation 4

Figure 10. Simulation 5

Figure 11. simulation 6

The simulation results showed that all emails were successfully bounced and did not reach the intended inboxes (Kulkarni & Girish, 2024). The logs indicated 'Blocked SPAM' for these emails.

Training Awareness

Following the simulation, a comprehensive awareness training program was rolled out to enhance employees' understanding of cybersecurity threats. These training sessions were designed with interactive quiz-based themes such as "Beware of Phishing," "The Importance of Protecting Personal Data," and other relevant security topics to engage employees and reinforce key concepts.

To further solidify this initiative, an email blast campaign was implemented, providing employees with visually engaging infographics and clear explanations regarding various cyber risks. These emails served as periodic reminders to encourage proactive security practices in daily operations.

Additionally, as part of a continuous reinforcement strategy, desktop wallpapers across all company devices were regularly updated with cybersecurity awareness messages. This ensured that every time an employee accessed their workstation, they were reminded of best practices for safeguarding company data. By integrating these multiple layers of awareness, the organization aimed to instill a culture of cybersecurity vigilance across all levels (Shishodia & Nene, 2022). Employees who have been caught by phishing simulations twice consecutively will undergo training, including a post-test (Vashishth et al., 2024).

Contribution on This Project

For this project, the author's contributions included: conducting phishing simulation exercises; performing data loss prevention (DLP) testing personal environments; and developing post-test for employees caught in the phishing tests.

Conclusion

Based on the phishing simulation that was conducted, the pattern was almost the same, featuring a sender email domain that closely resembled the original. Employees are typically easily trapped if they do not carefully read the domain and immediately follow the instructions in the email body. Phishing emails usually have a business context and are perceived as being sent by a trusted person, such as a supervisor, a colleague from the same division, or from a different division. User behavior analysis is key to identifying vulnerabilities to phishing attacks. Understanding user interaction patterns with emails can help develop effective mitigation strategies. Implementing DLP as a defense layer can proactively detect and prevent phishing emails from reaching users' inboxes. Proper DLP configuration is crucial for successful implementation. User education and training are vital components to increase awareness of phishing threats. Equipping users with the skills to recognize and avoid phishing attacks can significantly reduce organizational vulnerability.

Acknowledgements

Thank you to the lecturers of Data Science Cyber Security, Swiss German University Indonesia who have supported the NIST Cybersecurity Framework 2.0 research, which will later provide a structured approach to identifying and analyzing user behavior.

Author Contributions

This article was prepared by two people, namely T.S.Y. and T.Y.: writing original draft preparation introduction, result, discussion, methodology, and then conclusion. These two authors also have ideas for the research process, data processing, conversion to English, review, editing.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

References

Abid, N. (2020). Advancements and Best Practices in Data Loss Prevention: A Comprehensive Review. *Global Journal of Universal Studies*, *1*(1), 190–225. Retrieved from https://media.neliti.com/media/publications/590136-advancements-and-best-practices-in-data-a5521663.pdf

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682. https://doi.org/10.3390/info15110682

Ahmed, M. N., Mahmood, H., & Iqbal, Z. (2023). A Novel Framework for Email's Data Leak Prevention Through Semantic Analysis. *2023 International Conference on It and Industrial Technologies (ICIT)*, 1–6. https://doi.org/10.1109/icit59216.2023.10335896

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why Phishing Still Works: User Strategies for Combating Phishing Attacks. *International Journal of Human Computer Studies*, *82*, 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Aziz, F., Mayasari, N., Sabhan, S., Zulkifli, Z., & Yasin, M. F. (2022). The Future of Human Rights in the Digital Age: Indonesian Perspectives and Challenges. *Journal of Digital Law and Policy*, *2*(1), 29–40. https://doi.org/10.58982/jdlp.v2i1.292

Beyer, J. L. (2023). The Politics of Cybersecurity and the Global Internet. *Perspectives on Politics*, *21*(2), 664–668. https://doi.org/10.1017/s1537592723000361

Chaganti, R., Varadarajan, V., Gorantla, V. S., Gadekallu, T. R., & Ravi, V. (2022). Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet*, *14*(9), 1–20. https://doi.org/10.3390/fi14090250

Dawkins, S., & Jacobs, J. (2023). *NIST Phish Scale User Guide*. Gaithersburg: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.TN.2276

Domnik, J., & Holland, A. (2024). On Data Leakage Prevention Maturity: Adapting The C2m2 Framework. *Journal of Cybersecurity and Privacy*, *4*(2), 167–195. https://doi.org/10.3390/jcp4020009

Emenike, S. U. (2021). *Data Loss Prevention in A Remote Work Environment*. Retrieved from https://urn.kb.se/resolve?urn=urn%3anbn%3ase%3ahis%3adiva-20203

Firdaus, G. A., Sukowati, P., & Adi, D. S. (2023). Licensing of MSME Business Through Online Single Submission Risk Based Approach. *Cross Current International Journal of Economics, Management and Media Studies*, *5*(02), 11–20. https://doi.org/10.36344/ccijemms.2023.v05i02.001

Hassib, B., & Shires, J. (2024). Digital Recognition: Cybersecurity and Internet Infrastructure in UAE–Israel Diplomacy. *International Affairs*, *100*(6), 2399–2418. https://doi.org/10.1093/ia/iiae233

Montano, I. H., Diaz, J. R., Aranda, J. J. G., Molina-Cardín, S., López, J. J. G., & Díez, I. D. L. T. (2024). Securecipher: An Instantaneous Synchronization Stream Encryption System for Insider Threat Data Leakage Protection. *Expert Systems with Applications*, *254*, 124470. https://doi.org/10.1016/j.eswa.2024.124470

Isaura, E. R., Chen, Y.-C., Su, H.-Y., & Yang, S.-H. (2020). The Relationship between Food Security Status and Sleep Disturbance Among Adults: A Cross-Sectional Study in An Indonesian Population. *Nutrients*, *12*(11), 3411. https://doi.org/10.3390/nu12113411

ISO/IEC. (2018). *ISO/IEC 27005: 2018 Information Security Risk Management-Guidelines*. *2018*. Retrieved from https://www.iso.org/standard/75281.html

Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The Role of Deterrability for the Effect of Multi-Level Sanctions on Information Security Policy Compliance: Results of a Multigroup Analysis. *Information & Management*, *58*(3), 103318. https://doi.org/10.1177/14624745211068870

Kapoor, M. (2024). Comparative Analysis of AI Algorithms for Enhancing Phishing Detection in Real-Time Email Security. *Aitoz Multidisciplinary Review*, *3*(1), 338–352.

Khan, A. W., Saeed, S., & Kakar, M. S. (2024). Cybersecurity as a Geopolitical Tool: The Growing Influence of Digital Warfare in Statecraft. *International Research Journal of Social Sciences and Humanities*, *3*(2), 345–357. Retrieved from https://irjssh.com/index.php/irjssh/article/view/209

Khanna, A. (2024). Ransomware Prevention. In *Securing An Enterprise* (Bll 119–138). Apress. https://doi.org/10.1007/979-8-8688-1029-9_7

Kintonova, A., Vasyaev, A., & Shestak, V. (2021). Cyberbullying and Cyber-Mobbing in Developing Countries. *Information & Computer Security*, *29*(3), 435–456. https://doi.org/10.1108/ics-02-2020-0031

Kovaitė, K., Šūmakaris, P., & Stankevičienė, J. (2020). Digital Communication Channels in Industry 4.0 Implementation. *Management*, *25*(1), 171–191. https://doi.org/10.30924/mjcmi.25.1.10

Kulkarni, S., & Girish, G. N. (2024). Navigating The Abyss–Illuminating Data Leakage Threats, Mitigations, and Future Horizons. In *Cloud Security* (Bll 37–51). Chapman And Hall/Crc.

Leo, M., Sharma, S., & Maddulety, K. (2019). Machine Learning in Banking Risk Management: A Literature Review. *Risks*, *7*(1), 29. https://doi.org/10.3390/risks7010029

Li, H., Ge, D., Liu, S., Zhang, W., Wang, J., Si, J., & Zhai, J. (2019). Baduanjin Exercise for Low Back Pain: A Systematic Review and Meta-Analysis. In *Complementary Therapies In Medicine*. https://doi.org/10.1016/j.ctim.2019.01.021

Liesnaia, Y., & Malakhov, S. (2023). The Analysis of Development, Typical Objectives and Mechanisms of Phishing Attacks. *Computer Science and Cybersecurity*, *1*, 6–27. https://doi.org/10.26565/2519-2310-2023-1-01

Liu, S., & Kuhn, R. (2010). Data Loss Prevention. *It Professional*, *12*(2), 10–13. https://doi.org/10.1109/mitp.2010.52

Mansikka, J. (2023). *Data Loss Prevention: For Securing Enterprise Data Integrity*. Retrieved from https://urn.fi/urn:nbn:fi:amk-2023101827711

Marcillo-Delgado, J. C., Alvarez-Garcia, A., & García-Carrillo, A. (2022). Communication Strategies on Risk and Disaster Management in South American Countries. *International Journal of Disaster Risk Reduction*, *76*, 102982. https://doi.org/10.1016/j.ijdrr.2022.102982

Marques, L. (2024). *Enhancing Data Breach Prevention Measures in Corporate Setting*. Retrieved form https://repository.stcloudstate.edu/msia_etds/144

Moore, J. (2024). *Keeping up with the NIST CyberSecurity Framework*. Retrieved from https://medium.com/@jefferywmoore/keeping-up-with-the-nist-cybersecurity-framework-3ff9fd983cc9

Nayak, A., Patnaik, A., Satpathy, I., & Patnaik, B. C. M. (2024). Data Storage and Transmission Security in the Cloud. *Indian Journal of Cryptography and Network Security*, *2*(2), 194–212. https://doi.org/10.4018/979-8-3693-1431-9.ch009

Omodara, H. (2022). *Cloud Security: A Survey of Information Communication Technology (ICT) and Cybersecurity Professionals' Perception on Data Loss Prevention (DLP) Measures for Software-as-a-Service (SaaS) Application-Related Data Breaches and Leakage*. Retrieved from https://www.academia.edu/88587761/Cloud_Security_A_survey_of_Information_Communication_Technology_ICT_and_Cybersecurity

Omotunde, H., & Ahmed, M. (2023). A Comprehensive

Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. *Mesopotamian Journal of Cybersecurity*, *2023*, 115–133. http://dx.doi.org/10.58496/MJCSC/2023/016

Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction. *Nanotechnology Perceptions*, *20*, 332–353.

Saunders, A., Cornett, M. M., & Erhemjamts, O. (2021). *Financial Institutions Management: A Risk Management Approach*. Mcgraw-Hill.

Senapati, K. K., Kumar, A., & Sinha, K. (2023). Impact of Information Leakage and Conserving Digital Privacy. In *Malware Analysis and Intrusion Detection in Cyber-Physical Systems* (Bll 166–188). Igi Global. https://doi.org/10.4018/978-1-6684-8666-5.ch008

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Shishodia, B. S., & Nene, M. J. (2022). Data Leakage Prevention System for Internal Security. *2022 International Conference on Futuristic Technologies (INCOFT)*, 1–6. https://doi.org/10.1109/incoft55651.2022.10094509

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing Human Phishing Difficulty: A Phish Scale. *Journal of Cybersecurity*, *6*(1), 1–16. https://doi.org/10.1093/cybsec/tyaa009

Syarova, S., Toleva-Stoimenova, S., Kirkov, A., Petkov, S., & Traykov, K. (2024). Data Leakage Prevention and Detection in Digital Configurations: A Survey. *Environment, Technologies, Resources, Proceedings of The International Scientific and Practical Conference*, *2*, 253–258. https://doi.org/10.17770/etr2024vol2.8045

Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Enhancing Cloud Security. In *Improving Security, Privacy, and Trust in Cloud Computing* (Bll 85–112). Igi Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-1431-9.ch004

Wang, C., Cheng, Z., Yue, X.-G., & Mcaleer, M. (2020). Risk Management of Covid-19 by Universities in China. *Journal of Risk and Financial Management*, *13*(2), 36. https://doi.org/10.3390/jrfm13020036

Wendy, W. (2024). The Nexus between Financial Literacy, Risk Perception and Investment Decisions: Evidence from Indonesian Investors. *Investment Management & Financial Innovations*, *21*(3), 135-147. http://dx.doi.org/10.21511/imfi.21(3).2024.12

Wiranata, G. A., Ucuk, Y., Subekti, S., & Sidarta, D. D. (2024). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Phishing. *Court Review: Jurnal Penelitian Hukum (E-Issn: 2776-1916)*, *4*(02), 13–25. https://doi.org/10.69957/cr.v4i02.1503

Yadav, I., & Gupta, H. (2023). Designing Data Loss Prevention System for the Enhancement of Data Integrity in Cyberspace. *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 1361–1365. https://doi.org/10.1109/ICAC3N60023.2023.10541823