Rajguru Tejas Prakash ,2026, 14:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Phishing Attacks: A Review Of Types, Attack Techniques And Prevention Strategies

Rajguru Tejas Prakash; Prof. M. R. Kumbhoje; Prof. M. C. Kolse; Prof. S. K. Said
Department Of Artificial Intelligence And Data Science Jaihind College Of Engineering Pune, Maharashtra, India

Abstract—Phishing remains one of the most common entry points for cyberattacks, tricking people into revealing credentials, installing malware or transferring money. Phishing has diversified far beyond mass emails into targeted spear phishing, executive whaling, SMS smishing, voice vishing, clone phishing, malicious websites and social-media lures. This paper reviews phishing from three perspectives. First, it classifies phishing types by channel and targeting. Second, it examines attacker techniques, including social engineering using information from social networks, look-alike domains through typosquatting and homograph characters, cloned websites, and modern adversary-in-the-middle toolkits that intercept credentials and one-time codes to bypass multi-factor authentication, along with evidence on the lifecycle and effectiveness of real campaigns. Third, it reviews prevention strategies across technical controls, such as email authentication, phishing-resistant authentication, browser warnings and detection systems, and human measures, such as training and organizational reporting cultures. A five-layer defence-in-depth framework is proposed, together with research gaps, objectives, a comparison of authentication methods and challenges. The review concludes that no single control stops phishing, but layered technical and human defences greatly reduce its success.

Index Terms—Phishing attacks, spear phishing, smishing, vishing, typosquatting, adversary-in-the-middle, phishing-resistant MFA, security awareness

I. INTRODUCTION

A single convincing message can give an attacker access to email, bank accounts or a company network. Reports from the Anti-Phishing Working Group [1] show persistently high phishing volumes, and Thomas *et al.* [2] found that victims of phishing kits faced a higher risk of account hijacking than victims of third-party data breaches.

Phishing succeeds because it targets human psychology rather than software flaws. Dhamija *et al.* [3] showed that well-made phishing sites fooled many users, who relied on visual cues and ignored security indicators. As defences improved, attackers adapted with targeted, multi-channel and technically advanced techniques.

This paper reviews phishing types, attack techniques and prevention strategies, and proposes a defence-in-depth framework.

II. THEORETICAL BACKGROUND

1. Types Of Phishing

Fig. 1 classifies phishing by channel (email, SMS, voice, web, social media) and by targeting (mass, spear, whaling, business email compromise).



Fig. 1. Classification of phishing attacks.

2. Anatomy Of An Attack

A typical campaign involves reconnaissance, preparation of a lure and infrastructure (domains and websites), delivery, credential capture or payload execution, and monetization. Oest *et al.* [4] measured the end-to-end lifecycle of phishing attacks and found

© 2026 Rajguru Tejas Prakash, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

that most victims are lured within hours of a campaign's start, before blocklists catch up.

III. SURVEY OF EXISTING APPROACHES

Social engineering. Jagatic *et al.* [5] showed that phishing emails appearing to come from a friend, using information from social networks, had a much higher success rate than generic ones. Sheng *et al.* [6] analysed who falls for phishing and found that some demographic groups were more susceptible and that training reduced susceptibility.

Deceptive domains. Gabrilovich and Gontmakher [7] described homograph attacks using visually similar characters, and Agten *et al.* [8] studied typosquatting abuse over months and found many malicious registrations of misspelled popular domains.

Bypassing MFA. Kondracki *et al.* [9] analysed man-in-the-middle phishing toolkits that relay traffic between the victim and the real site, capturing session cookies and one-time codes, and proposed network-level detection.

Prevention. Kumaraguru *et al.* [10] showed that embedded training improves recognition, but Lain *et al.* [11] found in a large long-term organizational study that some forms of embedded training did not reduce susceptibility, while crowdsourced reporting by employees was effective. Visual detectors such as Phishpedia [12] identify fake brand pages, and WebAuthn [13] provides phishing-resistant authentication. Table I summarizes these works.

TABLE I Summary of Literature Survey

Ref.	Method	Key Findings	Limitations
[7]	Homograph attack	Look-alike character domains	Short communication
[3]	Why phishing works	Users ignore security cues	Laboratory study
[5]	Social phishing experiment	Friend-based lures far more effective	Single university
[6]	Susceptibility analysis	Training reduces susceptibility	Online survey sample
[8]	Typosquatting study	Widespread malicious misspellings	Domain-level only
[4]	Phishing lifecycle measurement	Most victims in first hours	Large-provider data
[9]	MITM phishing toolkits	Bypass of MFA; detection method	Evolving toolkits
[11]	Long-term organizational study	Reporting effective; some training not	Single organization

IV. COMPARATIVE STUDY

Table II compares authentication methods by resistance to phishing. Passwords and SMS codes can be phished, app-based codes can be relayed by adversary-in-the-middle kits, and FIDO2 passkeys resist phishing because they are bound to the legitimate domain.

Method	Phishable	AiTM Relay	Recommendation
Password only	Yes	Yes	Avoid alone
Password + SMS OTP	Yes	Yes	Better than none
Authenticator app code	Yes	Yes	Moderate
Push with number matching	Partly	Partly	Good
FIDO2 passkey / key	No	No	Strongly recommended

TABLE II Comparison of Authentication Methods Against Phishing

V. RESEARCH GAPS

1. 1) SMS and voice phishing in Indian languages are under-studied.

2. 2) MFA bypass with adversary-in-the-middle kits is growing faster than defences.

3. 3) Evidence on which training methods work is mixed.

4. 4) Detection lags behind short-lived phishing sites.

5. 5) Small organizations lack resources for layered defences.

VI. AIMS AND OBJECTIVES

- To classify phishing attacks by channel and targeting.
- To review attacker techniques, including deceptive domains and MFA bypass.
- To examine technical and human prevention strategies.
- To propose a defence-in-depth framework.
- To identify challenges and future directions.

VII. PROPOSED ARCHITECTURE

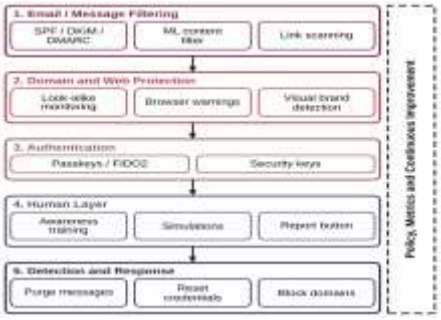


Fig. 2 presents the proposed defence-in-depth framework.

Fig. 2. Proposed defence-in-depth framework against phishing.

1. Email And Message Filtering Layer

SPF [14], DKIM [15] and DMARC [16] authenticate senders; machine learning filters score message content and links.

2. Domain And Web Protection Layer

Monitoring of newly registered look-alike domains, browser safe-browsing warnings and visual brand detection block fake sites.

3. Authentication Layer

Phishing-resistant MFA such as passkeys and security keys ensures that stolen passwords or relayed codes cannot be reused.

4. Human Layer

Short, practical awareness training, simulated exercises and a one-click reporting button turn users into sensors.

5. Detection And Response Layer

Reported and detected phishing triggers removal of messages from all inboxes, password resets and blocking of malicious domains.

VIII. PROCESS FLOW AND EVALUATION

Fig. 3 describes the response workflow. Organizational susceptibility can be tracked with the click rate and the reporting rate in simulations:

$$Click\ rate = N_clicked / N_sent, \quad Report\ rate = N_reported / N_sent \qquad (1)$$

A healthy security culture shows a falling click rate and a rising report rate over time.

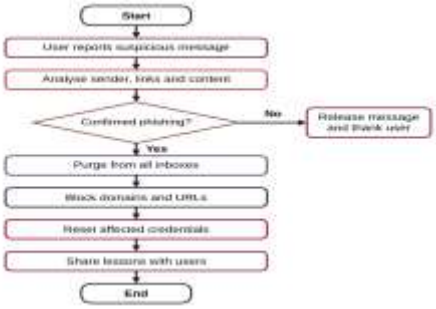


Fig. 3. Phishing report and response workflow.

IX. LIMITATIONS AND FUTURE SCOPE

Table III summarizes challenges. Future directions include AI-generated phishing detection, QR-code phishing defences, protection against deepfake voice calls, and wider adoption of passkeys.

Challenge	Mitigation
Short-lived sites	Real-time ML and visual detection
MFA bypass	Phishing-resistant passkeys
Smishing / vishing	Carrier filtering; verification habits
Training fatigue	Short, contextual training; reporting culture
AI-written lures	Intent-based detection; authentication

TABLE III Challenges and Mitigation

X. CONCLUSION

Phishing has evolved into a diverse set of attacks across email, SMS, voice, web and social media, with

techniques that can even bypass traditional MFA. The reviewed literature shows that layered defences combining sender authentication, domain monitoring, phishing-resistant authentication, user reporting and rapid response are far more effective than any single measure. Organizations and individuals should adopt these layers to reduce phishing risk and protect sensitive information.

1. Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

REFERENCES

1. Anti-Phishing Working Group, "Phishing activity trends report," APWG, quarterly reports. [Online]. Available: https://apwg.org/trendsreports/
2. K. Thomas et al., "Data breaches, phishing, or malware? Understanding the risks of stolen credentials," in Proc. ACM CCS, 2017, pp. 1421–1434.
3. R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI), 2006, pp. 581–590.
4. A. Oest et al., "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale," in Proc. 29th USENIX Security Symp., 2020, pp. 361–377.
5. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Commun. ACM, vol. 50, no. 10, pp. 94–100, 2007.
6. S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in Proc. CHI, 2010, pp. 373–382.
7. E. Gabrilovich and A. Gontmakher, "The homograph attack," Commun. ACM, vol. 45, no. 2, p. 128, 2002.
8. P. Agten, W. Joosen, F. Piessens, and N. Nikiforakis, "Seven months' worth of mistakes: A longitudinal study of typosquatting abuse," in Proc. NDSS, 2015.
9. B. Kondracki, B. A. Azad, O. Starov, and N. Nikiforakis, "Catching transparent phish: Analyzing and detecting MITM phishing toolkits," in Proc. ACM CCS, 2021, pp. 36–50.
10. P. Kumaraguru et al., "Protecting people from phishing: The design and evaluation of an embedded training email system," in Proc. CHI, 2007, pp. 905–914.
11. D. Lain, K. Kostiainen, and S. Čapkun, "Phishing in organizations: Findings from a large-scale and long-term study," in Proc. IEEE Symp. Security Privacy, 2022, pp. 842–859.
12. Y. Lin et al., "Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages," in Proc. 30th USENIX Security Symp., 2021, pp. 3793–3810.
13. W3C, "Web Authentication: An API for accessing public key credentials, Level 2," W3C Recommendation, Apr. 2021.
14. S. Kitterman, "Sender Policy Framework (SPF) for authorizing use of domains in email, version 1," IETF RFC 7208, 2014.
15. D. Crocker, T. Hansen, and M. Kucherawy, "DomainKeys Identified Mail (DKIM) signatures," IETF RFC 6376, 2011.
16. M. Kucherawy and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)," IETF RFC 7489, 2015.