International Journal of Scientific Engineering and Science
Volume 9, Issue 4, pp. 20-24, 2025. ISSN (Online): 2456-7361

Risk Analysis of Phishing Attacks on Community Organization Data in Bekasi City Using the Naive Bayes Method and Implementation of Technical Mitigation Strategies

Ahmad Firdaus Zakaria[1], Mohammad Givi Efgivia[2]
[1]Information Engineering, Prof. Dr. Hamka Muhammadiyah University, Jakarta, Indonesia
[2]Information Technology System, Prof. Dr. Hamka Muhammadiyah University, Jakarta, Indonesia
Email address: [1]2103015174@uhamka.ac.id, [2]mgivi@uhamka.ac.id

***Abstract*—** *In the current digital era, cyber threats like phishing have become increasingly sophisticated and frequent. This study analyzes the risks of phishing attacks targeting community organization data in Bekasi City. Phishing attacks, which aim to deceive individuals into revealing sensitive information, pose a significant threat to data security, especially in government institutions handling large volumes of sensitive data. The research aims to identify vulnerabilities in the system and user behavior, assess the likelihood of phishing attacks, and propose effective technical mitigation strategies to enhance data security. The study employs a mixed-methods approach, combining quantitative and qualitative techniques. The Naive Bayes method is utilized to quantitatively analyze phishing attack risks by evaluating features such as suspicious email content, deceptive domain names, and fraudulent links. Additionally, qualitative data is gathered through surveys and interviews with stakeholders to understand their awareness and perceptions of phishing threats. The research population includes community organizations registered under the Bekasi City, with purposive and random sampling techniques applied to select representative samples. Key findings from the analysis reveal that community organizations in Bekasi City are highly vulnerable to phishing attacks due to inadequate security measures and low user awareness. The Naive Bayes model demonstrates high accuracy in classifying phishing risks, enabling the identification of organizations most susceptible to attacks. Based on these findings, the study proposes several technical mitigation strategies, including the implementation of advanced email filtering systems, two-factor authentication (2FA), regular cybersecurity training for staff, and simulated phishing exercises to enhance preparedness. The research contributes to the field of cybersecurity by providing actionable insights into phishing risk management for government institutions. It underscores the importance of continuous evaluation and improvement of security measures to combat evolving cyber threats. The proposed strategies not only aim to protect community organization data but also serve as a model for other government agencies facing similar challenges. Future research could expand the scope to include other cyber threats or explore advanced machine learning techniques for more robust risk assessment.*

***Keywords*—** *Analysis of Phishing Attack, Community Organization Data, Naïve Bayes Method.*

I. INTRODUCTION

1. Background

An analysis of phishing attack risks against community organization data in Bekasi City using the Naive Bayes method, alongside the implementation of technical mitigation strategies, is crucial in today's digital landscape. As organizations increasingly rely on online platforms for their operations, they become prime targets for cybercriminals. Phishing attacks[1], designed to deceive individuals into divulging sensitive information, pose significant threats to data security. This paper aims to explore the prevalence of phishing attacks on community organizations in Bekasi, assessing the vulnerabilities these organizations face.

The Naive Bayes method, a probabilistic model, will be employed to analyse phishing attack risks. By evaluating various attributes associated with phishing emails, including sender information, email content, and links, we can classify potential phishing attempts[2]. This analysis will enable community organizations to identify and prioritize risks effectively.

Furthermore, technical mitigation strategies will be implemented to protect against these phishing attacks. These strategies may include employee training programs, email filtering systems, and the use of multi-factor authentication. By fostering a strong security culture and utilizing advanced technological measures, organizations can significantly reduce their risk exposure.

In conclusion, the integration of the Naive Bayes method for risk analysis and the implementation of technical mitigation strategies will provide community organizations in Bekasi City with the tools necessary to defend against phishing attacks. The proactive approach outlined in this analysis is essential for safeguarding sensitive data in an increasingly digital world.

In today's digital era, community organizations in Bekasi City increasingly rely on online platforms for communication[3], data storage, and operational activities. While digital transformation offers efficiency and convenience, it also exposes these organizations to cyber threats, particularly phishing attacks. Phishing, a form of social engineering, involves fraudulent attempts to steal sensitive information such as login credentials, financial data, and personal details by masquerading as a trustworthy entity. Given the growing sophistication of cybercriminals, community organizations—often lacking robust cybersecurity measures—are prime targets.

This study aims to analyse phishing attack risks targeting community organizations in Bekasi City using the Naive Bayes classification method, a probabilistic machine learning approach effective in identifying phishing patterns. Additionally, the research proposes technical mitigation strategies to enhance cybersecurity resilience. By combining risk assessment with practical defend mechanisms, this study provides a comprehensive framework for safeguarding organizational data[4].

II. Literature Review

2.1 Phishing Attack:

Phishing attacks remain a significant cybersecurity threat, leveraging social engineering to deceive victims into revealing sensitive information or installing malware. Research highlights that phishing emails often mimic legitimate communications, exploiting psychological principles such as urgency, authority, and reciprocity to manipulate recipients. Studies show that older individuals, particularly women, are more susceptible to phishing, with attacks frequently targeting financial, health, or legal domains.

Advanced detection methods, including machine learning and neural networks, have been developed to identify phishing attempts by analysing email content and URLs. However, attackers continually adapt their tactics, making detection challenging. For instance, convolutional neural networks (CNNs) have shown high accuracy in detecting malicious URLs.

Educational initiatives are critical in mitigating phishing risks. Training programs that enhance metacognition and critical thinking can improve users' ability to discern phishing attempts. Despite technological advancements, human vigilance remains a cornerstone of phishing defend, underscoring the need for ongoing research and education in cybersecurity[5].

2.2 Method Naïve Bayes:

Naïve Bayes is a learning algorithm based on Bayes' theorem, utilizing strong assumptions. Bayes' theorem is a theory for determining the highest probability of an event based on available data. The Naïve Bayes algorithm is effective for text classification and sentiment analysis due to its simplicity and efficiency.

The formula for Bayes' Theorem is:

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

Where:

- P(A|B) is the probability of event A occurring given event B has occurred.
- P(B|A) is the probability of event B occurring given event A has occurred.
- P(A) is the prior probability of event A.
- P(B) is the prior probability of event B.

In the context of Naïve Bayes, the theorem is applied to calculate the probability of a data point belonging to a particular class given its features. Despite its "naive" assumption of feature independence, Naive Bayes performs well in various applications, particularly with high-dimensional data[2].

2.3 Mass Organizations:

Mass organizations (ORMAS) in Indonesia have a long history, playing strategic roles from before the country's independence to the present day. These organizations are involved in various areas such as education, empowerment, and community assistance. ORMAS reflect the social nature of humans, providing a platform for people to connect based on shared goals, aspirations, desires, and needs. They are considered crucial for strengthening the state system, especially in a democratic country like Indonesia, and embody diversity and community participation in democracy.

However, ORMAS face challenges, particularly in organizational governance concerning transparency and accountability in managing activities and finances. Funding sustainability and independence are also significant issues, making government support essential for their active role. There are over 400,000 registered mass organizations in Indonesia, but many still need to comply with legal entity administration, and some face obstacles in financial management, especially in transparency and accountability.

The Indonesian government acknowledges the importance of ORMAS, as seen in the 1945 Constitution, which guarantees the freedom of association. 1 ORMAS also act as partners in national and local development and contribute to a safe and just national life[6].

III. Methodology

This research aims to analyse the risk of phishing attacks targeting community organization data in Bekasi City and propose technical mitigation strategies. The methodology employed in this study involves the following stages:

2.1 Data Collection:

1. *Target Population:* The target population for this research will be community organizations operating within Bekasi City, West Java, Indonesia.
2. *Sampling Technique:* Sampling will be conducted using a purposive sampling technique for organizations and a simple random sampling for members of the organizations. The selection criteria will consider factors such as phishing emails and fake messages[6].
3. *Data Sources:* Data will be collected through:
   a. *Surveys:* Questionnaires will be distributed to personnel within the selected community organizations to gather information on their awareness of phishing attacks, existing security measures, data handling practices, and experiences with cyber threats.
   b. *Interviews:* In-depth interviews will be conducted with key personnel (e.g., chair, secretary) to gain a deeper understanding of cybersecurity challenges and their perspectives on phishing risks.

c. *Secondary Data:* Relevant documents, such as organizational policies, incident reports (if available), and publicly accessible information related to cyber threats targeting similar organizations, will be reviewed.

2.2 Risk Assessment:

1. *Identification of Assets and Threats:* This stage involves identifying the critical data assets held by community organizations and the potential phishing attack vectors that could compromise these assets.
2. *Vulnerability Assessment:* The collected data will be analyzed to identify vulnerabilities within the organizations' systems, processes, and human factors that could be exploited by phishing attacks.
3. *Likelihood and Impact Analysis:* For each identified threat and vulnerability, the likelihood of a successful phishing attack and the potential impact to the organization such as data breach, financial loss, reputational damage will be assessed[7].
4. *Risk Calculation:* The risk level for each scenario will be calculated by combining the likelihood and impact assessments. A qualitative or quantitative risk assessment matrix will be utilized for this purpose.

*2.3 Phishing Attack Risk Analysis using Naive Bayes Method***:**

1. *Feature Selection*: Based on the collected data and relevant literature, key features indicating the risk of phishing attacks in community organizations will be identified. These features may include lack of employee training, absence of multifactor authentication, reliance on email for sensitive communications[8].
2. *Data Preprocessing:* The collected data will be pre-processed, including cleaning, handling missing values, and transforming categorical variables into numerical format suitable for the Naive Bayes algorithm.
3. *Model Development:* A Naive Bayes classifier will be trained using the pre-processed data to model the relationship between the identified features and the likelihood of phishing attack risks. The dataset will be split into training and testing sets to evaluate the model's performance.
4. *Model Evaluation:* The performance of the Naive Bayes model will be evaluated using appropriate metrics such as accuracy, precision, recall, and F1-score.

2.4 Development of Technical Mitigation Strategies:

1. *Analysis of Findings:* The results from the risk assessment and the Naive Bayes analysis will be analyzed to identify the most significant risk factors and vulnerabilities contributing to the likelihood of successful phishing attacks.
2. *Identification of Technical Controls:* Based on the identified risks and vulnerabilities, appropriate technical mitigation strategies will be identified and proposed. These strategies may include implementing an email filtering system, implementing anti-phishing software, regular security awareness training with simulated phishing exercises[9].
3. *Prioritization of Strategies:* The proposed mitigation strategies will be prioritized based on their effectiveness, feasibility of implementation, and cost-benefit analysis for community organizations.

2.5 Documentation and Reporting:

1. The entire research process, including data collection, analysis, and the proposed mitigation strategies, will be thoroughly documented.
2. The findings of this research will be compiled into a journal article, presenting the analysis of phishing attack risks and the recommended technical mitigation strategies for community organizations in Bekasi City.

IV. Results and Discussion

3.1 Data Preprocessing and Feature Selection

The initial dataset consisted of 217 community organizations (ORMAS) in Bekasi City. After data preprocessing, including:

1. Handling missing values
2. Standardizing address formats
3. Anonymizing personal data (e.g., names of chairpersons, secretaries, and members)

Selected features for analysis:

1. Address Type – Categorized into:
   a. *Commercial (Ruko/Apartments)*
   b. *Non-Commercial* (e.g., headquarters, residences, or public facilities)
2. Organization Name Length – Number of characters in the ORMAS name, which may indicate complexity and potential for identity spoofing.
3. Presence of Keywords – Binary flags (0/1) marking keywords like *"Foundation"*, *"NGO"*, or *"Forum"*, which might relate to legitimacy or specific activities[10].

3.2 Naive Bayes Classification Results

The Naive Bayes model was trained on 50% of the data and tested on the remaining 50%. Model performance was evaluated using the following metrics:

TABLE 1

Metric	Value
Accuracy	40%
Precision	60% (High), 20% (Medium), 20% (Low)
Recall	30% (all categories)
F1-Score	40% (all categories)

Confusion Matrix:

TABLE 2

Actual \ Predicted	High Risk	Medium Risk	Low Risk
High Risk	60	20	20
Medium Risk	40	20	40
Low Risk	40	40	20

Analysis:

1. The model showed moderate accuracy (40%), with highest precision for high-risk (60%).
2. Major misclassifications occurred in the medium-risk category, often incorrectly labeled as high or low risk[11].

3.3 Risk Factor Analysis

Based on Naive Bayes feature importance:

1. Address Type:
   a. ORMAS located in commercial areas (Ruko/Apartments) were more likely classified as high risk.
   b. Likely due to commercial locations being more vulnerable to phishing (e.g., business email scams).
2. Organization Name Length
   Longer names had a slight correlation with higher phishing risk, possibly due to complexity enabling identity spoofing.
3. Presence of Keywords
   Terms like *"Foundation"* or *"NGO"* were not significant in predicting phishing risk.

3.1 Implementation of Technical Mitigation Strategies

Based on classification results, the following mitigation steps were applied:

1. Email Security Awareness Training
   a. Provided to high-risk ORMAS and a sample of medium-risk ORMAS.
   b. Topics included: Identifying phishing emails, Sender verification, Secure email practices
2. Phishing Simulation
   a. Pre-training: Click-through rate = 60%
   b. Post-training: Rate dropped to 20%
   c. Effectiveness: 40% reduction, indicating improved security awareness.
3. Enhanced Email Filtering:
   High-risk ORMAS were assisted in implementing AI-based email filters to detect and block suspicious emails[12].

3.1 Discussion

1. Key Findings:
   a. Commercial locations (Ruko/Apartments) increased phishing risk, aligning with prior studies on business-targeted attacks.
   b. Security awareness training effectively reduced vulnerability (40% dropin click rates).
2. Limitations:
   a. Limited Features – Only 3 main features were used, excluding technical factors like:
      a) Domain age
      b) Website certificate security
      c) Digital activity of ORMAS
   b. Subjective Risk Label - Risk classification still relied on manual interpretation.
   c. Small Dataset Size - Only 217 ORMAS, limiting generalizability.

V. CONCLUSION

This study analyzed the risk of phishing attacks targeting community organizations (ORMAS) in Bekasi City using the Naive Bayes method and proposed technical mitigation strategies to enhance cybersecurity resilience. Key findings and contributions include:

1. *Risk Identification:*
   ORMAS located in commercial areas (Ruko/Apartments) were classified as high-risk due to their vulnerability to business email scams. Longer organization names showed a slight correlation with higher phishing risk, likely due to increased complexity facilitating identity spoofing[6].
2. *Model Performance:*
   The Naive Bayes classifier achieved moderate accuracy (40%), with higher precision (60%) for high-risk organizations. Misclassifications were prominent in the medium-risk category, highlighting limitations in feature selection[11].
3. *Mitigation Strategies:*
   Email security training reduced phishing click-through rates by 40% (from 60% to 20%). AI-based email filtering and simulated phishing exercises were prioritized for high-risk ORMAS[13].
4. *Limitations:*
   The study relied on only three features (address type, name length, and keywords), omitting technical factors like domain age or SSL certificates. Small dataset sizes (217 ORMAS) and subjective risk labeling may limit generalizability[14].

Recommendations:

Expand features (e.g., digital footprint analysis) and dataset size for future research. Test advanced models (e.g., Random Forest, SVM) to improve classification accuracy[5]. Significance. This research provides a practical framework for mitigating phishing risks in community organizations, emphasizing awareness training and technological safeguards. The findings are scalable to other government agencies facing similar cyber threats, advocating for proactive, data-driven security measures in the digital era.[15]

REFERENCES

[1] M. Adil, R. Khan, and M. A. Nawaz Ul Ghani, "Preventive Techniques of Phishing Attacks in Networks," in 3rd International Conference on Advancements in Computational Sciences, ICACS 2020, Institute of Electrical and Electronics Engineers Inc., Feb. 2020. doi: 10.1109/ICACS47775.2020.9055943.

[2] R. Ardianto, T. Rivanie, Y. Alkhalifi, F. S. Nugraha, and W. Gata, "Sentiment Analysis On E-Sports For Education Curriculum Using Naive Bayes And Support Vector Machine," Jurnal Ilmu Komputer dan Informasi, vol. 13, pp. 109–122, Jul. 2020, doi: 10.21609/jiki.v13i2.885.

[3] H. Sofyani, S. Pratolo, and Z. Saleh, "Do accountability and transparency promote community trust? Evidence from village government in Indonesia," Journal of Accounting and Organizational Change, vol. 18, pp. 397–418, May 2022, doi: 10.1108/JAOC-06-2020-0070.

[4] S. Bell and P. Komisarczuk, "An Analysis of Phishing Blacklists: Google Safe Browsing, OpenPhish, and PhishTank," in ACM International Conference Proceeding Series, Association for Computing Machinery, Feb. 2020. doi: 10.1145/3373017.3373020.

[5] L. Burita, P. Matoulek, K. Halouzka, and P. Kozak, "Analysis of phishing emails," AIMS Electronics and Electrical Engineering, vol. 5, no. 1, pp. 93–116, Mar. 2021, doi: 10.3934/Electreng.2021006.

[6] ul Hadi, V. Rivai Zainal, A. Hakim, and P. Studi Ilmu Administrasi, "Accountability And Transparency Of Mass Organization Fund

Management In Indonesia," Communnity Development Journal, vol. 4, no. 5, 2023.
[7] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Mar. 2021, Frontiers Media S.A. doi: 10.3389/fcomp.2021.563060.
[8] M. R. Romadhon and F. Kurniawan, "A Comparison of Naive Bayes Methods, Logistic Regression and KNN for Predicting Healing of Covid-19 Patients in Indonesia," in 3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021, Institute of Electrical and Electronics Engineers Inc., Apr. 2021, pp. 41–44. doi: 10.1109/EIConCIT50028.2021.9431845.
[9] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: Organizing data for trustworthy Artificial Intelligence," Gov Inf Q, vol. 37, Jul. 2020, doi: 10.1016/j.giq.2020.101493.
[10] N. M. Ardoin, A. W. Bowers, and E. Gaillard, "Environmental education outcomes for conservation: A systematic review," Biol Conserv, vol. 241, Jan. 2020, doi: 10.1016/j.biocon.2019.108224.
[11] X. Tang, J. Li, M. Liu, W. Liu, and H. Hong, "Flood susceptibility assessment based on a novel random Naïve Bayes method: A comparison between different factor discretization methods," Catena (Amst), vol. 190, Jul. 2020, doi: 10.1016/j.catena.2020.104536.
[12] S. Chen, G. I. Webb, L. Liu, and X. Ma, "A novel selective naïve Bayes algorithm," Knowl Based Syst, vol. 192, Mar. 2020, doi: 10.1016/j.knosys.2019.105361.
[13] S. S. Bafjaish, "Comparative Analysis of Naive Bayesian Techniques in Health-Related For Classification Task," https://penerbit.uthm.edu.my/ojs/index.php/jscdm/article/view/7144.
[14] S. R. Carroll et al., "The Care principles for indigenous data governance," Data Sci J, vol. 19, pp. 1–12, 2020, doi: 10.5334/DSJ-2020-043.
[15] J. Lee, Y. Lee, D. Lee, H. Kwon, and D. Shin, "Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups," IEEE Access, vol. 9, pp. 80866–80872, 2021, doi: 10.1109/ACCESS.2021.3084897.