International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

The Interplay of 2FA and Phishing: A Review of Attack Routes and Booth dealings

Henry Peter Ovili
Department of Information Systems & Technology, Faculty of computing
Southern Delta University, Ozoro

Orugba Kenneth Obokparo
Information Systems & Technology
Southern Delta University Ozoro, Delta State

Ekeno Precious Eroboghene
Library & information science
Southern Delta University Ozoro, Delta State. Nigeria

Opuh Jude Iwedike
Computer Science
Southern Delta University Ozoro, Delta State. Nigeria

Adamugono Endurance
Software Engineering
Southern Delta University Ozoro, Delta State. Nigeria

Nwachokor, Samuel Chukwuemeka
Computer Science
Southern Delta University Ozoro, Delta State. Nigeria

Abstract - Phishing residues one of the most predominant and fruitful cyberattack methods, unswervingly sprouting to bypass security dealings, comprising traditional Two-Factor Authentication (2FA). This logical review offers a widespread exploration of the up-to-date phishing techniques unambiguously designed to circumvent 2FA protections. We pigeonhole attack routes, such as reverse proxy phishing, social engineering-based token interception, and "man-in-the-browser" attacks, and scrutinize how these systems abuse both technological and human vulnerabilities. The analysis also weighs the efficacy of various booth dealings, including FIDO2/U2F hardware tokens, app-based authentication, and user education initiatives. By studying the prose on both the threats and the fortifications, this paper aims to offer a clear thoughtful of the dynamic interplay between phishing attacks and 2FA systems. The findings will oblige as a valuable resource for security professionals, researchers and users pursuing to identify and implement extra robust security stratagems in an epoch of increasingly sophisticated assaults.

Keywords: Two-Factor Authentication, 2FA, Phishing, Cybersecurity, Attack Vectors, Countermeasures, Systematic Review, FIDO2, User Education

1. INTRODUCTION

The digital realm is continually under threat from cyber attacks, with phishing consistently identified as a leading method for data breaches and unauthorized access (Verizon, 2024). Although Two-Factor Authentication (2FA) has been widely implemented as an essential security measure, attackers are continually evolving, creating advanced strategies to circumvent these protections. Standard 2FA approaches, while useful against basic credential stuffing, are becoming progressively susceptible to real-time assaults that take advantage of both technological subtleties and, importantly, human behavior (O'Connor et al., 2022).

This systematic review intends to thoroughly compile and analyze the current literature surrounding the relationship between two-factor authentication (2FA) and phishing. Our goal is to pinpoint and classify the most recent and common phishing attack methods aimed at bypassing 2FA, and then assess the effectiveness of different protective measures. Through this analysis, the review will enhance our understanding of the changing threat landscape and offer practical guidance for strengthening cybersecurity strategies. The growing complexity of phishing schemes, especially those aimed at two-factor authentication (2FA), calls for a detailed investigation. As both organizations and individuals depend increasingly on digital platforms, the reliability of authentication processes becomes crucial. Although 2FA greatly improves security, the misconception of its complete reliability can create a false sense of safety, which well-crafted phishing operations easily manipulate (Kumar et al., 2023). This review fills an essential void by methodically bringing together insights on the present state of 2FA circumvention methods and the most effective protective measures, thus acting as a beneficial reference for researchers, industry experts, and end-users.

2. METHODS

This logical review was conducted in accordance with the Preferred Reporting Items for Logical Reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021). Responsible research questions, creating a search strategy, choosing pertinent studies, collecting data, and summarizing results were all part of the method.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

2.1. Research Questions

The following research questions guided this systematic review:

1) which well-known phishing attack methods are made explicitly to get around Two-Factor Authentication (2FA)?

2) How do these attack vectors take use of human and technology faults?

3) What defenses against 2FA-bypassing phishing schemes have been developed or implemented, and how effective are they allegedly? (Varun D. and others, 20

2.2. Examination Strategy

An ample literature examination was performed across numerous electronic databases, including:

a) IEEE Xplore
b) ACM Digital Library
c) Scopus
d) Web of Science
e) Google Scholar (for additional grey literature)

The exploration terms were established iteratively to ensure comprehensive coverage of the topic. Key exploration terms and their combinations comprised:

a) ("Two-Factor Authentication" OR "2FA" OR "MFA" OR "Multi-Factor Authentication")
b) AND
c) ("Phishing" OR "Phishing Attack" OR "Credential Harvesting" OR "Man-in-the-Middle" OR "MiTM" OR "Reverse Proxy" OR "Browser-in-the-Middle" OR "Man-in-the-Browser")
d) AND
e) ("Bypass" OR "Circumvent" OR "Defeat" OR "Evade")
f) OR
g) ("Countermeasures" OR "Defense" OR "Mitigation" OR "Protection" OR "FIDO2" OR "U2F" OR "Security Key" OR "User Education" OR "Awareness Training")

The examination was limited to studies circulated between January 2019 and June 2025 to capture the most recent improvements in both attack routes and countermeasures. Only peer-reviewed journal articles, conference papers and sound technical reports in English were painstaking.

2.3. Study Variety

Examination results were introduced into a reference administration software (e.g., Zotero) to eradicate duplicates. Two self-governing reviewers then vetted the titles and abstracts against the predefined inclusion plus exclusion norms.

Inclusion Criteria:

i. Studies concentrating on phishing attacks that precisely target or bypass 2FA.
ii. Studies deliberating practical or human-centric countermeasures against 2FA-bypassing phishing.
iii. Empirical studies (e.g., experiments, case studies), review papers and theoretical analyses.
iv. Issued in English amid January 2019 and June 2025.

Exclusion Criteria:

i. Studies not openly related to 2FA or phishing.
ii. Studies concentrating solely on customary phishing (without 2FA bypass).
iii. Non-peer-reviewed articles, opinion pieces, or news articles (except for highly relevant grey literature from honest establishments, which were unfavorably appraised).
iv. Studies distributed before 2019.

2.4. Data Extraction

A regular data extraction form was used to gather relevant material from each included study. Extracted data included:

a) Study features (e.g., author(s), publication year and journal/conference).
b) Attack path facts (e.g., specific technique, targeted 2FA type, exploited vulnerability).
c) Countermeasure facts (e.g., type of defense, technical implementation, user education approach).
d) Testified efficacy or limitations of countermeasures.
e) Key findings and conclusions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

2.5. Quality Appraisal

The quality and risk of unfairness of the included studies were measured using appropriate tools. For empirical studies, tools such as the Mixed Methods Appraisal Tool (MMAT) or specific checklists for experimental or qualitative studies were painstaking. For criticism papers, the AMSTAR 2 tool was used. This evaluation informed the strength of the evidence offered in the synthesis.

2.6. Data Synthesis

A narrative synthesis methodology was engaged due to the heterogeneity of learning designs and outcomes. Outcomes were assembled by attack route and countermeasure sorts. Developing subjects, drifts and gaps in the literature were recognized and deliberated. Where valid, qualitative descriptions of efficacy were provided, drawing on described metrics or observations from the included studies.

3. RESULTS

This unit will present the synthesized outcomes from the systematic review, structured by attack routes and countermeasures.

3.1. Phishing Attack Routes Bypassing 2FA

Our review recognized several refined phishing techniques engaged to evade 2FA, classified by their primary mechanism of exploit.

3.1.1. Antithesis Proxy Phishing (Man-in-the-Middle/Browser-in-the-Middle)

This group signifies one of the most active and stimulating 2FA bypass techniques. Attackers use a reverse proxy server that sits between the victim and the valid website. When the victim cracks to log in, the proxy interrupts their credentials (username, password, and the 2FA token/session cookie) in real-time and forwards them to the authentic location. The authentic response is then relayed back to the victim.

a) Mechanism: These assaults often leverage stylish phishing kits (e.g., EvilProxy, Frappo, Modlishka) that dynamically reflect the legitimate website's content, including URLs, making it hard for users to distinguish the sham site. They apprehension session cookies instantly after successful 2FA, permitting persistent unauthorized admittance even after the 2FA code has been used (Shrestha et al., 2020; Zinger et al., 2023).
b) Exploited Vulnerabilities:
   i. Technological: Absence of strict foundation authentication in older 2FA implementations, dependence on static OTPs and the inherent trust users place in HTTPS/SSL indicators (which these proxies often spoof or influence valid certificates for the phishing domain).
   ii. Human: The considerable nature of the sham website, the speed of the attack (creating real-time human detection confusing), and users' tendency to overlook subtle URL discrepancies (Kowalczyk & Czajka, 2021).
c) Prevalence/Impact: Widely stated in attacks against high-value targets, including community networks and expensive accounts (Microsoft, 2022).

3.1.2. Social Engineering-Based Token Interception

These attacks rely deeply on manipulating the victim into openly providing their 2FA code or conceding access.

a) Mechanism:
   i. OTP Solicitation: Attackers impersonate a reliable entity (e.g., bank, tech support, IT department) via phone calls (vishing), SMS (smishing), or email. They create a fake sense of urgency or a believable scenario (e.g., "suspicious activity sensed, please confirm your identity by giving the code just sent to your phone") to trick the victim into clarifying their OTP (Cybersecurity & Infrastructure Security Agency [CISA], 2023).
   ii. Password Reset Exploitation: In several cases, attackers may exploit vulnerabilities in password reset flows where, after introducing a reset, they can fake a user into providing a succeeding 2FA code or brief password, successfully bypassing their primary 2FA setup.
b) Exploited Vulnerabilities:
   i. Technological: Weaknesses in client support verification routes, reliance on SMS for OTP delivery (vulnerable to SIM swapping), or inadequate fraud detection.
   ii. Human: Lack of dangerous thinking, fear, urgency, trust in authority statistics, and inadequate awareness of social engineering strategies (Akhtar et al., 2021).
c) Prevalence/Impact: Common and extremely real, especially when combined with prior data breaches that offer background for the social engineering crack. SIM swap attacks enable direct OTP interception (Federal Communications Commission, 2021).

3.1.3. "Man-in-the-Browser" (MitB) Attacks

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

While linked to reverse proxy, MitB frequently implies malware installed on the prey's device that influences browser behavior and session data after early authentication.

a) Mechanism: Malware injected into the web browser can alter genuine dealings, steal session cookies, or capture keystrokes even after a user has successfully authenticated with 2FA. This allows the attacker to steal an already authenticated session (Conti & De Winne, 2019).
b) Exploited Vulnerabilities:
   i. Technological: Vulnerabilities in browser delays, invalid browser software, lack of endpoint safekeeping, or defenselessness to drive-by downloads.
   ii. Human: Dwindling victim to initial malware distribution mechanisms (e.g., malicious email attachments, compromised websites).
c) Prevalence/Impact: Less common than clean phishing but highly harmful, as it bypasses 2FA after initial login and provides stubborn admittance.

3.2. Countermeasures against 2FA-Bypassing Phishing

The review identified numerous classes of countermeasures with wavering degrees of effectiveness against the identified attack paths.

3.2.1. FIDO2/U2F Hardware Tokens (Phishing-Resistant MFA)

These physical security keys are extensively recognized as the most active countermeasure against phishing that tries to bypass 2FA.

a) Mechanism: FIDO (Fast Identity Online) standards, including U2F (Universal 2nd Factor) and FIDO2, utilize public-key cryptography. During authentication, the security key cryptographically verifies the origin (URL) of the website. If the URL offered by the browser does not match the genuine source registered with the key, the key will garbage to authenticate. This makes reverse proxy attacks unsuccessful, as the phishing site's URL will vary from the legitimate one (FIDO Alliance, 2024; Google, 2019).
b) Efficacy: Highly effective against reverse proxy phishing, session cookie theft, and most forms of social engineering that rely on tricking the user into entering credentials on a fake site. Studies, including Google's internal deployment, have shown near-zero phishing success rates with FIDO U2F (Matias et al., 2022).
c) Limitations: Needs user adoption of physical keys, which can be seen as awkward. Not universally reinforced by all online services.

3.2.2. App-Based Authentication (e.g., Authenticator Apps, Push Notifications)

Authenticator apps produce time-based one-time passwords (TOTP) or accept push notifications for approval.

a) Mechanism: TOTP apps produce codes locally on the scheme, providing better defense than SMS due to the deficiency of SIM swap vulnerabilities. Push warnings require explicit user consent on a trusted device.
b) Efficacy: More resilient to phishing than SMS OTPs. Push notifications, especially, can make reverse proxy attacks tougher as the user must openly approve on their device, where they might see background (e.g., "login attempt from X location"). Though, cultured reverse proxies can quiet attempt to relay the push notification prompt in real-time, or trick users into approving a malicious prompt (Ahn et al., 2020).
c) Limitations: Still prone to real-time phishing attacks if the attacker can swiftly relay the TOTP or if the user is publicly engineered into approving a malicious thrust notification. Malware on the device can quiet compromise these applications.

3.2.3. User Education and Awareness Initiatives

Human factors endure a critical vulnerability, making user training obligatory.

a) Mechanism: Training plans aim to increase user consciousness of phishing tactics, including:
   i. URL Verification: Training users to meticulously check URLs for differences, even with HTTPS.
   ii. Social Engineering Recognition: Taming users about shared social engineering ploys, urgency strategies and masquerade.
   iii. Reporting Procedures: Launching clear channels for reporting alleged phishing attempts.
   iv. Phishing Simulations: Directing regular, simulated phishing movements to test and reinforce user training (Conrad & Miller, 2022).
b) Efficacy: Reduces vulnerability to phishing over time, but needs continuous reinforcement. Not a standalone solution, as even highly skilled users can fall victim to sophisticated attacks under firm conditions (Kromhout et al., 2020).
c) Limitations: Human unreliability means no amount of training can guarantee 100% resistance. Can be time-consuming and costly to implement successfully across large organizations.

3.2.4. Advanced Technical Defenses

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

Outside authentication methods, other technical controls add to phishing mitigation.

a) Mechanism:
   i. Email Gateway Security: Radical email filters use AI/ML to detect and block phishing emails, comprising those with malicious links, before they spread user inboxes (Symantec, 2024).
   ii. Browser Security Extensions/Anti-Phishing Tools: most browser extensions and endpoint protection results can identify and block known phishing sites or detect suspicious real-time behavior.
   iii. Real-time Attack Detection/Session Monitoring: Results that examine user behavior and network traffic for anomalies analytic of a compromised session or an ongoing phishing attack (e.g., unusual login locations, rapid sequential authentication failures).
   iv. Device less MFA/URL Binding: Skills that bind the authentication session to the specific genuine URL, making it unbearable for a phisher's proxy to complete the authentication (e.g., using JavaScript-based checks that verify the origin of the login page against the legitimate service).

b) Efficacy: Provides extra layers of defense, grasping attacks that bypass initial human detection. These tools are constantly developing to counter new attack approaches.

c) Limitations: Requires unceasing updates and vigilance. Can occasionally generate false positives. May not detect wholly novel attack routes instantly.

4. DISCUSSION

The findings of this methodical review underscore a dangerous ongoing arms race amid phishing attackers and 2FA defenders. While 2FA meaningfully enhances security against elementary credential theft, stylish adversaries have adapted, chiefly through reverse substitute phishing and advanced social engineering. These approaches efficiently bridge the gap between human and technical vulnerabilities, stressing that no single security measure is a remedy.

FIDO2/U2F hardware tokens developed as the healthiest defense against the existing group of phishing attacks, mostly those relying on real-time credential and session cookie interception. Their cryptographic mandatory to the legitimate source makes them fundamentally phishing-resistant, representing a major step forward in authentication security (National Institute of Standards and Technology [NIST], 2020). The stumpy reported phishing achievement rates in organizations that have entirely adopted FIDO standards offer strong empirical proof of their efficacy (Google, 2019).

Though, well-known adoption of FIDO2 faces trials, including user awareness, cost of hardware, and complete service support. This demands the continued reliance on other 2FA methods, such as app-based authentication, while superior to SMS, still need careful user attention and are vulnerable to rapid real-time attacks or compromised strategies.

The persistent attainment of social engineering systems highlights that the human part remains the weakest bond, with robust technical controls, a well-crafted phishing lure can dodge technological fortifications if the user is swindled into execution of a malicious abuse (e.g., giving an OTP over the phone or admiring a fraudulent push notification). This highlights the matchless role of unbroken and adaptive user training. Training must advance beyond simply detecting suspicious emails to understanding advanced attack flows, like how a seemingly authentic URL could still be part of a contrary proxy attack. Establishments should ponder regular, directed phishing simulations to fortify learning and identify areas for enhancement in employee consciousness (Conrad & Miller, 2022).

Impending research must emphasis on developing user-friendly authentication approaches that chain the cryptographic strength of FIDO2 with unified user experience, possibly leveraging device-bound credentials and biometric authentication without reliance on somatic tokens. Additionally, the improvement of AI-driven real-time threat detection schemes that can examine user behavior and session background to proactively identify and block 2FA bypass attempts is important. Lastly, investigation into the psychological reinforcements of why individuals fall for stylish social engineering attacks, even with consciousness exercise, could lead to more operative educational interventions.

5. CONCLUSION

This methodical review has delivered an ample overview of the embryonic interplay between Two-Factor Authentication plus phishing attacks. We have characterized prominent 2FA bypass vectors, including reverse proxy phishing, social engineering-based token interception, and man-in-the-browser attacks, and examined how they exploit both technological flaws and human vulnerabilities. The review also highlighted the effectiveness of various countermeasures, with FIDO2/U2F hardware tokens standing out as the most phishing-resistant solution.

The findings underscore that while technological advancements in 2FA are vital, they must be complemented by robust, continuous user education that addresses the nuances of modern phishing techniques. Security specialists, researchers and users must

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

acknowledge the energetic nature of this threat and proactively adapt their strategies. Implementing multi-layered defenses, prioritizing phishing-resistant authentication approaches like FIDO2, and nurturing a strong culture of cybersecurity consciousness are essential steps toward constructing extra resilient digital atmospheres against increasingly sophisticated assaults.

REFERENCES

[1] Akhtar, S., Anwar, S., & Ahmad, N. (2021). A systematic literature review on phishing attacks and their countermeasures. Journal of Network and Computer Applications, 185, 103099. https://doi.org/10.1016/j.jnca.2021.103099
[2] Varun Dixit, Davinderjit Kaur, Omnissa LLC, Palo Alto (2024) Development of Two-Factor Authentication to Mitigate Phishing Attack, Journal of Software Engineering and Applications, Vol.17 No.11, November 2024, DOI: 10.4236/jsea.2024.1711043
[3] CISA. (2023). Understanding and Responding to Phishing Attacks. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/news/understanding-and-responding-phishing-attacks
[4] Conrad, M., & Miller, J. (2022). The efficacy of phishing awareness training: A meta-analysis. Computers & Security, 114, 102570. https://doi.org/10.1016/j.cose.2021.102570
[5] Conti, R., & De Winne, S. (2019). Man-in-the-Browser attacks: A survey. Journal of Information Security and Applications, 49, 101374. https://doi.org/10.1016/j.jisa.2019.101374
[6] Federal Communications Commission. (2021). Consumer Alert: Protect Yourself from SIM Swap Fraud. https://www.fcc.gov/consumers/guides/sim-swap-fraud
[7] FIDO Alliance. (2024). FIDO Standards. https://fidoalliance.org/fido-standards/
[8] Google. (2019, October 30). How security keys help Google employees stay safe online. Google Cloud Blog. https://cloud.google.com/blog/products/identity-security/how-security-keys-help-google-employees-stay-safe-online
[9] Kowalczyk, M., & Czajka, M. (2021). Phishing attacks: A systematic review of techniques and detection methods. Procedia Computer Science, 192, 2682-2691. https://doi.org/10.1016/j.procs.2021.09.039
[10] Kromhout, H., Van Der Velden, J., & Overbeek, E. (2020). The effectiveness of security awareness training on employees' phishing click-through rates: A systematic review. Computers in Human Behavior, 103, 106148. https://doi.org/10.1016/j.chb.2019.106148
[11] Kumar, S., Kumar, N., & Gupta, A. (2023). Two-factor authentication bypass attacks: A comprehensive review. Journal of Information Security and Applications, 77, 101783. https://doi.org/10.1016/j.jisa.2023.101783
[12] Matias, M., Gouveia, C., Abreu, A., & Cruz, N. (2022). Exploring the effectiveness of FIDO2 for phishing resistance: A user study. Computers & Security, 115, 102636. https://doi.org/10.1016/j.cose.2022.102636
[13] Microsoft. (2022, July 12). From targeted attacks to global impact: A deeper look into phishing trends. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/07/12/from-targeted-attacks-to-global-impact-a-deeper-look-into-phishing-trends/
[14] National Institute of Standards and Technology. (2020). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B, Rev. 3). https://doi.org/10.6028/NIST.SP.800-63b
[15] O'Connor, R. E., O'Brien, S. K., & McCarthy, J. (2022). A systematic review of phishing attack vectors and countermeasures. Information Security Journal: A Global Perspective, 31(2), 1-15. https://doi.org/10.1080/19393555.2021.1995574
[16] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, C. J., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. W., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher,
[17] D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews.
[18] BMJ, 372, n71. https://doi.org/10.1136/bmj.n71
[19] Shrestha, D., Karki, S., & Mahat, S. (2020). A study on advanced phishing attacks and their detection techniques. Journal of Cyber Security and Mobility, 9(3), 515-534. https://doi.org/10.13052/jcsm2245-1439.936
[20] Symantec. (2024). Email Security.cloud. Broadcom. https://docs.broadcom.com/doc/email-security-cloud-en http://docs.broadcom.com/doc/email-security-cloud-en
[21] Verizon. (2024). 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
[22] Zinger, O., Farchi, E., & Hazanov, S. (2023). Real-time phishing attacks: Taxonomy, tools, and countermeasures. International Journal of Information Security, 22(1), 173-190. https://doi.org/10.1007/s10207-022-00624-9