Phishing in Cyberspace: Trends, Vulnerabilities, and Strategies for Addressing this Global Menace

[1]Bernard, Olorunfemi Paul, Edegbe, Glory Nosawaru (PhD), .Chinedu, Pascal (PhD) & Makinde, O.S. (PhD)
Department of Computer Science
Edo State University
Uzairue, Edo State, Nigeria
Emails: [1]bernard20.olorunfemi@edouniversiy.edu.ng, [2]edegbe.glory@edouniversity.edu.ng,
[3]chinedu.paschal@edouniversity.edu.ng, [4]samuel.makinde@edouniversiy.edu.ng

ABSTRACT

Phishing attacks have become a prominent and worrisome cyber threat in the digital environment. The proliferation of advanced technologies and digital platforms has led to an exponential increase in the potential for security breaches, creating an advantageous environment for cyber attackers. This article examines the increasing threat of phishing in the digital realm, investigating the various tactics utilized by cybercriminals to manipulate users and acquire sensitive data. Drawing from recent research and statistics, we highlight the upward trend of phishing activities and their potential implications for the global economy. Furthermore, we shed light on the sectors most vulnerable to phishing attacks and the escalating rates of advanced fee fraud and credential theft. The article concludes by stressing the urgent need for effective countermeasures to safeguard cyberspace and protect vital information from compromise.

Keywords: Phishing, Cyberspace, Trends, Vulnerabilities, Strategies, Addressing, Global Menace

CISDI Journal Reference Format
Bernard, O.P., Edegbe, G.N., .Chinedu, P.. & Makinde, O.S. (2023): Phishing in Cyberspace: Trends, Vulnerabilities, and Strategies for Addressing this Global Menace.. Computing, Information Systems, Development Informatics Journal. Vol 13No 2, Pp 21-30. Available online at https://www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V14N2P3

1. INTRODUCTION

The tremendous growth of innovative technologies used for online services in the global economic space brings along vulnerabilities to security breaches. The upsurge of these vulnerabilities has created a level ground for cyber attacks to flourish. Recently, Phishing is the most mentioned and carried out cyber attack in cyberspace. It was the most overwhelming and worrying attack that has received global attention from end users and security experts (Dutta, 2021; Salloum *et al*., 2022; Do *et al*., 2022; Mughaid *et al*., 2022). Phishing is the nefarious act of deluding naïve users to steal confidential information using sophisticated content injection techniques (Catal *et al*., 2022). Users are deceived by phishing invaders via counterfeiting websites that make users provide their confidential information on a phishing website (Minocha and Singh, 2022). This article provides an analysis of the increasing patterns and susceptibilities linked to phishing, emphasizing the necessity for strong defensive measures to protect against this pernicious menace.

2. PHISHING: A NEFARIOUS GLOBAL MENACE:

The term "phishing" denotes a fraudulent activity in which perpetrators utilize counterfeit web pages and unsolicited electronic messages to mislead individuals into revealing their personal data (Mughaid et al., 2022). The term "phisher" refers to an individual engaged in criminal activities who exploits acquired information through phishing techniques.

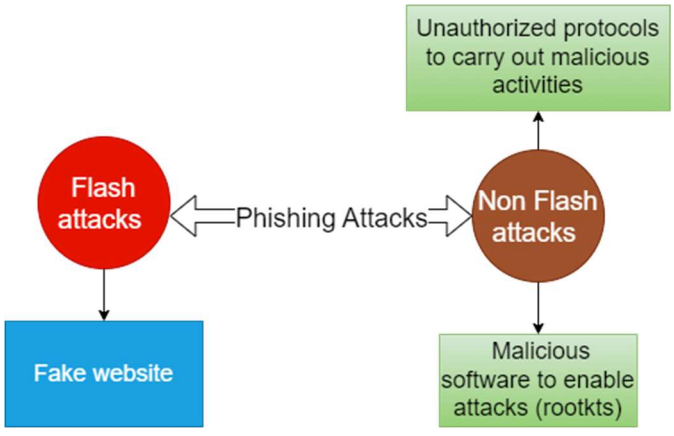
These activities may include stealing funds from victims' financial institutions or gaining unauthorized access to their computers. In some cases, the phisher may demand a ransom in exchange for restoring control (Jain and Gupta, 2021). Phishing perpetrators utilize a range of strategies to acquire personal information from individuals Examples of phishing attacks involve the perpetrator assuming the identity of the victim's financial institution and sending an email notification asserting that the victim's account is nearing expiration, thereby pressuring them to promptly update their personal information (Bhardwaj et al., 2021).

The perpetrator assumes the identity of the individual's financial institution and informs them of potentially fraudulent activities on their debit card. They then urge the individual to click on a hyperlink provided in the email to nullify these transactions (Alkhalil et al., 2021). According to Mensah and Ennin (2022), a deceptive email is dispatched to the target individual, falsely notifying them of their lottery triumph and instructing them to disclose their banking information via a secure hyperlink to redeem the prize.The perpetrator assumes the identity of the Inland Revenue and initiates contact with the target using an email. The email falsely claims that the recipient is eligible for a tax refund as a result of an excessive payment and proceeds to solicit the individual's banking information to facilitate the refund procedure (McNealy, 2022).

Phishing attackers employ various strategies to exploit the vulnerabilities of inexperienced users and technological loopholes (Catal *et al*., 2022; Minocha and Singh, 2022). These strategies encompass a range of phishing attack approaches, including technical subterfuge such as Ransomware, Trojan House, key-and screen-logger, Man-in-the-middle, Content injection, as well as social engineering approaches like website spooling, e-mail spooling, spear phishing, and the exploitation of mobile and online applications (Smishing, Vishing, WIFI, malicious applications, and spyware). Additionally, other methods employed by attackers include compromising web servers, utilizing botnets, DNS poisoning, and exploiting social networking platforms (Jain and Gupta, 2021; Sonowal, 2022; Fuertes *et al*., 2022; Sahoo *et al*., 2022; Aldo *et al*., 2022; Mbona and Eloff, 2022; Akande *et al*., 2022).

3 CATEGORIES OF PHISHING ATTACKS

According to Adebowale, (2020), a phishing scam or attack can be a flash or non-flash attack as presented in Figure 1. According to Gautam *et al.* (2021).



Fi

Figure 1: Categories of Phishing Attacks (Adebowale. 2020)

Flash assaults are characterized by the dissemination of a good number of homogeneous messages in a short time. In contrast, non-flash attacks employ a similar approach but spread the messages over an extended period (Adebowale, 2020). The effectiveness of these attacks hinges on the engagement between the recipient and the message, which can take place when the recipient engages with a malicious hyperlink, discloses valuable information in response, or inadvertently completes a deceptive form with pertinent data, thereby facilitating the success of the attack.

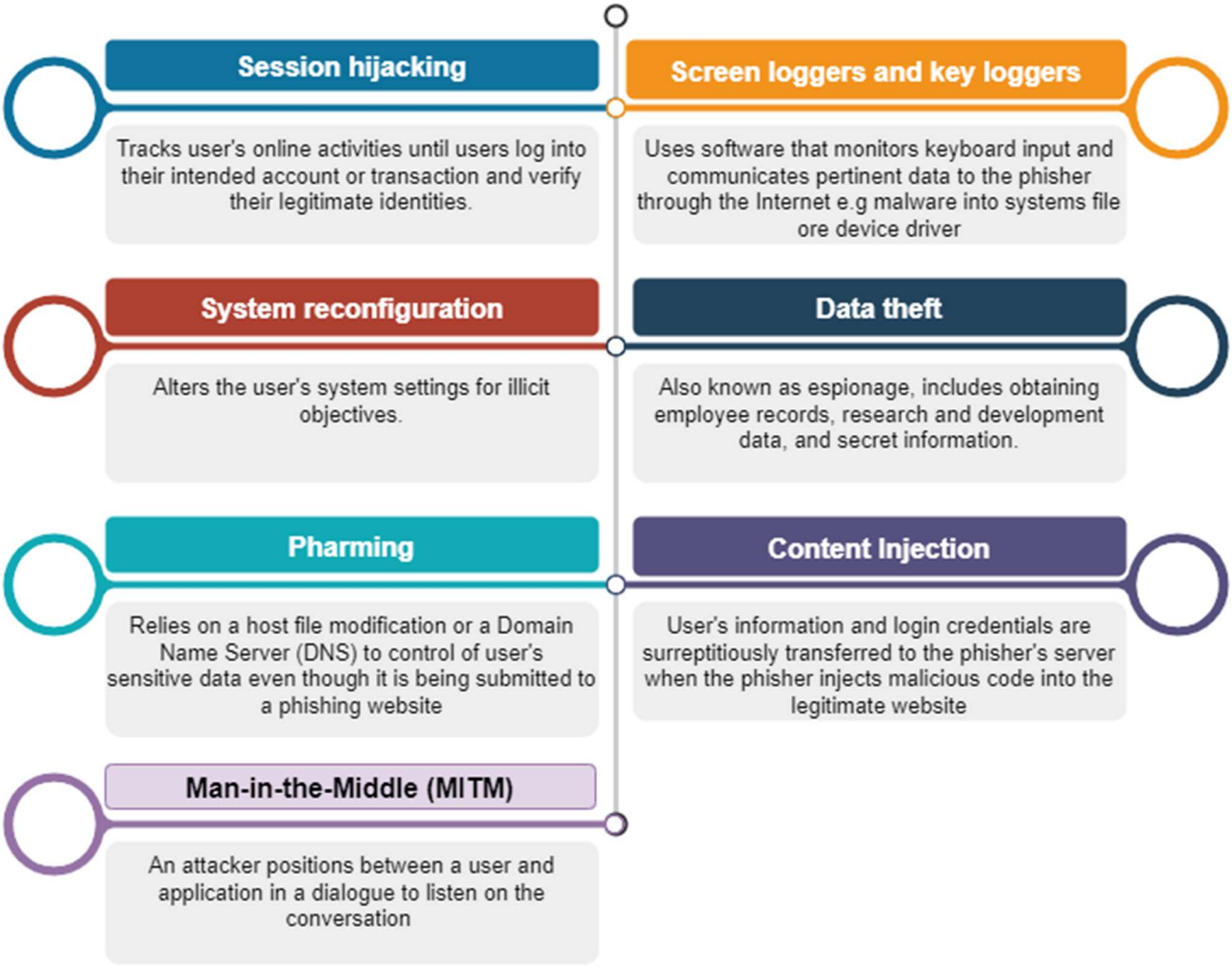


Figure 2. Sophisticated Types of Phishing

More sophisticated types of phishing attacks are Session hijacking (Ghelani *et al*., 2022), Screen loggers and key loggers (Alkhalil *et al*., 2021), System reconfiguration (Potteiger *et al*., 2022), Data theft (Singh and Singh, 2022), Pharming (Chanti and Chithralekha, 2022), Content Injection (Alharbi *et al*., 2022) and Man-in-the-Middle- MITM (Thankappan *et al*., 2022) as presented in Figure 2

3.1 Process of phishing attacks

Irrespective of the attack type, they typically adhere to a consistent five-phase process flow, as illustrated in Figure 3: (Do *et al*., 2022).

Figure 3: Five process flow of phishing attacks (Do *et al.*, 2022).

4. TRENDS AND INCIDENCE OF PHISHING ATTACKS:

Based on the findings presented in the report by the Anti-phishing Working Group (APWG), the incidence of phishing activity experienced an upward trend during the third quarter (July to September) of 2022. Specifically, the total number of phishing attacks recorded during this period reached 1,270,883, surpassing the figures of 1,025,968 and 1,097,811 observed during the first and second quarters of the same year, as documented by APWG (2022). Figure 5 illustrates that the financial sector experiences the highest percentage of phishing attacks at 23.2%, with Software-as-a-System/Webmail following at 17% and social media at 11%. The advanced fee fraud popularly called “Yahoo-Yahoo” is increasing at an alarming rate of over 1000%. Credential theft rose by 7% from the impersonation of corporate executives on social media due to increasing social media platforms (see Figure 6) and cryptocurrency targets rose to 6.6%. If these phishing trends go unchecked and no adequate and quick-response countermeasures to mitigate this global menace, the entire economic life wire (cyberspace) is undoubtedly threatened and will explode with compromised information.

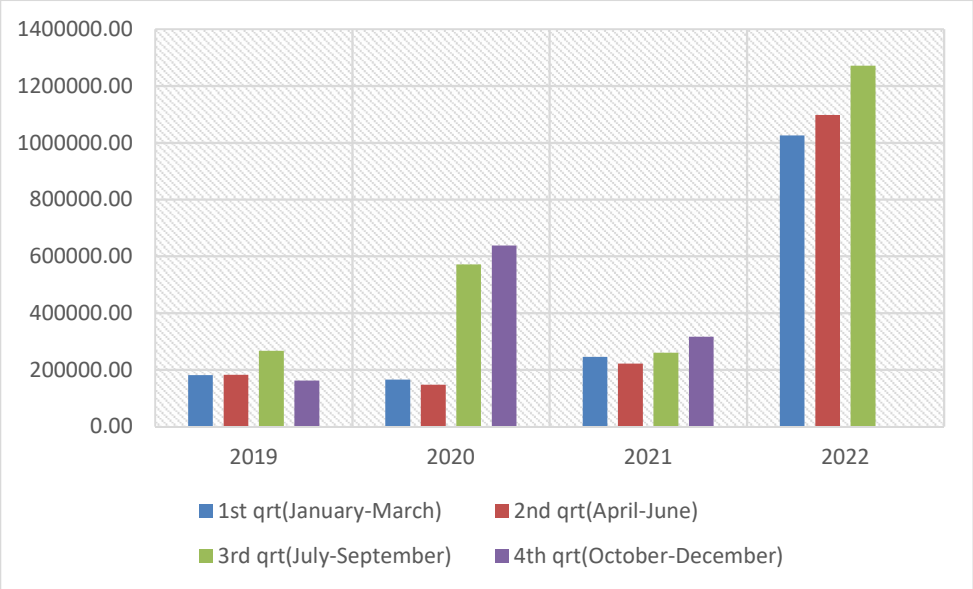


Figure 4: Global Phishing attack trend from 2019 to 3rd quarter of 2022 (Source: APWG, 2022)

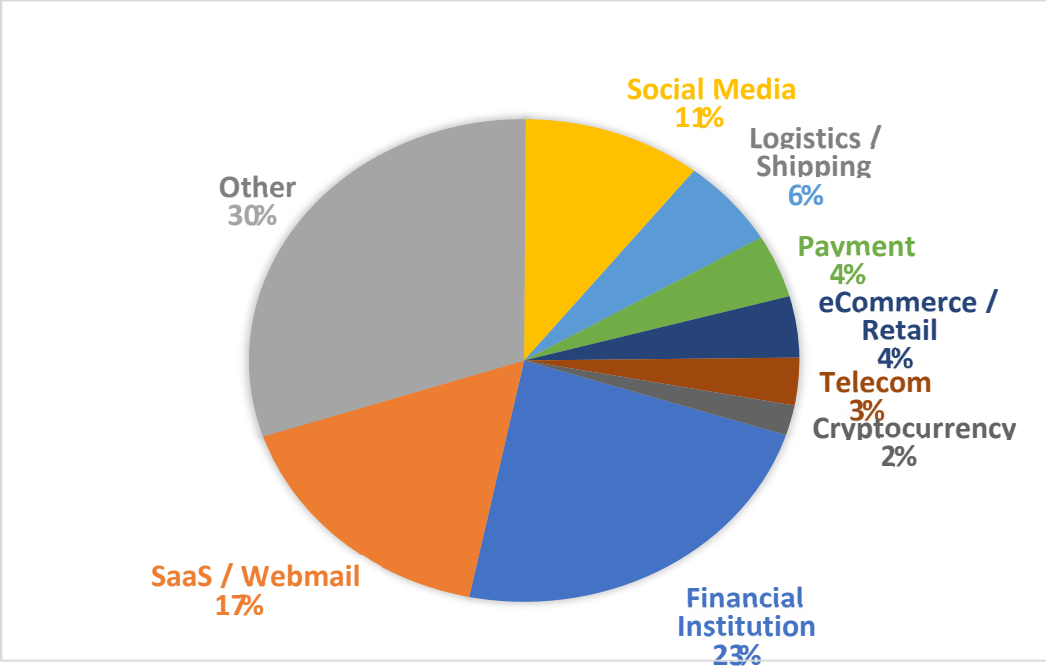


Figure 5: Most targeted industries, 3rd quarter of 2022 (Source: APWG, 2022)

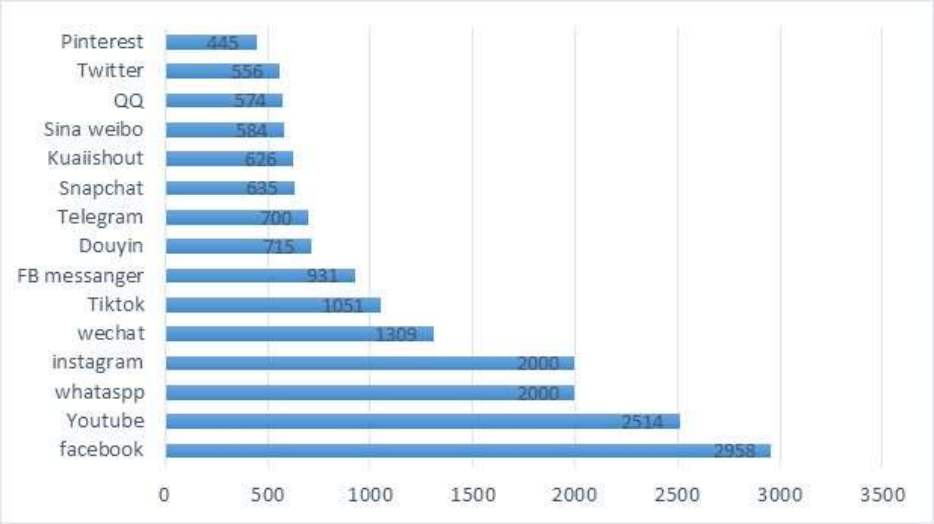


Figure 6: Global statistics of social media users as of Jan 2023 in millions

(Source: Datareporter, 2022)

5. IMPLICATIONS FOR THE GLOBAL ECONOMY

The increasing threat posed by phishing attacks has significant consequences for the global economy. According to Busari (2023), Americans lost $10.3 billion to various online frauds last year -2022. Similarly, Bleach (2023) revealed that fraudsters in the UK made away with a total of £4 billion in 2022. Likening the reported UK loss of £4 billion to fraud statistics from 2021 (which totaled £2.4 billion), there is a 67% rise. In Nigeria, a total of N2.72 billion was lost to fraud in the first and second quarters of 2022 as revealed by Tunji (2023). He disclosed further, that there was a total of 67,878 cases of fraud recorded within the period. Website phishing poses a significant threat to online security, with assailants constantly adapting their methods to deceive users and capture sensitive data. Traditional methods of phishing detection are frequently unable to keep up with these sophisticated assaults, resulting in an increasing number of successful phishing incidents. Although there are numerous and impressive anti-phishing approaches and solutions available, the rising occurrences of phishing-related crimes can be attributed to cybercriminals' dynamic use of techniques that mimic those powered by conventional phishing detection solutions (Do *et al.,* 2022).

6. STRATEGIES FOR MITIGATING THE GLOBAL MENACE: A COMPREHENSIVE ANALYSIS

Addressing the worldwide issue of phishing necessitates the implementation of a comprehensive approach that encompasses various dimensions, including technical, educational, and organizational measures. Ajayi *et al*. (2022) and Wang (2023), outlined several essential strategies for effectively mitigating phishing attacks:

i. Implementing sophisticated and real-time phishing detection tools is essential. These tools employ machine learning algorithms and behavioral analysis techniques to effectively detect and classify phishing websites and emails According to Do *et al.* (2022). It is imperative to ensure the regular updating and continuous improvement of these tools to effectively adapt to the ever-evolving tactics employed in phishing activities.
ii. Promoting User Education and Awareness: The dissemination of knowledge regarding phishing threats and the advocacy of optimal practices among users is of paramount importance. It is imperative to provide users

with appropriate training to enhance their ability to identify and discern phishing emails, websites, and various forms of social engineering techniques. Organizations can regularly administer cybersecurity awareness training sessions to equip users with the necessary knowledge to effectively recognize and evade potential phishing attacks.

iii. The implementation of Multi-Factor Authentication (MFA) enhances the security measures in place to safeguard user accounts by introducing an additional layer of protection. Multi-factor authentication (MFA) serves as an effective measure against unauthorized access, particularly in scenarios where credentials have been compromised through phishing attacks. By incorporating additional authentication factors, such as the utilization of one-time codes transmitted to mobile devices, MFA significantly enhances security and mitigates the risk of unauthorized entry.

iv. Implementation of Effective Email Filtering and Spam Detection: Employ robust mechanisms for email filtering and spam detection to proactively mitigate the risk of phishing emails infiltrating users' inboxes. These systems possess the capability to detect and prevent the access of suspicious or malicious emails before any user engagement.

v. One effective strategy for enhancing online security is the implementation of web content filtering, which involves the restriction of access to websites that are identified as being involved in phishing activities or hosting malicious content. This proactive measure aids in the prevention of users unintentionally accessing phishing websites.

vi. To mitigate the risk of phishing attacks, developers and organizations must adhere to secure coding practices, which serve to minimize vulnerabilities that could potentially be exploited by malicious actors. Regular security assessments and code reviews play a crucial role in the identification and remediation of potential vulnerabilities.

vii. The facilitation of collaborative partnerships among organizations, cybersecurity experts, and government agencies plays a crucial role in fostering the exchange of threat intelligence and best practices. The dissemination of knowledge regarding emerging phishing threats and attack methodologies can facilitate a more prompt and effective response, thereby enhancing overall security measures.

viii. The implementation of a delineated incident response plan facilitates the expeditious and efficient response of organizations to phishing attacks. The proposed plan ought to encompass protocols for the documentation and notification of occurrences, the implementation of measures to mitigate the impact of an attack, and the execution of a comprehensive analysis following the incident to proactively avert future recurrences.

ix. Continuous monitoring and analysis are essential practices for organizations to proactively identify indications of phishing attacks. This involves the ongoing observation of network traffic, user behavior, and system logs to promptly detect any suspicious activities. The utilization of real-time analysis has the potential to effectively identify and mitigate threats promptly, thereby preventing the occurrence of substantial harm.

x. Facilitating legal and law enforcement collaboration is imperative in promoting the initiation of legal proceedings against cybercriminals engaged in phishing attacks. Collaboration with law enforcement agencies has the potential to facilitate the identification and legal pursuit of wrongdoers, thereby serving as a preventive measure against prospective assailants.

7. CONCLUSION

It is apparent that phishing attacks have emerged as a significant and pressing worldwide menace, posing considerable risks to the integrity of the digital domain and the protection of sensitive information. The escalating trends and vulnerabilities associated with phishing demand immediate attention and robust mitigation measures. By implementing collaborative efforts and adopting proactive strategies, the international community can strengthen its cybersecurity defenses and protect vital economic assets from potential compromise.

8. POTENTIAL AVENUES FOR FUTURE RESEARCH AND DEVELOPMENT.

Looking ahead, continued research and development in the field of cybersecurity are imperative to stay ahead of the evolving phishing tactics. Further exploration of advanced machine learning (ML) techniques such as Deep learning, Hybrid/ Ensemble ML, reinforcement learning techniques and behavioral analytics may lead to even more effective phishing detection and prevention strategies (Do *et al.,* 2022). Additionally, raising awareness and promoting best practices among users will play a vital role in fortifying cyberspace against the global menace of phishing. In light of the ongoing evolution of the digital landscape, it is imperative to recognize that effectively addressing the challenges presented by phishing attacks necessitates a collaborative endeavor involving all relevant parties. By implementing proactive measures at present, it is possible to protect the cyberspace and foster a safer and more secure online environment for everyone.

REFERENCES

1. Adebowale, M. A. (2020). *An Intelligent Phishing Detection and Protection Scheme using a fusion of Images, Frames, and Text* (Doctoral dissertation, Anglia Ruskin University).
2. AJAYI, W., Ibeto, O., Olomola, T., & Madewa, M. (2022). ANALYSIS OF MODERN CYBERSECURITY THREAT TECHNIQUES ANDAVAILABLE MITIGATING METHODS. *International Journal of Advanced Research in Computer Science*, *13*(2).
3. Akande, O. N., Akande, H. B., Kayode, A. A., Adeyinka, A. A., Olaiya, F., Oluwadara, G. (2022). Development of a Real-Time Smishing Detection Mobile Application using Rule Based Techniques. *Procedia Computer Science*, *199*, 95-102. https://doi.org/10.1016/j.procs.2022.01.012
4. Aldo Tenis, A., Santhosh, R. (2022). Challenges and Security Issues of Online Social Networks (OSN). *Mobile Computing and Sustainable Informatics*, 703-709. https://doi.org/10.1007/978-981-16-1866-6_53
5. Alharbi, A., Alotaibi, A., Alghofaili, L., Alsalamah, M., Alwasil, N., Elkhediri, S. (2022, January). Security in social-media: Awareness of Phishing attacks techniques and countermeasures. In *2022 2nd International Conference on Computing and Information Technology (ICCIT)* (pp. 10-16). IEEE.
6. Alkhalil, Z., Hewage, C., Nawaf, L., Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.
7. APWG (2022) *Unifying the Global Response to Cybercrime* [Online], Washington, D.C, USA: Anti-Phishing Working Group. Available at: https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf
8. Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers & Electrical Engineering*, *96*, 107546.
9. Bleach T. (2023). UK Residents Lost £4billion to Fraudsters in 2022 Alone. Published 2nd February 2023, Accessed 20th March 2023, available: https://thefintechtimes.com/money-co-uk-uk-lost-4billion-to-fraudsters-in-2022/#:~:text=A%20total%20of%20%C2%A34billion,of%20fraud%20throughout%20the%20year
10. Busari, B. (2023). Americans lost over $10bn to internet scams in 2022 – FBI. Published 15th March 2023, Accessed 20th March 2023, available: https://www.vanguardngr.com/2023/03/americans-lost-over-10bn-to-internet-scams-in-2022-fbi/#:~:text=The%20most%20highly%20reported%20crimes,2022%2C%20according%20to%20the%20Bureau

11. Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., Shukla, S. (2022). Applications of deep learning for phishing detection: a systematic literature review. *Knowledge and Information Systems*, 1-44. https://doi.org/10.1007/s10115-022-01672-x
12. Chanti, S., Chithralekha, T. (2022). A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, *9*(89), 446.
13. Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., Fujita, H. (2022). Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions. *IEEE Access*. doi: 10.1109/ACCESS.2022.3151903.
14. Dutta AK (2021) Detecting phishing websites using machine learning technique. PLoS ONE 16(10): e0258361. https://doi.org/10.1371/journal.pone.0258361
15. Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., ... Benavides, E. (2022). Impact of Social Engineering Attacks: A Literature Review. *Developments and Advances in Defense and Security*, 25-35. https://doi.org/10.1007/978-981-16-4884-7_3
16. Gautam, H., Kumar, V., Sharma, V. (2021). Phishing Prevention Techniques: Past, Present and Future. In *Proceedings of Integrated Intelligence Enable Networks and Computing: IIENC 2020* (pp. 83-98). Springer Singapore
17. Ghelani, D., Hua, T. K., Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.
18. *Global Social Media Statistics — DataReportal – Global Digital Insights*. (n.d.). DataReportal – Global Digital Insights. https://datareportal.com/social-media-users
19. Jain, A. K., Gupta, B. B. (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527-565. : https://doi.org/10.1080/17517575.2021.1896786
20. Mbona, I., Eloff, J. H. (2022). Feature selection using Benford's law to support detection of malicious social media bots. *Information Sciences*, *582*, 369-381. https://doi.org/10.1016/j.ins.2021.09.038
21. McNealy, J. E. (2022). Platforms as phish farms: Deceptive social engineering at scale. *New Media Society*, *24*(7), 1677-1694.
22. Mensah, R., Ennin, D. (2022). Cybercrime in Ghana and Victims Accounts. *Available at SSRN 4172385*.
23. Minocha, S., Singh, B. (2022). A novel phishing detection system using binary modified equilibrium optimizer for feature selection. *Computers Electrical Engineering*, *98*, 107689. https://doi.org/10.1016/j.compeleceng.2022.107689
24. Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, 1-10. https://doi.org/10.1007/s10586-022-03604-4
25. Potteiger, B., Dubey, A., Cai, F., Koutsoukos, X., & Zhang, Z. (2022). Moving target defense for the security and resilience of mixed time and event triggered cyber–physical systems. *Journal of Systems Architecture*, *125*, 102420.
26. Sahoo, S. R., Gupta, B. B., Peraković, D., Peñalvo, F. J. G., Cvitić, I. (2022). Spammer Detection Approaches in Online Social Network (OSNs): A Survey. In *Sustainable Management of Manufacturing Systems in Industry 4.0* (pp. 159-180). Springer, Cham. DOI:10.1007/978-3-030-90462-3_11
27. Salloum, S., Gaber, T., Vadera, S., Sharan, K. (2022). A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques. *IEEE Access*. doi: 10.1109/ACCESS.2022.3183083.

28. Singh, U., & Singh, P. (2022). Managing Cyber Security. *Journal of Management and Service Science (JMSS)*, *2*(1), 1-10.
29. Sonowal, G. (2022). Types of Phishing. In: Phishing and Communication Channels. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-7744-7_2
30. Thankappan, M., Rifà-Pous, H., Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Systems with Applications*, 118401.
31. Tunji S. (2023). Bank customers lose N2.72bn to fraudsters. Published 29th January 2023, Accessed 29th March 2023, available: https://punchng.com/bank-customers-lose-n2-72bn-to-fraudsters- report
32. Wang, Y. (2023). Mitigating phishing threats (Doctoral dissertation, The University of St Andrews).