ISSN: 2394-3122 (Online)
ISSN: 2394-6253 (Print)
Impact Factor: 6.03

Volume 12 Issue 11, November 2025

SK International Journal of Multidisciplinary Research Hub

Journal for all Subjects
e-ISJN: A4372-3088
p-ISJN: A4372-3089

Research Article / Survey Paper / Case Study
Published By: SK Publisher (www.skpublisher.com)

A Monthly Double-Blind Peer Reviewed Refereed Open Access Multidisciplinary & Multilingual International Journal - Included in the International Serial Directories

Phishing Attack Detection and Prevention in Cyber Security

Kalyani Raval[1]
Guide and Faculty,
Bachelor of Computer Application (B.C.A.),
M. J. College of Commerce,
Bhavnagar-364002, Gujarat, India

Pratik Arvindbhai Rathod[1]
Student,
Bachelor of Computer Application (B.C.A.),
M. J. College of Commerce,
Bhavnagar-364002, Gujarat, India

DOI: Available on author(s) request

Abstract: ***Cyber security has become a critical concern in the modern digital world. One of the most common and dangerous cyber threats is phishing attacks, where attackers deceive users into revealing sensitive information such as passwords, banking details, and personal data. This research focuses on understanding phishing attacks, their types, detection methods, and prevention techniques. The study highlights the importance of user awareness and basic security mechanisms to reduce phishing risks. The research concludes that a combination of technical solutions and cyber security awareness is the most effective approach to combat phishing attacks.***

Keywords: phishing attacks; security; detection methods;

I. INTRODUCTION

Cyber security refers to the protection of computer systems, networks, and data from cyber-attacks. With the rapid growth of internet usage, online banking, e-commerce, cloud computing, and social media, cyber threats have increased significantly. Attackers use various methods to exploit system vulnerabilities and human weaknesses.

Phishing attacks are among the most widely used cyber-attacks. In phishing, attackers impersonate legitimate organizations to trick users into providing confidential information. These attacks are often carried out through emails, fake websites, text messages, or social media platforms. Due to their simplicity and effectiveness, phishing attacks remain a major cyber security challenge up to 2025.

II. PROBLEM STATEMENT

Cyber security refers to the protection of computer systems, networks, and data from cyber-attacks. With the rapid growth of internet usage, online banking, e-commerce, cloud computing, and social media, cyber threats have increased significantly. Attackers use various methods to exploit system vulnerabilities and human weaknesses.

Phishing attacks are among the most widely used cyber attacks. In phishing, attackers impersonate legitimate organizations to trick users into providing confidential information. These attacks are often carried out through emails, fake websites, text messages, or social media platforms. Due to their simplicity and effectiveness, phishing attacks remain a major cyber security challenge up to 2025.

III. Objectives of the Study

The main objectives of this research are:

1. To understand the concept of phishing attacks
2. To study different types of phishing attacks
3. To analyze existing phishing detection methods
4. To explore prevention techniques
5. To suggest effective solutions to reduce phishing attacks

IV. Scope of the Study

This research focuses on common phishing attacks such as email phishing, website phishing, and social engineering-based attacks. The study is mainly theoretical and descriptive, making it suitable for beginners and certificate-level research projects.

V. Literature Review

Several studies have been conducted on phishing detection and prevention. Researchers have proposed various methods such as spam filtering, blacklist-based URL detection, and user awareness programs. Some studies also focus on machine learning-based phishing detection systems. However, these systems have limitations such as high false positives and the inability to detect new phishing techniques.

VI. Types of Phishing Attacks

- **Email Phishing:** Email phishing involves sending fake emails that appear to be from trusted organizations such as banks or companies.
- **Website Phishing:** Attackers create fake websites that look similar to legitimate websites to steal user credentials.
- **SMS Phishing (Smishing):** Phishing messages sent through SMS containing malicious links.
- **Social Media Phishing:** Fake profiles or messages on social media platforms to deceive users.

VII. Phishing Detection Techniques

Traditional Detection Methods

- Blacklist-based URL detection
- Spam filters
- Browser security warnings

Machine Learning-Based Detection (Overview): Machine learning techniques analyze email content, URLs, and user behavior to identify phishing attempts. These methods improve detection accuracy but require quality data and training.

VIII. Prevention Techniques

- **User Awareness**

  Avoid clicking unknown links

  Verify sender email addresses

  Check website URLs carefully

- **Technical Measures**

  Two-factor authentication (2FA)

  Secure email gateways

  Browser security extensions

- **Organizational Measures**

  Employee cyber security training

  Regular system updates

  Security policies and guidelines

IX. Research Methodology

This research follows a descriptive and analytical methodology. Information was collected from research papers, cyber security reports, online articles, and case studies. The study analyzes phishing attack techniques and existing prevention strategies.

X. Results and Discussion

The research reveals that phishing attacks are increasing due to lack of awareness and advanced attack techniques. Users are often the weakest link in cyber security. Awareness training combined with basic security tools significantly reduces the success rate of phishing attacks.

XI. Future Scope

- AI-based phishing detection systems
- Browser-integrated phishing protection
- Automated phishing response mechanisms

XII. Conclusion

Phishing attacks remain one of the most serious cyber security threats. This study concludes that user education, secure authentication methods, and awareness programs play a vital role in preventing phishing attacks. Future research can focus on advanced AI-based phishing detection systems.

References

1. K. Jain and B. B. Gupta, “Phishing Detection: Analysis of Visual Similarity Based Approaches,” Security and Communication Networks, 2017.
2. M. Aleroud and L. Zhou, “Phishing Environments, Techniques, and Countermeasures: A Survey,” Computers & Security, vol. 68, 2017.
3. Anti-Phishing Working Group (APWG), “Phishing Activity Trends Report,” 2023.
4. NIST, “Cybersecurity Framework and Guidelines,” National Institute of Standards and Technology, USA.

:::. Cite this article .:::

Raval, K., & Rathod, A. P. (2025). A Study on the Impact of Artificial Intelligence in Education. SK INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH HUB, 12(11), 49–51. https://skpublisher.com/docs/papers/volume12/issue11/SKV12I11-0007.pdf

