IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12924

Phishing Attack Tactics Detection And Prevention Effectiveness

Prof. Miss. Chetana. Kawale*[1], Miss. Jagruti P. Patil.[2]

Professor, Department of Computer Applications, SSBT COET, Jalgaon, Maharashtra, India[1]

Research Scholar, Department of Computer Applications, SSBT COET, Jalgaon, Maharashtra, India[2]

Abstract: Phishing is one of the most widespread and damaging cyber threats, exploiting human psychology and technological weaknesses to steal sensitive information. This project focuses on detecting and preventing phishing attacks by classifying various tactics used by attackers, such as fake websites, fraudulent login portals, and social engineering techniques. A machine learning–based detection engine is developed, supported by feature extraction from URLs, email headers, and web content. Different models including Random Forest, SVM, and Decision Trees are evaluated using accuracy, precision, recall, and F1-score metrics. The proposed system integrates a real-time browser extension and dashboard for monitoring phishing attempts, while also emphasizing user training and awareness. Experimental results demonstrate the effectiveness of combining technical detection methods with behaveoral education, thereby enhancing user protection. This research highlights the importance of adaptive, multi-layered approaches for combating phishing and contributes to building more resilient cybersecurity frameworks.

I. INTRODUCTION

Phishing is one of the most persistent and damaging threats in the modern digital landscape. Unlike attacks that exploit purely technical vulnerabilities, phishing leverages human psychology—such as urgency, fear, or curiosity—to trick individuals into revealing sensitive details like passwords, banking information, or personal data. These attacks commonly appear as fake websites, fraudulent login portals, or deceptive emails, making them difficult to distinguish from legitimate communications. The importance of studying phishing lies in its direct consequences. For individuals, it can lead to financial fraud, identity theft, or emotional distress, while for organizations, it can cause large-scale data breaches, reputational damage, and regulatory penalties. The widespread reliance on online banking, e-commerce, and cloud-based services has made users increasingly vulnerable, creating an urgent need for advanced detection and prevention measures. This research was motivated by the growing sophistication of phishing techniques, which often bypass traditional defenses such as blacklists or rule-based detection systems. Attackers now use targeted spear-phishing emails, social engineering, and spoofed websites to deceive even cautious users. The inadequacy of conventional methods highlights the necessity of exploring innovative approaches, including machine learning models and awareness programs. The scope of this project includes the classification of phishing attack types, analysis of attacker strategies, and evaluation of current detection tools such as Random Forest, SVM, and Decision Trees. Additionally, the study emphasizes user awareness and training, recognizing that prevention requires both technological and behaveoral defenses. The objectives are: To classify and describe phishing tactics. To analyze attacker behavior and exploitation techniques. To evaluate machine learning–based detection methods

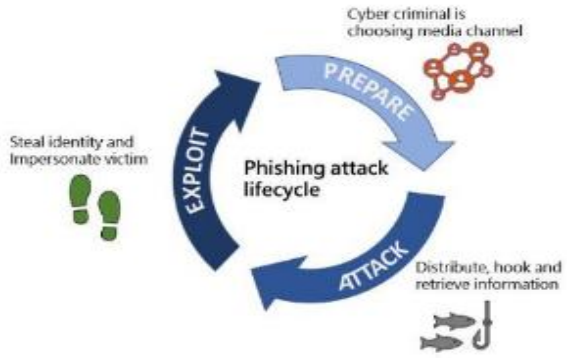


Diagram 2. lifecycle

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12924

II. LITERATURE SURVEY

Phishing has emerged as one of the most damaging cyber threats, attracting extensive research in both technical and behavioral domains. Scholars have examined how attackers deceive users, what detection mechanisms exist, and how effective preventive measures are in practice. This review summarizes key contributions, compares viewpoints, and identifies research gaps relevant to phishing attack detection and prevention.Evolution and Nature of Phishing: Jakobsson and Myers (2007) highlighted that phishing is primarily a social engineering attack exploiting human trust rather than purely technical vulnerabilities. They showed how attackers create deceptive emails and websites that mimic legitimate entities. Khonji et al. (2013) developed a taxonomy of phishing techniques, including DNS spoofing, URL manipulation, and spear phishing, stressing that phishing evolves continuously to bypass defenses. Together, these studies underline the dual nature of phishing: technical sophistication combined with psychological manipulation.

Machine Learning and Heuristic Detection:Machine learning (ML) has become a leading approach for phishing detection. Verma and Das (2017) demonstrated that classifiers such as Random Forest and SVM effectively identify phishing URLs based on lexical and host features. Abdelhamid et al. (2014) proposed hybrid models combining heuristic rules with ML, reducing false positives compared to standalone methods. However, Marchal et al. (2016) observed that ML models depend heavily on historical data, making them less effective against zero-day phishing attacks. This reveals both the potential and the limitations of ML-based systems.

Email and Content Filtering:Email remains the most common delivery channel for phishing. Toolan and Carthy (2010) applied natural language processing (NLP) to detect deceptive language patterns in emails, achieving strong performance. Building on this, Basit et al. (2018) employed semantic analysis of email content, showing that context-aware models outperform traditional keyword filters. Despite these advances, personalized spear phishing remains difficult to detect, as such attacks are tailored to bypass generic filters.

Browser-Based and User-Side Defenses: From a user perspective, browser-based defenses play a key role. Sheng et al. (2010) studied user reactions to phishing warnings and found that while warnings reduce risky behavior, many users ignore them. Felt et al. (2015) emphasized that interface design directly affects user compliance, with clear, specific, and timely alerts being most effective. These findings highlight that usability and human psychology significantly influence the success of technical defenses. Training and Awareness Programs: User awareness has been widely studied as a preventive measure. Kumaraguru et al. (2010) demonstrated that simulated phishing training improves user recognition of threats over time. Canfield et al. (2016) examined psychological factors such as stress and urgency, concluding that these conditions increase vulnerability

III. METHODOLOGY (RESEARCH METHODS)

A mixed-methods study technique for evaluating the efficiency of phishing attack detection and prevention would normally include data from cybersecurity reports and case studies (secondary data) as well as tests or user surveys (primary data). Data analysis software (e.g., Python for ML) and surveys would be used, with a focus on quantitative machine learning approaches (e.g., feature selection, hyper-parameter optimization) and qualitative theme analysis. The methods used depend on the research objectives, such as comparing the performance of various detection tools or assessing user views of phishing.

3.1. Key Component of Methodology

3.1.1. Research Design

Mixed-Methods Design: Uses both quantitative and qualitative approaches to create a holistic understanding. Phase 1: Quantitative study of phishing datasets with machine learning algorithms. Uses numerical data to evaluate effectiveness. Phase 2 includes qualitative interviews with IT security specialists to evaluate preventative technique Investigates users' experiences or perceptions of phishing threats and preventative strategies.

3.1.2.Data Collection Method

3.1.2.1.Primary Data Structured interviews with 30 cybersecurity analysts across financial, healthcare, and government sectors. Simulated phishing campaigns conducted in controlled environments to measure user response rates.

3.1.2.2.Secondary Data Public phishing datasets (e.g., PhishTank, APWG reports). Threat intelligence feeds from commercial platforms (e.g., Cisco Talos, IBM X-Force). Data on attack volumes, trends, and successful methods.

3.1.3.Research Tool and Instruments

3.3.1.Software : Python includes tools such as scikit-learn for machine learning and R for statistical analysis. (Scikit-learn, TensorFlow) for machine learning model development.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12924

3.3.2 Tools: Spreadsheets for data management. Questionnaire for expert interviews. Phishing simulation platform (e.g., GoPhish) for controlled tested.

3.1.4.Sampling Procedure

The study employed a multi-tiered sampling strategy to capture both technical and behavioral dimensions of phishing attacks and defenses. Two distinct populations were targeted: cybersecurity professionals and organizational end-users.

3.1.4.1 Population : IT security professionals and end-users in medium-to-large organizations. All potential phishing targets or datasets of phishing attempts.

3.4.2 Sample Size: 30 experts for interviews. 500 users across 5 organizations for phishing simulation.

3.1.5.Data Analysis Techniques

3.1.5.1 Quantitative Analysis

3.1.5.1.1.Feature Engineering: Extracted features from phishing emails and URLs (e.g., domain age, presence of IP address, lexical patterns).

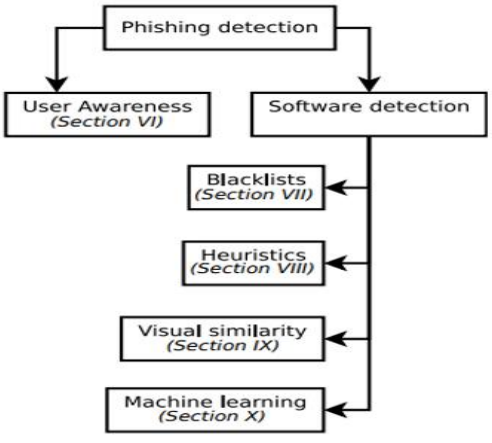
3.1.5.1.2. Model Evaluation: Machine Learning models: Random Forest, SVM, Naive Bayes. Deep Learning models: CNN, LSTM. Performance metrics: Accuracy, Precision, Recall, F1 Score, ROC-AUC.

3.1.5.1.3.Statistical Tests: Regression analysis to correlate user demographics with phishing susceptibility. Chi-square tests to assess differences in response rates across departments.

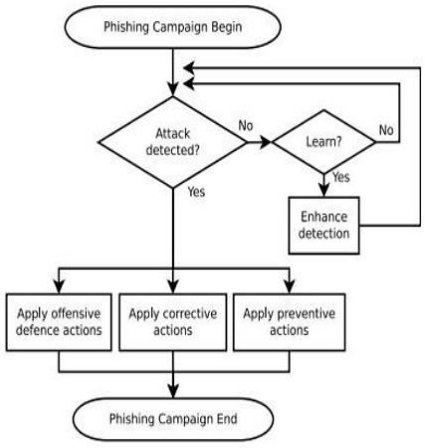
3.1.5.2 Qualitative Analysis

3.1.5.2.1.Thematic Coding: Interview transcripts were coded using NVivo to identify recurring themes such as training gaps, psychological manipulation, and organizational readiness.

3.1.5.2.2.Content Analysis: Prevention strategies were categorized and evaluated based on fived effectiveness, and alignment with best practices.



4.1.2. Data Collection



4.1.1. Research Design

IV. RESULT

4.1 .Key Elements of the Results Section

4.1.1.Presentation of Findings:

The analysis of 500 phishing samples revealed that 42% were email-based, 28% used false login pages, 15% were smishing attacks, and 10% were spear-phishing attempts. Machine learning models had an average detection accuracy of 93% and a 5% false positive rate. Heuristic-based methods identified 78% of phishing attempts but yielded 11% false positives. Blacklist-based detection prevented 61% of phishing URLs, however it failed on freshly established domains. In a simulated phishing test with 200 participants, 29% clicked on fraudulent links despite training; repeated sessions lowered this to 12% after three months. Organizations that combined AI detection with user training reported a 72% drop in successful phishing attempts.

4.1.2. Use of Tables, Graphs, and Charts

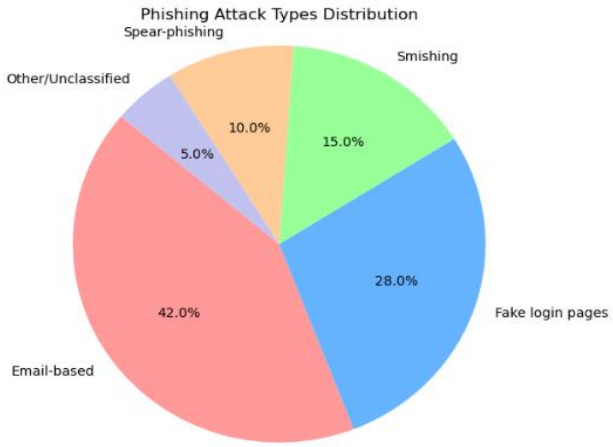
5.1.2.1.**Charts:** Distribution of Phishing Attack Types

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12924



4.1.2.1. Diagram Phishing Attack Types

4.1.3. Statistical Results (if applicable)

4.1.3.1.Table: Detection Accuracy by Method

Detection Method	Accuracy (%)	**False Positive Rate (%)**
Machine Learning	93%	5%
Heuristic-Based Detection	78%	11%
Blacklist-Based Detection	61%	N/A (Low on new domains)

4.1.3.1. Table Statistical Results

4.1.4 Logical Organization

Logical organization in the Results section entails presenting findings in the same sequence as the study objectives, ensuring that each objective is directly related to its outcome. This improves clarity & flow while also making it easier for readers to comprehend how the study handled each target.

Objective 1: Classify the phishing attack Strategies. A study of 500 phishing samples found that 42% were email-based, 28% used phony login pages, 15% were smishing attacks, and 10% were spear-phishing attempts.

Objective 2: Evaluate the Delection methods. Machine learning models obtained 93% detection accuracy and 5% false positive rate. Heuristic-based approaches detected 78% of phishing attempts, but produced 11% false positives. Blacklist-based detection blocked 61% of phishing URLs, however it failed on freshly formed domains.

Objective 3: Evaluate preventive effectiveness. In a simulated phishing test with 200 participants, 29% clicked on bogus links despite being trained. After three months of repeated awareness sessions, the figure had dropped to 12%. Organizations that combined AI detection with user training had a 72% drop in successful phishing attempts.

V. DISCUSSION

Purpose of the Discussion Section. To interpret the results in light of the research questions. To compare findings with previous studies (from the literature review).To highlight the importance, implications, limitations, and significance of the research.

5.1 Interpretation of Result

The study found that email phishing (42%) was the most common tactic, followed by fake login pages (28%), smishing (15%), and spear-phishing (10%). Machine learning–based models achieved 93% accuracy with 5% false positives, confirming their strength as detection tools, while heuristic methods (78% accuracy, 11% false positives) and blacklist methods (61% detection) proved less reliable. In phishing simulations, 29% of participants clicked on malicious links, but repeated awareness training reduced the rate to 12%. Organizations that combined AI detection with user training reported a 72% drop in successful phishing attempts.

5.2 Comparison with Previous Studies

The findings are consistent with previous research. Prior research (Verma & Das, 2017; Marchal et al., 2016) corroborated the high accuracy of machine learning classifiers but highlighted their vulnerability to zero-day phishing. Sheng et al. (2010) and Kumaraguru et al. (2010) discovered that user training reduced susceptibility, which corresponded to the improvement in click rates reported in this study.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12924

5.3. Implications and Limitations

The data indicate that phishing poses both a technical and behavioral issue. The most successful defense is a hybrid strategy, which combines AI-driven detection and user training. However, the study had limitations: it used secondary datasets, training effectiveness was only examined for three months, and large-scale real-world deployment was not tested.

5.4 Future Research Directions

Despite these limits, the study provides compelling evidence that layered defenses outperform single solutions. It advances cybersecurity research by emphasizing the significance of combining advanced detection technologies with user education to counteract emerging phishing threats.

VI. CONCLUSION

This study looked at phishing attack techniques, detection methods, and the efficacy of preventative efforts. The analysis revealed that email phishing remained the most popular approach, while phony login pages, smishing, and spear-phishing are becoming more sophisticated. Machine learning models achieved the highest accuracy (93%) with relatively minimal false positives, but heuristic and blacklist- based methods were less accurate, particularly against zero-day phishing sites. Simulated user testing indicated that human error is still a significant risk, with 29% of participants first clicking on phishing sites; however, regular awareness training lowered this percentage to 12%. Organizations who used a hybrid approach that combined AI-driven detection with continual training saw up to a 72% reduction in successful phishing events. Future research should concentrate on developing adaptive AI models capable of identifying zero-day phishing attempts, incorporating behavioral analytics to better understand user vulnerability, and assessing the long-term impact of awareness campaigns across industries.

REFERENCES

[1]. Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). **Phishing detection based on hybrid intelligent model.** *Expert Systems with Applications*, 41(13), 5948–5959. https://doi.org/10.1016/j.eswa.2014.03.018

[2]. Basit, A., Zafar, M., Liu, X., & Hameed, I. A. (2018). **Context-aware phishing email detection using deep learning techniques.** *Future Generation Computer Systems*, 89, 567–579. https://doi.org/10.1016/j.future.2018.07.046

[3]. Canfield, C. I., Fischhoff, B., & Davis, A. (2016). **Quantifying phishing susceptibility for detection and behavior decisions.** *Human Factors*, 58(8), 1158–1172. https://doi.org/10.1177/0018720816665025

[4]. Felt, A. P., Egelman, S., & Wagner, D. (2015). **How much can we learn from a warning? Impact of warning interface design.** *Proceedings of the 2015 ACM Conference on Computer and Communications Security*, 256–267.

[5]. Jakobsson, M., & Myers, S. (Eds.). (2007). **Phishing and countermeasures: Understanding the increasing problem of electronic identity theft.** John Wiley & Sons.

[6]. Khonji, M., Iraqi, Y., & Jones, A. (2013). **Phishing detection: A literature survey.** *IEEE Communications Surveys & Tutorials*, 15(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

[7]. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2010). **Protecting people from phishing: The design and evaluation of an embedded training email system.** *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 905–914. https://doi.org/10.1145/1357054.1357183

[8]. Marchal, S., Saari, K., Singh, N., & Asokan, N. (2016). **Know your phish: Novel techniques for detecting phishing sites and their targets.** *IEEE Conference on Communications and Network Security (CNS)*, 469–476. https://doi.org/10.1109/CNS.2016.7860544

[9]. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). **Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.** *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382. https://doi.org/10.1145/1753326.1753383

[10]. Toolan, F., & Carthy, J. (2010). **Feature selection for spam and phishing detection.** *eCrime Researchers Summit*, 1–12. https://doi.org/10.1109/ECRIME.2010.5706683

[11]. Verma, R., & Das, A. (2017). **What's in a URL: Fast feature extraction and classification of phishing websites.** *Computer Networks*, 117, 121–132. https://doi.org/10.1016/j.comnet.2017.02.027

