Phishing Resistant Systems: A Literature Review

Jonathan Luckett
College of Business, Innovation, Leadership and Technology
Marymount University
Arlington, Virginia
Jonathan_luckett@marymount.edu

***Abstract*—Phishing is one of the leading cyber attack vectors against businesses and consumers. President Biden signed an Executive Order on Improving the Nation's Cybersecurity in May of 2021. The Administration followed up with Memorandum M-22-09, which in addition to laying out a Zero Trust strategy for the federal government to follow, also provides special emphasis on phishing resistant systems such as MFA. This paper provides a literature review of phishing resistant systems and covers Microsoft solutions for the enterprise, eliminating passwords as specified in the Web Authentication API and FIDO 2 standards. Research into how threat actors accomplish phishing schemes is examined, along with email authentication (Sender Policy Framework, SPK; Domain Key Identified Mail (DKIM); and the Domain-Based Message Authentication, Reporting and Conformance (DMARC) standard). Browser-based detection systems are also reviewed, along with phishing intelligence databases that developers can integrate into their applications.**

Keywords—phishing; phishing-resistant; FIDO; SPK; DKIM; DMARC; Defender.

I. INTRODUCTION

On May 12th of 2021, President Biden signed EO 14208, Executive Order on Improving the Nation's Cybersecurity. The Executive Order directs federal agencies to enhance cybersecurity through several initiatives [1]. One of the specific initiatives spelled out in the EO is that within 180 days agencies must adopt Multi-factor Authentication (MFA). The White House followed up with Memorandum M-2209 in January of 2022, spelling out a Zero Trust strategy and placing special emphasis on the use of phishing-resistant MFA that protects users from cyberattacks [2]. The Memorandum defines phishing resistant authentication as "authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system,"[2]. The Memorandum notes that some MFA approaches do not protect against sophisticated attacks since they can spoof applications and interact dynamically with users. For example, users can be fooled into issuing a one-time code or responding to a security prompt that grants access to the attacker. The Federal Government's Personal Identity Verification (PIV) card protects against these types of attacks. The World Wide Web Consortium (W3C)'s web authentication standard is another approach that is effective that will be discussed later.

II. LITERATURE REVIEW

A. Discussion

The Anti-Phishing Working Group (APWG) noted in their Phishing Activity Trends Report for Q3, 2021 that webmail and Software-as-a-Service (SAAS) providers accounted for 29.1% of phishing attacks [3]. Figure 1 shows the most targeted industries [3].

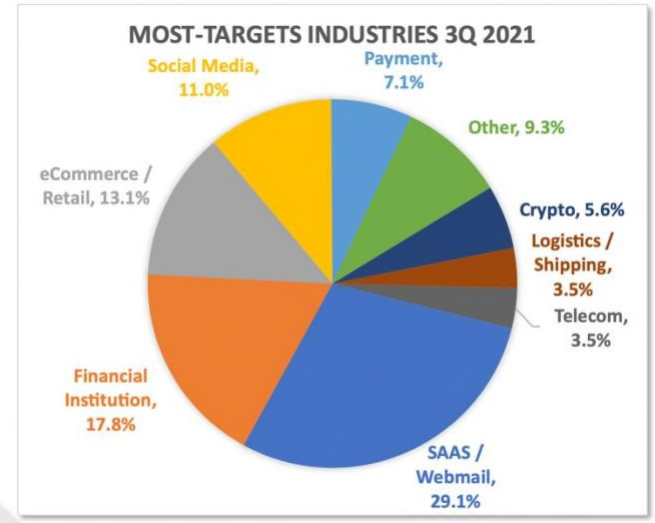

Fig 1. Most Targeted Industries, 3Q 2021 as originally published [3]

Younis and Musbah [4] note that smishing or SMS phishing is an attack that uses the SMS service that is an appealing attack vector for cybercriminals. Two-factor authentication (2FA) uses a hardware token, USB key, QR scan, one-time password, push notification, or contextual awareness to authenticate [5]. However, some 2FA approaches are vulnerable since they do not verify the webpage that the user is interacting with. In this attack, the user is tricked into entering the 2FA credentials into a counterfeit website. There are emerging protocols, such as FIDO (covered later) that help protect against this type of

 ISBN: 978-1-68558-007-0

runtime phishing, which is where a user discloses their credentials and second factor codes to the adversary.

Phishing is the fraudulent practice of sending emails to lure you into providing credentials such as login information, passwords, and other sensitive information. This paper focuses primarily on phishing resistant techniques and technologies that provide a control against phishing emails. The paper also looks at technologies that can protect again malicious links or websites.

According to Dooremaal, et al. [6], phishing detection technologies that protect against fraudulent websites can be grouped into three categories: (1) list-based, (2) visual similarity-based, and (3) heuristic-based [6]. List-based approaches look at the URL of the website a user is visiting and compare that to a list of known phishing/malicious websites (called a block list) or a list of known legitimate websites (called an allow list). There are several anti-phishing websites such as, OpenPhish, PhishTank, and PhishStats. The main issue with list-based approaches is that they are not effective against zero-day attacks and these data sources need to be constantly updated to be useful. Han et al. found that some sites can take up to twenty days to add a site to their list [7]. Visual similarity-based alternatives utilize content on the website to determine its legitimacy. Techniques include examining the favicon (small image next to the website title), examining the logo or comparing screenshots of two websites to determine if one is trying to imitate the other. Heuristic-based approaches analyze features extracted from a website, such as the presence of an SSL certificate [7].

This research looks at a sampling of academic papers consisting of sixteen papers. The research did not take into consideration the number of surveys that have been conducted on phishing attacks. The papers were selected from cybersecurity databases such as Communications & Mass Media Complete, Telecommunications, ABI/INFORM Collection, ABI/INFORM Dateline, ACM Digital Library, and IEEE Computer Society. Keywords included phishing, phishing resistant, FIDO, authentication, MFA, 2FA, and others. Each paper was aligned to one of the four categories (compromised CSP, fraudulent website, stolen credentials and phishing emails) based on the discussion and results section of the paper.

B. *Microsoft Phishing Resistant Solutions*

There are configurations within Microsoft 365 and Exchange to enable anti-phishing settings [8]. Microsoft offers Microsoft Defender for Office 365 and Exchange Online Protection (EOP). EOP is a cloud-based filtering service that protects against spam, malware, and other threats [9]. EOP works by routing each message through filters that check for sender's reputation, malware, mail flow rules that the organization may have set up, and then delivered to the recipient, assuming no malicious content has been found. EOP utilizes the following [9]:

- URL block lists that help detect known malicious links within messages.
- List of domains that are known to send spam.
- Multiple anti-malware engines.
- Inspects the active payload in the message body and all message attachments for malware.

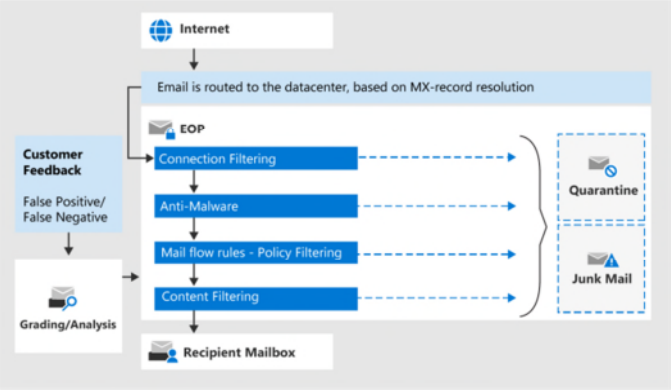

Fig 2. EOP Processing Email as originally published [8]

Microsoft Defender for Office 365 is a standalone product that builds on the protection afforded in EOP. Defender adds safe attachment scanning (for malware), URL scanning and real-time scanning of suspected links, anti-phishing protection (impersonation protection, protected users–specify email addresses that are protected from impersonation, and domain protection) [10]. Defender also adds post-breach investigation, hunting and response tools that allow administrators to see malware detected by the program, view phishing URLs, automate an investigation and response process, and investigate malicious emails [10]. It should be noted that the researcher did not test the effectiveness of these technical solutions.

C. *Eliminating Passwords*

One phishing resistant solution involves eliminating passwords. Passwords are a critical element in a phishing attack; so eliminating them goes a long way towards thwarting a phishing attack. The Web Authentication API, known as WebAuthn, is a specification developed by the World Wide Web Consortium (W3C) and the FIDO Alliance [11]. The API provides a mechanism for servers to register and authenticate users utilizing public key encryption instead of a password. It works with authentication systems that are built into devices such as Windows Hello and Apple's Touch ID. During registration a public/private key pair is created for a website. The user can use a FIDO Compliant authentication app or an

 ISBN: 978-1-68558-007-0

external authenticator. The private key is stored securely on the device. Other sensitive information such as fingerprint and face ID data never leave the device. The server retains the user's public key and a randomly generated credential ID. The server uses the public key and credential ID to validate and authenticate a user to its services. The private key is never shared, and the public key is worthless without the corresponding private key [11]. Typically, a server would request a user ID and password from a user, which it would store online. A threat actor could seal the credentials from the server or with phishing, obtain the credentials from the user. Utilizing WebAuthn, when a user needs to access a web server, it sends a signature which is created with the private key. The server verifies the signature with the user's public key that was created during registration.

FIDO implementation comes in two forms: Platform authenticators are those that are embedded in a device such as a smartphone, tablet, or laptop. Many times, these devices have built-in biometric capabilities like Touch ID, Face ID and Windows Hello. FIDO supports Windows, Mac, Linux, Chrome OS, and Android. Cross-platform authenticators are external, physical devices that support USB, NFC, and Bluetooth [12]. FIDO supports biometrics including face, voice, iris, fingerprint, etc. [13]. FIDO keys include products from Yubico, Thetis, Google Titan, and Kensington, to name a few.

The FIDO Alliance is an industry association that is focused on reducing the reliance on passwords. FIDO stands for Fast Identity Online. FIDO has developed several specifications and standards, including FIDO and FIDO2. FIDO2 is the update to FIDO and was released in 2018. The main component of FIDO is WebAuthn. WebAuthn provides browser-based support for web authentication. FIDO2 also utilizes the Client-to Authenticator Protocol (CTAP), which allows for external authenticators, such as USB, NFC (Near Field Communication), or BLE (Bluetooth Low Energy) [14]. There is a growing number of companies that support FIDO including Apple, AWS, Coinbase, Dashlane, Dropbox, Ebay, Facebook, GitHub, GoDaddy, Google, Login.Gov, Microsoft, Oracle, Salesforce, Twitter, and Yahoo [14].

Miriam, et al. [15] researched how threat actors accomplish phishing schemes by posing as buyers in black-market services. They found five types of email lures: impersonating an associate, a stranger, a bank, Google, or a government authority. All of the services utilized domain squatting–registering and utilizing an internet domain name with the intent of profiting off of someone else's trademark (Nolo, n.d.). The threat actors were able to capture passwords in six out of nine attempts and immediately used the credentials to log in to the victim's account. Where 2FA was activated, the hackers sent subsequent phishing messages to victims asking for their phone number. Clicking on the link in the phishing message led to a fraudulent page that requested the 2FA code that was sent to the victim's phone. When the researchers inputted the 2FA code into the fraudulent page, the hackers were able to successfully log in [15]. The researchers noted that 2FA adds "friction" to attacks. Some dark web services noted that they could not access accounts without the victim's phone number and then had to add additional phishing messages to obtain the 2FA code, which added complexity to their attack [15].

MFA (and 2FA) are not without their flaws. Hendricks and Kettani [17] note that biometrics data is stored in a database and attackers could target those databases and use the biometrics to pass MFA. Further, threat actors have been successful in impersonating customers and resetting accounts and moving cell phone numbers to different SIM cards. Once that happens, the hacker can have the 2FA code sent to the new phone number [17]. Setting up an account PIN or some other form of identification is the best way to protect against this kind of vulnerability.

Razaq et al. [18] found that some threat actors mask fraudulent phone numbers by tricking victims into saving phone numbers as contacts so future calls from that number appear legitimate. Haworth defines Multi-factor authentication (MFA) fatigue as "the name given to a technique used by adversaries to flood a user's authentication app with push notifications in the hope they will accept and therefore enable an attacker to gain entry to an account or device," [19]. Threat actors have been observed using multiple authentication attempts in short succession against accounts that have MFA enabled. This technique, otherwise known as push notification spamming, works because users are often distracted or overwhelmed with notifications and will silence the authentication requests by approving the request [20]. Office 365 can limit these requests by configuring the default limits to the MFA service. Additionally, customers can utilize Microsoft Authenticator app, which works by providing a unique two-digit number that must be confirmed by inputting the number into the app. The authenticator app also supports industry standard time-based one-time passcodes (TOTP or OTP).

D. Email Authentication

By default, email headers and body are not encrypted or protected cryptographically. Thus, the sender's address is not a reliable verification of the sender's identity. There are, however, several methods that can be utilized to authenticate the sender [21]:

- The Sender Policy Framework (SPF) allows administrators to authorize hosts that are allowed to send mail.
- The Domain Key Identified Mail (DKIM) is a standard that provides outgoing email messages with a digital

signature. Recipients can use the signature to verify the validity of the sender.

- The Domain-Based Message Authentication, Reporting and Conformance (DMARC) standard builds on SPF and DKIM by providing a protocol for sender authentication and provides guidance on how to deal with a message that fails the SPF or DKIM test.

Adoption rates for these standards and protocols are low; Hu et al. [22] noted a 44.9% adoption rate in 2018 for SPF and 5.1% for DMARC. A 2019 study by 250ok found that 91.4% of non-profits have no DMARC policy in place despite holding a significant amount of PII [23]. Further, only 23% of Fortune 500 companies have some form of DMARC policy in place. Tatang et al. [23] noted that most email providers utilized some form of authentication. Their study revealed that out of 25 free email service providers, only one did not support SPF; DKIM was supported in 18 out of 25 service providers; and 14 out of 25 supported DMARC [24]. Hu et al. [22] noted a number of technical weaknesses with SPF, DKIM, and DMARC that impacted adoption of these standards and protocols. Table 1 displays these weaknesses.

TABLE I. SPF, DKIM, and DMARC TECHNICAL WEAKNESSES [22]

Protocol	Weakness	Problem Description
SPF	P1. Alignment	The SPF verified sender address can be different from the one displayed to users.
	P2. Mail forward	A forwarded email by default cannot pass the SPF test.
	P3. Mailing list	Emails sent to a mailing list by default cannot pass the SPF test.
DKIM	P4. Alignment	The sender domain that signed DKIM can be different from the one user sees.
	P5. Mailing list	Mailing lists often modify the email content, which will fail the DKIM test.
DMARC+SPF	P2. Mail forward	A forwarded email by default cannot pass the SPF test, and thus fails DMARC.
	P3. Mailing list	Emails sent to a mailing list cannot pass SPF and DMARC at the same time.
DMARC+DKIM	P5. Mailing list	Mailing lists often modify the email content, which will fail the DKIM test.
DMARC+SPF+DKIM	P5. Mailing list	SPF always fails; DIKM will fail if the mailing list modifies email content.

As noted in Table 1, the sender's domain can be different from what the end user sees. Figure 3 displays how SPF authentication focuses on the return-path domain, which can be different from what the user sees [22].

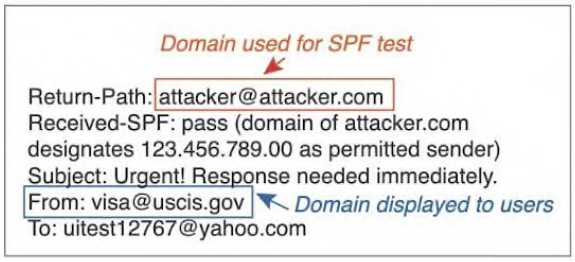

Fig 3. Return path Domain is Different that the Domain Displayed to User as originally published [22]

Additionally, the researchers found that administrators shared implementation challenges as well, such as, lack of control of their DNS servers [22].

E. Browser-Based Phishing Detection

Modern web browsers utilize safe browsing, which are a set of security measures that work to prevent unauthorized activity while an end user surfs the web. Safe browsing should protect against hackers, vulnerabilities, and online exploits. Google's Safe Browsing service that checks website URLs against a database of known malicious sites that is updated every 30 minutes [25]. Chrome actually samples a website's color profile and compares those to known phishing domains. Chrome counts basic colors in each pixel and stores the count in hashmaps. According to Google, image-based phishing is up to 50 times faster at the 50th percentile [25]. Apple's browser, Safari, also uses Google's Safe Browsing, as does Firefox, Chrome and Brave.

Some browsers offer third-party add-ons that provide anti-phishing toolbars and indicators to warn users of malicious sites. Research has shown, however, that these tools do not protect users against high-quality phishing attacks, and that users typically do not pay much attention to browser warnings [21]. Kaushik et al. [25] have found that hackers can take advantage of browser extensions to steal credentials, deliver malware, change browser settings, modify user interface elements, and substitute web content. The researchers noted that there are third-party applications that can scan an extension to see if it is legitimate or not. One such tool is Ext Analysis. While this tool can help prevent the installation of malicious extensions, they are time consuming to use and would need to be deployed on an enterprise level.

F. Phishing Intelligence Databases

There are several phishing intelligence databases that capture information on cloned websites. OpenPhish provides phishing feeds and has several developer plans that can get updates from 12 hours to (free) to five minutes (subscription) [27]. The site also offers an API that developers can use to integrate the searching of malicious URLs into a custom program. PhishTank is a collaborative clearing house for phishing data, which also provides an open API for developers to utilize [28]. PhishStats is a third dataset that is updated every 90 minutes. Developers can use an API as well [28]. All of these sites are useful but do not protect against zero day phishing exploits that have yet to be reported.

Figure 4 notes the top impersonated brands for December 2021 according to OpenPhish [30].

 ISBN: 978-1-68558-007-0

Brand	Industry	Hostnames
Facebook, Inc.	Social Networking	1992
Amazon.com Inc.	e-Commerce	1459
WhatsApp	Social Networking	1264
Office365	Online/Cloud Service	869
Outlook	Online/Cloud Service	624
Crypto/Wallet	Cryptocurrency	613
PayPal Inc.	Payment Service	358
Webmail Providers	Email Provider	344
Tencent	Online/Cloud Service	329
M & T Bank	Financial	295

Fig 4. Top 10 Impersonated Brands–December 2021 as originally published [30]

III. ANALYSIS

The intent is to identify new or variants of a tactic or technique as well as new or updated mitigation strategies. The sample of academic research consisted of sixteen papers. The papers were selected from cybersecurity databases such as Communications & Mass Media Complete, Telecommunications, ABI/INFORM Collection, ABI/INFORM Dateline, ACM Digital Library, and IEEE Computer Society. Keywords included phishing, phishing resistant, FIDO, authentication, MFA, 2FA, and others. Each paper was aligned to one of the four categories based on the discussion and results section of the paper.

70% of the academic papers reviewed fell into two of the four categories: fraudulent website and compromised credentials. 25% of the academic papers fell into the phishing email category.

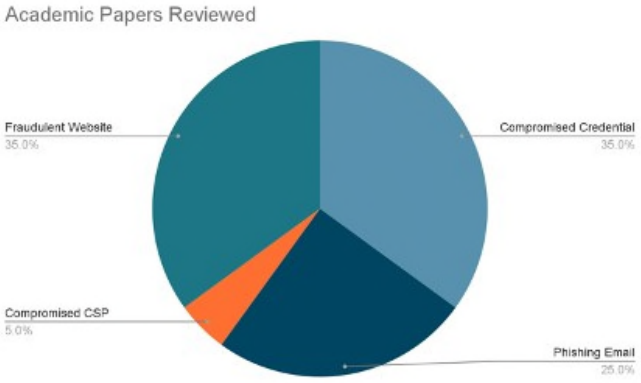

Fig 5. Academic Papers Reviewed.

IV. PASSWORDLESS AUTHENTICATION

Since the literature review of phishing resistant systems was completed, a new entrant is making its way to the market. As of September of 2022, passwordless authentication is being adopted by a number of vendors [5]. Passkeys are a fido authentication credential that provides passwordless entry to online systems [31]. Support for passkeys [6] has been announced by Apple, Google, and Microsoft. Passkeys utilize biometrics or a pin to authentication [32]. Apple integrates Touch ID or Face ID into passkeys and makes it simple to log into a website [7]. Passkeys are synced across user's Apple devices and are encrypted (even Apple [8] does not know that encryption password), [33]. Microsoft utilizes Microsoft Hello for Business, their Authenticator app [9], and fido2 security keys to implement passwordless authentication [10][34]. Google has also expressed support for fido passwordless authentication and will utilized passkeys stored on mobile phones and synced to the cloud for authentication [11] [35]

V. CONCLUSION

The purpose of this study was to review the literature of phishing resistant systems. The author reviewed 16 papers and categorized them into four categories: Fraudulent website, compromised credentials, Compromised CSP, and Phishing Emails. The literature review revealed that there is no single product that provides full protection against phishing attacks. This study is limited in some ways. The scope of the literature review only contained 16 papers. A future study could further expand the number of papers reviewed and map the literature review to the MITRE ATT&CK and D3FEND frameworks. The most exciting technology to prevent phishing is undoubtedly passwordless systems. With support from the fido Alliance, and the big three tech companies (Apple, Microsoft, and Google) the impact of passwordless authentication should significantly reduce phishing initiated attacks.

REFERENCES

[1] J. Biden, "Executive Order on Improving the Nation's Cybersecurity," *The White House*, May 12, 2021. https://www.whitehouse.gov/briefingroom/presidential-actions/2021/05/12/executive-order-on-improving-thenations-cybersecurity/ (accessed Mar. 08, 2022).

[2] S. Young, "M-22-09.pdf." Jan. 26, 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[3] APWG, "Phishing Activity Trends Report, 3QTR, 2021." Nov. 22, 2021.

[4] Y. A. Younis and M. Musbah, "A Framework to Protect Against Phishing Attacks," in *Proceedings of the 6th International Conference on Engineering & MIS 2020*, Almaty Kazakhstan, Sep. 2020, pp. 1–6. doi: 10.1145/3410352.3410825.

[5] E. Ulqinaku, D. Lain, and S. Capkun, "2FA-PP: 2nd factor phishing prevention," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Miami Florida, May 2019, pp. 60–70. doi: 10.1145/3317549.3323404.

[6] B. van Dooremaal, P. Burda, L. Allodi, and N. Zannone, "Combining Text and Visual Features to Improve the Identification

of Cloned Webpages for Early Phishing Detection," in *The 16th International Conference on Availability, Reliability and Security*, Vienna Austria, Aug. 2021, pp. 1–10. doi: 10.1145/3465481.3470112.

[7] X. Han, N. Kheir, and D. Balzarotti, "PhishEye: Live Monitoring of Sandboxed Phishing Kits," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna Austria, Oct. 2016, pp. 1402–1413. doi: 10.1145/2976749.2978330.

[8] C. Davis, U. Gandhi, B. Shilpa, D. Hanson, and D. Coulter, "Anti-phishing policies - Office 365." https://docs.microsoft.com/en-us/microsoft365/security/office-365-security/set-up-anti-phishing-policies (accessed Jan. 30, 2022).

[9] C. Davis, "Exchange Online Protection (EOP) overview - Office 365," Feb. 17, 2022. https://docs.microsoft.com/en-us/microsoft-365/security/office-365security/exchange-online-protection-overview (accessed Mar. 08, 2022).

[10] MSFTTracyP, C. Davis, and D. Simpson, "Office 365 Security including Microsoft Defender for Office 365 and Exchange Online Protection - Office 365," Feb. 17, 2022. https://docs.microsoft.com/en-us/microsoft365/security/office-365-security/overview (accessed Mar. 08, 2022).

[11] Duo Security, "Guide to Web Authentication," *Guide to Web Authentication*. https://webauthn.guide (accessed Jan. 30, 2022).

[12] Hideez, "What is FIDO2 and how does it work? Passwordless Authentication Advantages & Disadvantages," *Hideez*, Jan. 31, 2022. https://hideez.com/blogs/news/fido2-explained (accessed Mar. 09, 2022).

[13] fido Alliance, "What is FIDO?," *FIDO Alliance*. https://fidoalliance.org/what-is-fido/ (accessed Jan. 30, 2022).

[14] S. Tzur-David, "Your Complete Guide to FIDO, FIDO2 and WebAuthn," *Secret double octopus*, Jun. 30, 2020. https://doubleoctopus.com/blog/biometrics/your-complete-guide-to-fido-fastidentity-online/ (accessed Mar. 09, 2022).

[15] A. Mirian, J. DeBlasio, S. Savage, G. M. Voelker, and K. Thomas, "Hack for Hire: Exploring the Emerging Market for Account Hijacking," in *The World Wide Web Conference on - WWW '19*, San Francisco, CA, USA, 2019, pp. 1279–1289. doi: 10.1145/3308558.3313489.

[16] Nolo, "Cybersquatting: What It Is and What Can Be Done About It," *www.nolo.com*. https://www.nolo.com/legal-encyclopedia/cybersquattingwhat-what-can-be-29778.html (accessed Mar. 10, 2022).

[17] A. Henricks and H. Kettani, "On Data Protection Using Multi-Factor Authentication," in *Proceedings of the 2019 International Conference on Information System and System Management*, Rabat Morocco, Oct. 2019, pp. 1–4. doi: 10.1145/3394788.3394789.

[18] L. Razaq, T. Ahmad, S. Ibtasam, U. Ramzan, and S. Mare, "'We Even Borrowed Money From Our Neighbor': Understanding Mobile-based Frauds Through Victims' Experiences," *Proc. ACM Hum.-Comput. Interact.*, vol. 5, no. CSCW1, pp. 1–30, Apr. 2021, doi: 10.1145/3449115.

[19] J. Haworth, "MFA fatigue attacks: Users tricked into allowing device access due to overload of push notifications," *The Daily Swig | Cybersecurity news and views*, Feb. 16, 2022. https://portswigger.net/daily-swig/mfa-fatigueattacks-users-tricked-into-allowing-device-access-due-to-overload-of-pushnotifications (accessed Feb. 18, 2022).

[20] L. Ubiedo, "Current MFA Fatigue Attack Campaign Targeting Microsoft Office 365 Users," *GoSecure*, Feb. 14, 2022. https://www.gosecure.net/blog/2022/02/14/current-mfa-fatigue-attackcampaign-targeting-microsoft-office-365-users/ (accessed Feb. 18, 2022).

[21] O. Wiese, J. Lausch, J. Bode, and V. Roth, "Beware the downgrading of secure electronic mail," in *Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust*, San Juan Puerto Rico, Dec. 2018, pp. 1–9. doi: 10.1145/3361331.3361332.

[22] H. Hu, P. Peng, and G. Wang, "Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems," in *2018 IEEE Cybersecurity Development (SecDev)*, Cambridge, MA, Sep. 2018, pp. 94–101. doi: 10.1109/SecDev.2018.00020.

[23] D. Tatang, F. Zettl, and T. Holz, "The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws," in *24th International Symposium on Research in Attacks, Intrusions and Defenses*, San Sebastian Spain, Oct. 2021, pp. 354–369. doi: 10.1145/3471621.3471842.

[24] A. Bannister, "Google supercharges Chrome's phishing detection mechanism," *The Daily Swig | Cybersecurity news and views*, Jul. 22, 2021. https://portswigger.net/daily-swig/google-supercharges-chromes-phishingdetection-mechanism (accessed Mar. 12, 2022).

[25] K. Kaushik, S. Aggarwal, S. Pandey, S. Mudgal, and S. Garg, "Investigating and Safeguarding the Web Browsers from Malicious Web Extensions," vol. 6, no. 10, p. 10, Sep. 2021.

[26] OpenPhish, "OpenPhish-Phishing Intelligence." https://openphish.com/index.html (accessed Mar. 12, 2022).

[27] PhishTank, "PhishTank | Join the fight against phishing." https://phishtank.org/index.php (accessed Mar. 12, 2022).

[29] PhishStats, "PhishStats." https://phishstats.info/ (accessed Mar. 12, 2022).

[30] OpenPhish, "Phishing Trends: December 2021 - OpenPhish," Jan. 26, 2022. https://openphish.com/blog/phishing-trends-dec2021.html (accessed Mar. 12, 2022).

[31] fido Alliance, "Passkeys (Passkey Authentication)," *FIDO Alliance*.https://fidoalliance.org/multi-device-fido-credentials/ (accessed Sep. 24, 2022).

[32] I. Mehta, "What is Apple Passkey, and how will it help you go passwordless?," *TechCrunch*, Sep. 12, 2022. https://techcrunch.com/2022/09/12/apple-passkey/ (accessed Sep. 24, 2022).

[33] Apple, "About the security of passkeys," *Apple Support*. https://support.apple.com/en-us/HT213305 (accessed Sep. 24, 2022).

[34] Microsoft, "Passwordless authentication | Microsoft Security." https://www.microsoft.com/en-us/security/business/solutions/passwordlessauthentication (accessed Sep. 24, 2022).

[35] S. Srinivas, "One step closer to a passwordless future," *Google*, May 05, 2022. https://blog.google/technology/safety-security/one-step-closer-to-apasswordless-future/ (accessed Sep. 24, 2022).

 ISBN: 978-1-68558-007-0