# Discover and Automate New Adversarial Attack Paths to Reduce Threat Risks for The Security of Organizations

Ghafoor, Azhar; Shah, Munam Ali; Zaka, Bilal; and Nawaz, Muhammad

**Abstract:** ***Phishing remains a pervasive cybersecurity threat, leveraging social engineering and technological deception to obtain sensitive information and credentials. This research explores novel attack paths employed by sophisticated adversaries, focusing on the identification and analysis of emerging tactics to enhance understanding and awareness of evolving phishing threats. The study uncovers various attack vectors, including the impersonation of reputable entities and the exploitation of legitimate platforms for malicious purposes. Notably, it highlights the increasing prevalence of document-based and social media-based phishing campaigns, underscoring the adaptability of attackers in exploiting diverse channels to deceive users. Furthermore, the research evaluates the effectiveness of current countermeasures and proposes actionable strategies to mitigate phishing risks for organizations. Recommendations include strengthening email protection measures, implementing robust web filtering systems, and conducting simulated phishing campaigns to enhance employee awareness. By providing insights into emerging attack paths and practical recommendations, this research contributes to the ongoing efforts to combat phishing threats and strengthen cybersecurity resilience. The findings underscore the critical importance of proactive measures and continuous vigilance in safeguarding against evolving cyber threats in today's dynamic digital landscape.***

**Index Terms:** ***Cyberattack, email gateway, exploitation, identity theft, phishing, PII, spam, spoofing, user credentials.***

## 1. INTRODUCTION

IN contemporary cyberspace, the pervasive threat of phishing looms large, representing a significant challenge to the security of individuals and organizations alike. Phishing, a form of cybercrime that utilizes a combination of social engineering techniques and technological deception, aims to fraudulently obtain sensitive information and credentials from unsuspecting users [1]. This insidious tactic typically involves the creation of deceptive communication channels, such as fraudulent emails, websites, or messages, which mimic legitimate entities or services to deceive victims into divulging confidential information [2].


Fig. 1. Basic flow of phishing attack

The evolution of phishing attacks has been marked by increasing sophistication and diversification, driven by the relentless ingenuity of malicious actors seeking to exploit vulnerabilities in digital ecosystems [3]. From traditional email-based phishing campaigns to more advanced techniques involving document-based and social media-based vectors, the landscape of phishing continues to evolve, presenting formidable challenges for cybersecurity practitioners [4].

At the heart of the phishing phenomenon lies the inherent vulnerability of human psychology to manipulation and deception. Cybercriminals leverage psychological principles and cognitive biases to craft convincing phishing messages that elicit desired responses from their targets [5]. By exploiting factors such as trust, authority, urgency, and fear, phishing perpetrators effectively bypass traditional security measures and exploit human fallibility to achieve their nefarious objectives [6].

In response to the escalating threat posed by phishing attacks, organizations are compelled to adopt proactive measures to enhance their

Manuscript received October 4, 2023.

M. A. Shah is associate professor with Department of Computer Networks and Communication, King Faisal University, Saudi Arabia., Pakistan (e-mail: mashah@kfu.edu.sa).

A. Ghafoor is with the Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan (e-mail: azharghafoor39@gmail.com ).

B. Zaka and S. Nawaz are with the COMSATS University Islamabad, Islamabad, Pakistan

cybersecurity posture and mitigate associated risks [7]. This necessitates a comprehensive understanding of the diverse attack vectors employed by cybercriminals, as well as the development and implementation of effective countermeasures to thwart phishing attempts [8].

TABLE I. Evolution of phishing attacks

| Year | Detail | Year | Detail |
|---|---|---|---|
| 1996 | First time term "phishing" was used | 2009 | Chat in the middle phishing attack |
| 1997 | Alerts about phishing attacks | 2011 | Phishing attack on Xbox users |
| 2001 | Use of spam messages foe phishing attack | 2016 | 500% increase in phishing attacks |
| 2003 | Use of spoofed domains for phishing | 2018 | More than 138 thousand phishing sites were detected |
| 2005 | Use of spear phishing | 2020 | Top targeted country was USA, 74% |
| 2006 | Vishing attack | 2021 | Vishing has raised 550% |

This research paper endeavors to contribute to the ongoing discourse on phishing cybersecurity by conducting a systematic exploration of novel attack paths utilized by sophisticated adversaries. By examining emerging trends and previously unexplored tactics, this study seeks to enhance awareness of evolving phishing threats and provide actionable insights for bolstering organizational resilience against cyber threats [9]. Through an empirical analysis of real-world attack scenarios and a critical review of existing literature, this research aims to elucidate the multifaceted nature of phishing attacks and inform strategic approaches to mitigate associated risks.

In the subsequent sections of this paper, we will delve into the intricate dynamics of phishing attacks, exploring various attack vectors, analyzing their implications for cybersecurity, and proposing effective countermeasures to mitigate phishing risks. By shedding light on the evolving landscape of phishing threats and offering practical recommendations for cybersecurity practitioners, this research aims to contribute to the advancement of knowledge in the field of cybersecurity and empower organizations to defend against the ever-present menace of phishing attacks.

## 2. *Literature Review*

Phishing is the act of sending a bogus e-mail (e.g., via a bulk mailer) to an individual or group of individuals in order to fool them into revealing sensitive information such as credit card numbers, logins, passwords, and so on. To earn the recipient's trust, the phony e-mail frequently closely resembles a legitimate organization [7]. Most security professionals believe that phishing is still a problem for most businesses [8][9]. According to the State of the Phishing Report [10], a study discovered that 76 percent of individuals who participated had been the target of phishing attacks, with smaller organizations more likely to fall victim, than larger firms [11].


Fig. 2. Different sources of phishing attacks

Some researchers deploy multiple phishing techniques in certain places or nations solely to assess people's awareness of cybersecurity assaults and their consequences. As [12] states, the end user's vulnerability to phishing attacks should be determined utilizing three phishing assault simulations: SNP, clone, and email phishing. In [13], particular emphasis was given to analyzing the Nigerian environment, specifically how much individuals are aware of such forms of phishing attacks. As a result, this analysis discovered that Vishing and Smishing are the most common attack routes. A recurrent neural network called SNAP-R, which we demonstrate here, learns to tweet phishing messages to specific persons. The algorithm was trained using data from spear phishing pen testing [14]. To guard against social engineering attacks, an intrusion detection system is presented [15].

Many prior studies, on the other hand, focused on detecting phishing techniques. [16] developed a novel proactive defensive strategy based on email address mutation in the sender. In our system, the sending email address is frequently updated, and only trustworthy peers can authenticate it. Within the Splunk platform, [17] is developing a machine-learning model for detecting fake URLs. In addition, the SVM and Random Forests algorithms were trained to provide a method to avoid phishing on many platforms by using an image as a signature on the authentication page [18]. The sender leaves content-agnostic features in the structure of an email. Proposing a system based on these characteristics capable of learning profiles for a large number of senders and identifying fraudulent emails as deviations from those profiles [19].

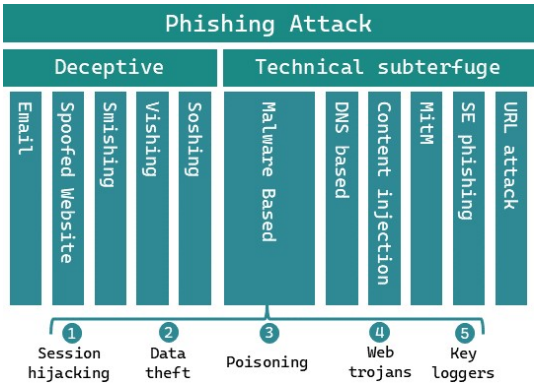


Fig. 3. Phishing Taxonomy

All Internet and mobile device users are vulnerable to phishing attacks. One of the most common purposes of a phishing scam is to obtain sensitive information to steal money or the identity of the victim. Passwords, credit card numbers, and bank account information are just a few examples of what may be gained through phishing. Scammers also employ voice phishing to trick users into thinking they are dealing with a trustworthy firm or people. A detailed taxonomy diagram of phishing attacks is illustrated in Fig. 3.

TABLE II. Comparison Table Of Different Studies

| Ref/year | Proposed Approach | Limitation |
|---|---|---|
| [7] 2021 | Friendly-natured whaling and regular phishing | Lack of adversarial approach |
| [20] 2021 | Adversarial emulation | Regular phishing style |
| [21] 2020 | Comparison of Whaling and Social Engineering Attacks | No solutions provided |
| [22] 2020 | Explanation of phishing attacks | Limited knowledge provided |
| [23]2021 | Autonomy of phishing attacks | Solutions were limited |
| [24] 2020 | Spear phishing | Friendly natured campaigns |
| [25] 2020 | Theoretical Spear phishing | Not user-friendly approach |
| [26] 2020 | URL based phishing | Lack of solution |
| [27] 2021 | Phishing comparison | Lack of adversarial approach |
| [28] 2018 | Theoretical spear phishing model | Lack of implementation |

Criminals utilize social media phishing to lure users into falling for their scams through posts or direct messages. URL hijacking is a tactic that is used to catch users who fill in an incorrect website URL. The "clickjacking" technique takes advantage of a website's design flaws to insert covert capture boxes. At coffee shops and airports, evil twin attacks that imitate public Wi-Fi networks are common. Phishing in search engine results uses strategies to mislead search engines into presenting a phony website above the real one.

Hackers employ phishing as one of their most efficient attack strategies [29]. Phishing assaults surged considerably in 2021 after doubling in 2020, as remote employment made it more difficult for companies to verify their customers weren't victims. As a result, why are organizations still at risk of phishing in the year 2022? This is due in part to the complexity of the assaults themselves. Attackers become increasingly creative in their efforts to get workers to hand over critical information or download dangerous documents. Phishing attacks, such as BEC, may be difficult to identify from legal emails because of previously collected data about a person, including that of a company's chief executive officer. As a result of these increasingly sophisticated assaults and the widely held belief that phishing is "simple to detect," many firms are expected to suffer a breach. Employees must be taught how to spot phishing attacks utilizing contemporary strategies and how to report phishing assaults as soon as they suspect they've been targeted, as well.

## 3. *Discovered Attack Paths*

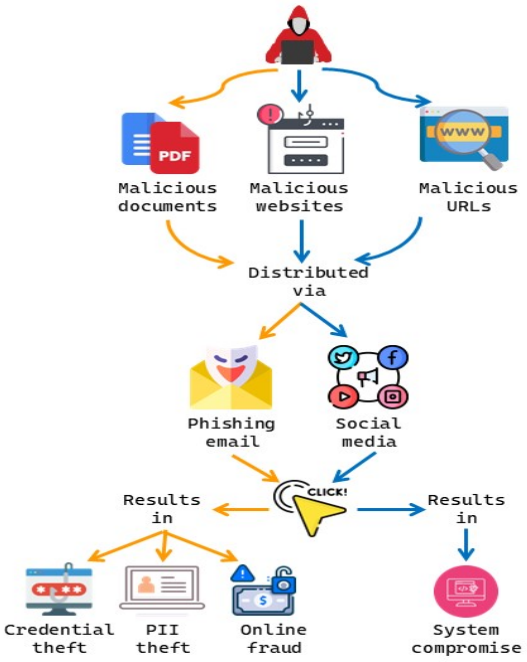


Fig. 4. Flow diagram of phishing attack

Phishing attacks are becoming more and more severe with time for organizations as attackers develop new strategies to overcome the precautionary measures taken by the organizations. Attackers accomplish their malicious objectives by exploiting vulnerabilities in systems or discovering opportunities. Among them are exploring the free services that are trustworthy or creating own services. In this

paper, we will explore some of the use cases that attackers make use of for such purposes. Fig. 3, explains the proposed approach that how attackers successfully send malicious attachments, URLs, and messages by bypassing the security controls such as sandbox analysis of attachments or malicious links detection.

### *2.1 FoolProof Email Spoofing*

There are many different websites used for various kinds of services such as social media, magazine publishing, e-commerce services, portfolios or representing governmental ministries. Users are allowed to share their thoughts in numerous ways such as by commenting on the post, sharing it with other friends, liking it or saving it to check it later on. Websites allow users to share posts either by using social accounts or by email. Most of the users prefer to use an email-sharing option as they can easily share the post without the need to log into the account. Although this was designed to assist the users but unfortunately proved to be an opportunity for hackers. Countless websites are purposefully designed to use them for sending phishing emails such as emkei.cz, endanonymousemail.net, and deadfake.com are a few examples. Although they are free to use, attackers avoid them because they are not well-reputed in the sense that simple email security controls can easily detect them and move them to the spam folder [30].

Fig. 4 conveys the whole idea in an easy-to-understand manner of how attackers use a legitimate service for their malicious purposes. Attackers construct such an email that feels to be authentic and undetectable. From the figure above it is seeable that attackers are spoofing Google's email and pretending it is a real email. This helps them bypass the email security control that checks for malicious links. So, when such links are successfully bypassed from security checks, email is directly moved to the inbox of the victim.

According to a report from Verizon, 25% of all data breaches involved phishing attacks and 85% of attacks became successful because of lack of knowledge. Further in another report from Terranova Security, statistics revealed that more than 20% of employees clicked on phishing links while 67.5% were those who entered their credentials. From these statistics, it became certain that when an email reaches an inbox, there is a strong chance that victims will not be able to differentiate it from the normal email. So, if the user clicks on the link, there are so many things that could be done by the hackers. They can steal information, ask for ransom or in the worst cases they may also make a persistent connection to conduct harmful activities in the future.

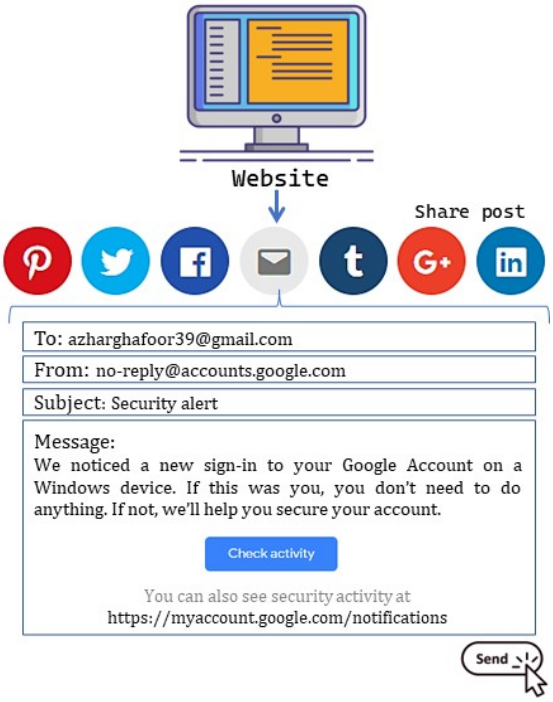


Fig. 5. Foolproof email spoofing to send phishing emails

Misconfigured websites that do not consider vulnerable sides while integrating such attributes are not only harmful for their businesses but also for other users. If websites belonging to governments have such vulnerable attack paths where attackers can easily send spoofed emails to the officials from their websites, then loss may be unbearable and in the worst cases may cause reputational damage.

Phishing comes in various ways and has fatal consciences so one must pay attention to these attacks. Organizations must go for proper penetration testing from experienced red teamers to discover and mitigate such vulnerable attack paths. Education is also a prime factor in the success of these attacks, so more attention is needed on the training side. Different studies have shown proven results of such investments as the number of attacks was reduced to few. Various phishing detection security controls must be purchased and added to the emails and these kinds of attacks could be stopped or lessened somehow. Another solution could be whitelisting senders to allow only a limited number of users to send emails, but it is not an appropriate solution because you have to deal with your customers.

### *2.2 Spoofed Domain*

Intruders create a domain that appears to be genuine but is a clone of the original. They might, for example, use this to create a clone of the original site and send bogus emails to catch

victims [31]. By providing the bogus URL to ad exchanges, they are misled into paying for space on the spoofed site rather than the real site.


Fig. 6. How attackers spoof domains

Hackers spoof domains by developing a realistic-looking phony website to trick users into thinking it is the authentic domain of well-known companies or personalities. They develop a duplicate domain that is so convincing that no one can tell it's not a real domain at first sight. They utilize a double "v" instead of a "w" or a "I" instead of a "l" to make it harder to be differentiated from the genuine one. In some cases, they simply change the TLDs (top-level domain), such as from ".net" to ".com" etc. As a result, when something is shared with users from these sites, they are easily duped and, in most cases, open attachments or click on URLs. These faked domains are the primary source of propagating malware, trojans, or creating bot networks by establishing a permanent connection in response to visitors clicking on malicious links or downloading attachments, resulting in a DDoS attack.

Domain spoofing is also used to carry out additional assaults, such as launching a phishing campaign, exchanging malicious documents, or requesting individuals to reveal their credentials, such as enticing them to obtain a reward by entering the malicious webpage, and so on. This is evident in Fig. 5, which depicts how this attack vector makes the attack more lethal and increases the likelihood of success of attacks. Although these are very hard to detect, some precautions could help in stopping them. One must carefully observe the domain name by hovering the mouse on the links that are sent in an email before clicking on them, should open attachments in a sandbox, and check whether domain names are real, or they have something changed in them, for example, attackers may use 'Í' instead of 'l' etc. Users must also check email headers to see whether the person claiming to be the sender is a real or spoofed identity. They must also make sure that links do not lead to subdomains or any other websites. In Chrome and Brave browsers, there is a padlock in the address bar, if it is green then the link you are visiting is secure, if there is a red crossing line over the lock then you must not trust it as it is not a secure site and may lead to harmful pages.

*1) Domain Spoofing* to Create Spoofed Emails: When an attacker uses a legal website's domain to set up a phony email account, this is known as email spoofing. Phishing attempts frequently make use of email spoofing as a tactic. Using a fake domain name, an attacker can fool users into believing that phishing emails are genuine. In general, an email that appears to be from someone in the company is more reliable than one from an unidentified third party. The goal of the phishing attempt could be to persuade users to visit a certain website, download malware, open a dangerous email attachment, enter account credentials, or transfer funds to an attacker-controlled account. It is not uncommon for emails to contain links to fraudulent websites that require the login and password of the targeted account to be obtained through website spoofing.

2) *Domain Spoofing for Ads:* To conceal the true source of traffic to their websites, ad fraudsters duplicate the domain names of the websites they manage and then auction them off with the help of advertisers. As a consequence, the display ads appear on a website that is less suited than the one specified by the marketers.

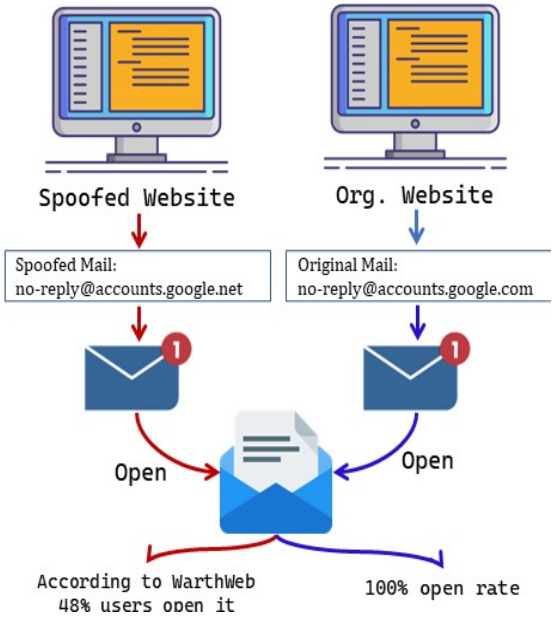


Fig. 7. Spoofed domain-making phishing attempts are more successful

### *2.3 Phishing Documents*

According to Palo Alto Networks during the years 2019 - 20, a huge increase of 1160% was recorded in the use of PDF files containing malicious code hidden in them. They were being transferred using different social media platforms such as LinkedIn, the top-used brand, and the other prime sharing mediums were email, malicious links, or licks on embedded links in those files. PDF files have been observed as the most interesting and luring attack vectors as they

work in multiple platforms irrespective of the type of operating system.

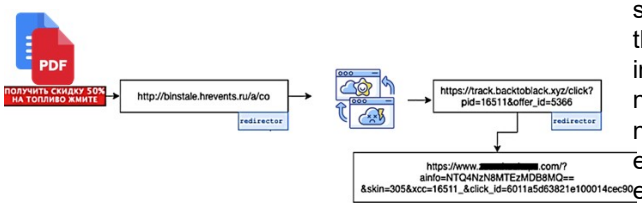


Fig. 8. Document-based attack chain

Malicious documents do not only come from PDF files, but they also range into multiple classes such as Word documents, Excel sheets, Images containing hidden links, Audio files etc. Each type of document has its benefits and drawbacks, but still, they are highly useful for attackers in abusing the vulnerable paths. Attackers also know only a small fraction of users update their office suite, so if any hack has been released it becomes handy to exploit them on unpatched suites. Microsoft Office utilities by default have options of adding macros where attackers usually place malicious code that can easily bypass security controls such as any antivirus or XDRs. If they as AV-bypassed it means they can run without any restriction and can do what they are crafted. In most cases, attackers try to have a reverse shell from the victim to maintain a persistent connection to have better control and know about the personal data present in the system [32].

Attackers craft such a malicious document that when a user simply opens the document, the code embedded starts its execution in the background. Recently, a zero-day was discovered in a Microsoft Word application that enables hackers to gain access to victims without the need for any actions. Researchers from Huntress have validated the most recent zero-day exploit, which exploits the diagnostic tool via an infected Microsoft Word document. The standard security alerts are not generated because the malicious file does not require macros. If the infected document is in RTF format, the script executes without the file needing to be opened in the Preview Tab of Internet Explorer. Instead, MSDT is used to pre-load the file if someone clicks or hovers over the payload to activate it. Further, if an attacker exploits this weakness correctly, it can execute a malicious script with the caller application's permission.

Antivirus must never be disabled. The auto-update option must also be enabled to automatically install new patches. As we cannot see what this document does by simply hovering over the mouse, so directly opening the documents, particularly from unknown senders must be prohibited. We should submit these documents to any of the freely available sandboxes such as cuckoo, cert, or virus total. If the file is safe, you can open it, but always keep in mind that if the content of the file does not need to be updated, deleted, or somehow needed to be copied, then do not click on 'enable editing' or 'enable content' options. Seminars and events must be organized by the organizations to guide them about new scam methods and precautionary measures.

## 4. *Effective Countermeasures*

Most phishing attempts are effective because they are difficult to detect by both users and security systems. Even though hackers are finding new ways to get around security systems, there are still ways to secure ourselves, our data, and our organizations [33]. Here are a few mostly used security aspects suggested by top cybersecurity researchers that help in avoiding phishing attacks and spoofing.


Fig. 9. Anti-phishing solutions

### *4.1 Email Protection*

Secure Email Gateways are the first line of defence against phishing, removing potentially damaging and malicious emails from user mailboxes and isolating them. A good email gateway filters out potentially hazardous hyperlinks and attachments, and also 99.99 % of junk mail. As a result, they perform a significant role in preventing phishing emails from reaching clients. Email gateways also inform organizations when accounts are breached, preventing assaults on business email accounts and the use of hacked accounts to send misused or phishing emails to enterprises. Cloud email security safeguards mailboxes from intruders by utilizing machine learning and artificial intelligence to detect such messages. Furthermore, they use antivirus to scan and identify email threats. On detecting any harmful email, they trigger warning flags on those emails to alert users that they may be harmful or will delete them from the network

based on administrator-defined policies.

### *4.2 Protection Against Web Spoofing*

Web filtering is a technique that effectively prevents customers from visiting websites flagged as phishing or spam websites. Many companies provide intelligence about such websites as they have developed various artificial intelligence-based models that help them know the maliciousness of the sites by examining their pages against many parameters. Using this information, organizations can make policies to prevent users from visiting such websites and submitting their important details. It is also real that stopping users from visiting harmful websites is crucial for organizations as they mostly use VPNs or proxies to bypass the restrictions. Users mostly visit such websites to download paid software for free, to download cracks, download other kinds of prohibited content such as videos, audio, or books etc. On such websites, there are many ads, and they unknowingly click on them, and this thing usually opens a new tab leading to some information stealing software or displaying some unpleasant content hosting websites. So, to overcome all such scenarios advanced web filtering systems must be used as they perform both static and dynamic analysis of URLs and attachments to search websites for phishing indicators, even if they may not contain malicious content.

### *4.3 Simulated Phishing Campaigns*

To combat phishing attempts, it is essential to test employees' ability to differentiate between legitimate and bogus emails. Administrators can use this information to figure out how dangerous phishing is for their whole organization and focus education efforts on the areas that need it most. It is not uncommon to find a platform that allows users to design and distribute their phishing-style email campaigns. Many of these businesses also offer security awareness education to enable their customers to spot phishing emails. Administrators, for example, can replicate phishing attempts on different target groups and assign varying degrees of difficulty to each group. Users who fail tests often should be easy to find and track down based on how often they fail [34].

## *5. CONCLUSION*

Phishing remains one of the greatest threats to individuals and organizations in the public and private sectors. Gateway attacks can lead to identity theft, ransomware attacks, and denial-of-service attacks. Unfortunately, the popularity and effectiveness of phishing are influenced by poor decisions, illiteracy, and lack of attention to detail of individuals. This paper gives an overview of the phishing problem and introduces the motives behind phishing and common attack vectors used in phishing attacks. We discussed different previously undiscovered attack vectors, and their implications, and provided solutions. This study was primarily concerned with identifying areas that an attacker could exploit by adopting their mindset. We performed various experiments to prove whether these attack vectors are important to discuss or not, and our findings proved to be right. In future research, we will try to explore in depth how these attack paths are being exploited by hackers and will try to provide a detailed comparison between various adversarial approaches.

## *REFERENCES*


[1] G. Kavallieratos and S. Katsikas, "Attack path analysis for cyber-physical systems," in *Computer Security*, 6th ed., New York, USA, 2020, pp. 19-33.

[2] I. Stellios, K. Mokos, and P. Kotzanikolaou, "Assessing smart light enabled cyber-physical attack paths on urban infrastructures and services," in *Connection Science*, vol. 34, no. 1, 2022, pp. 1401–1429.

[3] K. Owen and M. Head, "Motivation and Demotivation of Hackers in Selecting a Hacking Task," in *Journal of Computer Information Systems*, 2022, pp. 1-15.

[4] A. Matta, G. Sucharitha, B. Greeshmanjali, M. P. Kumar, and M.N.S. Kumar, "Honeypot: A Trap for Attackers," in *Artificial Intelligence and Industrial Internet of Things Paradigm*, 2022, pp. 91-101.

[5] A. Spagnolli, M. Masotina, A. Scarcia, B. Zuffi, and L. Gamberini, "How to get away with cyberattacks: An argumentative approach to cyberattacks' legitimization by common users," in *CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1-12.

[6] R. Abdillah, Z. Shukur, M. Mohd, and M. Z. Murah, "Phishing Classification Techniques: A Systematic Literature Review," in *IEEE Access*, 2022.

[7] B. Hanus, Y.A. Wu, and J. Parrish, "Phish me, phish me not," *Journal of Computer Information Systems*, 2021, pp. 1-11.

[8] S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," *Journal of the Association for Information Systems*, vol. 18, no. 1, 2017, p. 2.

[9] Verizon, "Data Breach Investigations Report," [Online]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Accessed: 22-09-2021, 07:12 pm].

[10] Wombat Security, "State of Phishing Report 2018," [Online]. Available: https://info.wombatsecurity.com/hubfs/2018.StateofthePhish/Wombat-StateofPhish2018.pdf. [Accessed: 22-09-2021, 07:25].

[11] Symantec, "Internet Security Threat Report Volume 24," 2019, [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf. [Accessed: 22-09-2021, 08:00 pm].

[12] D. Aljeaid, A. Alzhrani, M. Alrougi, and O. Almalki, "Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks," in *Information*, vol. 11, no. 12, 2020, p. 547.

[13] P. N. Mangut and K. A. Datukun, "The Current Phishing Techniques–Perspective of the Nigerian Environment," in *World Journal of Innovative Research (WJIR)*, vol. 10, no. 1, 2021, pp. 34-44.

[14] J. Seymour and P. Tully, "Weaponizing data science for social engineering: Automated E2E spear phishing on

Twitter," [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf. [Accessed: 23-10-2021, 08:00 pm].
[15] J. Nelson, X. Lin, C. Chen, J. Iglesias, and J. J. Li, "Social engineering for security attacks," in *Proceedings of the 3rd Multidisciplinary International Social Networks Conference on SocialInformatics 2016*, New York, NY, United States, 2016, pp. 1-4.
[16] N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, "Security and Privacy in Communication Networks," in *Springer SecureCom2020*, Washington DC, USA, 2020, pp. 21-23.
[17] O. Christou, N. Pitropakis, P. Papadopoulos, S. McKeown, and W. J. Buchanan, "Phishing URL detection through top-level domain analysis: A descriptive approach," arXiv preprint arXiv:2005.06599, 2020.
[18] R. Parthiban, V. Abarna, M. Banupriya, S. Keerthana, and D. Saravanan, "Web Folder Phishing Discovery and Prevention with Customer Image Verification," in *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*, IEEE, Pondicherry, India, 2020, pp. 1-5.
[19] H. Gascon, S. Ullrich, B. Stritter, and K. Rieck, "Reading between the lines: content-agnostic detection of spear-phishing emails," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, Springer, Cham, Donostia / San Sebastian, Spain, 2018, pp. 69-91.
[20] A. B. Ajmal, M.A. Shah, C. Maple, and M.N. Asghar, "Offensive security: Towards proactive threat hunting via adversary emulation," *IEEE Access*, vol. 9, 2021, pp. 126023-126033.
[21] D. Pienta, J.B. Thatcher, and A. Johnston, "Protecting a whale in a sea of phish," in *Journal of Information Technology*, vol. 35, no. 3, 2020, pp. 214-231.
[22] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, and S. Arthi, "Why is phishing still successful?," *Computer Fraud Security*, 2020, vol. 2019, pp. 15-19.
[23] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," in *Frontiers in Computer Science*, vol. 3, 2021, p. 6.
[24] P. Unchit, S. Das, A. Kim, and L.J. Camp, "Quantifying susceptibility to spear phishing in a high school environment using signal detection theory," in *International Symposium on Human Aspects of Information Security and Assurance*, Springer, Cham, July 2020, pp. 109-120.
[25] A. Aleroud, E. Abu-Shanab, A. Al-Aiad, and Y. Alshboul, "An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities," *Journal of Information Security and Applications*, vol. 55, 2020, p. 102614.
[26] A. AlEroud and G. Karabatis, "Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks," in *Proceedings of the Sixth International Workshop on Security and Privacy Analytics*, 2020, pp. 53-60.
[27] P.N. Mangut and K.A. Datukun, "The Current Phishing Techniques–Perspective of the Nigerian Environment," *World Journal of Innovative Research (WJIR)*, vol. 10, no. 1, 2021, pp. 34-44.
[28] M. Bossetta, "The weaponization of social media: Spear phishing and cyberattacks on democracy," in *Journal of International Affairs*, vol. 71, no. 1.5, 2018, pp. 97-106.
[29] V. Zolotarev, E. Zolotareva, and V. Mawla, "Phishing Attacks Digital Trace Analysis for Security Awareness," 2022.
[30] T. Wood, V. Basto-Fernandes, E. Boiten, and I. Yevseyeva, "Systematic Literature Review: Anti-Phishing Defences and Their Application to Before-the-click Phishing Email Detection," arXiv preprint arXiv:2204.13054, 2022.
[31] R. G. Atkinson et al., "U.S. Patent No. 7,398,315," Washington, DC: U.S. Patent and Trademark Office, 2008.
[32] J. Jiang et al., "Detecting malicious PDF documents using semi-supervised machine learning," in *IFIP International Conference on Digital Forensics*, Springer, Cham, February 2021, pp. 135-155.
[33] A. Sadiq et al., "A review of phishing attacks and countermeasures for the internet of things-based smart business applications in industry 4.0," in *Human behavior and emerging technologies*, vol. 3, no. 5, 2021, pp. 854-864.
[34] W. Yeoh et al., "Simulated phishing attack and embedded training campaign," *Journal of Computer Information Systems*, 2021, pp. 1-20.

**Azhar Ghafoor**, part of the Department of Cybersecurity at Air University, is a seasoned professional with 1.5+ years at Cytomate Solutions and 1.5 years as a Cybersecurity Researcher. Armed with a master's in information security, his focus spans compliance, malware analysis, computer-human interaction and knowledge-sharing through writing and freelancing. Email: azharghafoor39@gmail.com

**Munam Ali Shah** received the B.Sc. and M.Sc. degrees in computer science from the University of Peshawar, Pakistan, in 2001 and 2003, respectively, the M.S. degree in security technologies and applications from the University of Surrey, U.K., in 2010, and the Ph.D. degree from the University of Bedfordshire, U.K., in 2013. Since 2004, he has been working as an Assistant Professor with the Department of Computer Science, COMSATS University Islamabad, Pakistan. He has been included in Stanford's list of the top 2% of scientists. Email: mshah@comsats.edu.pk

**Bilal Zaka** is an experienced IT professional, academic manager and researcher; presently Head of IT Services at COMSATS University Islamabad Pakistan. He also provides consultancy services to the Higher Education Commission of Pakistan as a member of various technical committees. Bilal's current research interest is focused on the use of artificial intelligence to enhance capabilities of conventional information systems and unlock the value of structured and unstructured data. He did his PhD in Informatics from the Graz University of Technology - Austria, and an MSc in Electronics from Quaid-e-Azam University Islamabad Pakistan. E-mail: zaka@comsats.edu.pk

**Muhammad Nawaz** obtained his PhD from Cardiff Metropolitan University, UK, in 2021. He is currently serving as a manager at COMSATS University Islamabad Campus. His main areas of interest and research include Distance Learning, Hybrid Learning, and Technology-Enabled Learning. With extensive experience in the field of educational technology, Dr. Nawaz is dedicated to advancing the effectiveness and accessibility of learning through technological solutions. His work focuses on improving educational outcomes and enhancing the learning experience for students in various educational settings. Email: Nawaz@vcomsats.edu.pk