SAFEGUARDING SOCIAL MEDIA: STRATEGIES TO COUNTER PHISHING THREATS

Sefiya Aramide Galadima, Department of Computer Science & Engineering[1,2]
Vivekananda Global University, Jaipur, India
Dr. Manish Shrivastava, Department of Computer Science & Engineering[1,2]
Vivekananda Global University Jaipur, India
Dr. Gunikhan Sonowal, Department of Computer Science Galgotias University
Greater Noida, India
Ibrahim Saleh, Department of Development Studies Vivekananda Global University
Jaipur, India

ABSTRACT:

Social media phishing, a growing threat that exploits the interactive nature of online platforms to deceive users into divulging sensitive information. The introduction outlines the significance of social media as a communication medium and its associated vulnerabilities, setting the stage for an in-depth analysis of phishing attacks. This paper categorizes social media phishing, also known as Angler Phishing, into various forms, including account takeovers, impersonation, fraudulent schemes, and malware distribution, highlighting the unique challenges posed by these tactics.Subsequent sections investigates the tools and techniques employed by cybercriminals, particularly focusing on information gathering methods such as Open-Source Intelligence (OSINT) frameworks, which facilitate the collection of publicly available data for malicious purposes. The discussion emphasizes the role of sock puppet accounts in enhancing the credibility of phishing attempts, further complicating detection efforts.The paper also evaluates existing countermeasures against social media phishing, advocating for user education, the implementation of security features, and the establishment of effective reporting mechanisms. It underscores the importance of continuous monitoring and the integration of advanced technologies, including machine learning, to adapt to the evolving landscape of phishing threats.In conclusion, this paper emphasizes the need for a collaborative approach involving users, social media platforms, and cybersecurity experts to combat social media phishing effectively. By fostering awareness and employing comprehensive strategies, stakeholders can enhance the security of digital communication and protect users from the risks associated with phishing attacks.

Keywords-Social Media, Phishing, Angler Phishing, Cybersecurity, Machine Learning, Sock Puppet, Machine Learning, User Education, Information Gathering, Open-Source Intelligence (OSINT)

INTRODUCTION:

Social media platforms are digital technologies that enable the generation and dissemination of information, ideas, and content through virtual networks and communities. They also serve as a medium for electronic communication, facilitating the creation of online social networks[1].

They have revolutionized communication, allowing individuals and organizations to connect, share information, and engage with a global audience. However, this rapid growth has also created new vulnerabilities, one of which is phishing. Phishing attacks on social media platforms have become increasingly sophisticated and prevalent, posing a significant threat to users' privacy and security. These platforms often serve as a primary source of communication and information, making them attractive targets for scammers. By exploiting the trust and familiarity that users have with these platforms, attackers can deceive individuals into divulging sensitive personal information, such as login credentials, financial details, or even personal identification. The interconnected nature of social media networks further amplifies the risk, as a compromised account can potentially lead to the compromise of other accounts within the user's social graph.

Social media encompasses a wide range of activities, from personal interactions to professional networking. The vast amount of information shared on these platforms has created opportunities for targeted spear phishing attacks, leading to the emergence of a distinct category known as social media phishing[2].

This paper examines the significant threat posed by social media phishing attacks and the shortage of scholarly investigation into countermeasures. Section II analyzes the vulnerabilities exploited by threat actors on these platforms. Section III explores the tools utilized by phishers to deceive users. Section IV reviews existing countermeasures and proposed mitigation strategies. Finally, Section V concludes the paper.

SOCIAL MEDIA PHISHING :

Social media phishing, also known as Angler Phishing, capitalizes on the interactivity of online platforms. Social networking platforms have emerged as a preferred channel for cybercriminals to launch phishing attacks. These attacks can manifest in various forms, including account takeovers, impersonation, fraudulent schemes, and malware distribution[3], unlike traditional phishing methods, attackers weaponize the vast landscape of user-generated content (articles, images, videos, personal details) and the sheer diversity of platforms themselves. This very ease of connection, a cornerstone benefit for both individuals and organizations, transforms into a critical vulnerability. Blancaflor et. al.,[4] concluded that users were more susceptible to social media phishing compared to other forms such as SMS and Email Phishing.

For Example, Empirical data indicates that social media platforms were significantly more lucrative for scammers in 2021 compared to other communication channels.In 2021, social media scams resulted in losses exceeding $770 million for over 95,000 individuals. These losses constituted approximately 25% of all reported fraud losses that year, marking a substantial 18-fold increase from 2017 levels. While all age groups experienced an uptick in social media fraud reports, individuals aged 18-39 were significantly more vulnerable to these scams compared to older adults[5].

Personal information readily available on social media profiles fuels highly targeted spear phishing attacks. Malicious actors exploit this accessibility by luring victims with seemingly attractive links, promising exclusive content, fraudulent discounts, or even brand engagement. Within online environments, certain individuals may employ multiple usernames or engage in fake identity practices, such as creating ‘sock puppet’ accounts. These fabricated online personas are often used to manipulate online discussions or feign widespread support for products, services, or individuals. By impersonating others, these accounts aim to deceive online communities[6].

In the realm of brand impersonation, cybercriminals create sock puppet accounts that mimic legitimate entities, further obfuscating their malicious intent. Unsuspecting victims, deceived by the perceived authenticity, fall prey to these tactics, unwillingly surrendering sensitive information that grants attackers unauthorized access.

Sock puppet accounts are a fictitious online identities used for deceptive purposes on social media platforms[7]. These accounts can impersonate real people, fictional characters, or established brands. While some sock puppets are easily identifiable due to their overtly non-human personas, others are meticulously crafted to mimic legitimate users or brands[8]. These deceptive accounts empower fraudsters to engage in criminal activity on social media. In some cases, sock puppets operate for extended periods, accumulating posts and interactions to cultivate an illusion of legitimacy, making them even more deceptive to unsuspecting victims. These sock puppet accounts can be created on any form of public platform even unsuspecting ones like random groups on the internet.

TOOLS UED IN QR CODE PHISHING :

This section aims to evaluate the technologies underlying these attacks. To achieve a successful social media phishing campaign, a combination of technological elements is essential, and this section will examine these tools in detail.

A. ***Information Gathering Tools***

Social Media Phishing relies heavily on information gathering either of an individual or a corporation, there are various tools that aid in the gathering of these information. Such as

- OSINT Framework: Open-Source Intelligence (OSINT) refers to the systematic collection and analysis of publicly available information from overt sources, such as social media, news outlets, and government databases, to generate actionable insights about individuals or organizations. The OSINT framework[9] functions as a comprehensive toolkit, facilitating the collection and analysis of this publicly accessible data. This framework finds applications in various fields, including intelligence gathering, cybersecurity, investigations, threat monitoring, and even phishing countermeasures. Notably, some tools employed in anti-phishing efforts can also be utilized for malicious purposes. The OSINT framework addresses this challenge by streamlining information gathering. It provides a centralized platform with categorized tools, readily accessible even for novice users, enabling efficient collection of relevant data, phishers take advantage of this accessibility to gather information about their victim.
- Maltego: Maltego is a proprietary software application employed in open-source intelligence (OSINT) and forensic investigations. It specializes in facilitating the discovery and linkage of data from publicly available sources. This functionality is achieved through a library of pre-defined transformationsand the visualization of the information in a graph format. Maltego offers real-time data mining capabilities, presenting the collected information in a graphical user interface that allows for the clear identification of relationships between entities. Notably, the software focuses on analyzing connections within publicly accessible data pertaining to individuals, organizations, and infrastructure[10].

B. ***Phishing Kits***

While a significant portion of phishing kits are intended for educational simulations to raise awareness about phishing tactics, malicious actors have developed methods to exploit these very tools for real-world phishing attacks, targeting unsuspecting individuals. Phishing kits are a pre-packaged set of tools and resources that enable attackers launch phishing campaign with ease, these kits include fake website templates, email scripts, social media phishing templates, and automated tools for deploying and managing phishing attacks from start to finish. Phishing kits facilitate the manipulation of individuals into divulging confidential information. These tools include information gathering tools, email spoofing, credential harvesting, personalized attack vectors and scripts, website cloning. There are various phishing kits applicable to various communication mediums.

- SEToolkit: The Social-Engineer Toolkit (SET) [11] is an open-source framework designed for penetration testing and social engineering. It is one of the most advanced tools for executing social engineering attacks, providing a variety of attack vectors and techniques to trick users into divulging sensitive information [12]. It was designed by David Kennedy and developed by Trusted Sec [13]. The Social Engineering Toolkit (SET) offers a comprehensive suite of functionalities accessible through a user-friendly menu. These functionalities encompass social engineering attack vectors, penetration testing tools, and the integration of third-party modules.SET is used by attackers to harvest credentials through phishing attacks, primarily targeting social media accounts. These tools can aid in finding personal information through emails or social media profiles. The attacker typically uses social media platforms to contact victims, by either sending private messages or replying to public messages with information containing a link either disguised with an attractive image or with a promise of something to lure the victim. Clicking the link redirects the victim to a carefully crafted fake website that closely resembles the legitimate login page of the targeted social media platform. Convincing wording further deceives the victim, who unknowingly enters their login credentials. SET offers various functionalities to create these fake sites.

- Zphisher: Zphisher [14] is an open-source phishing tool [15], unlike Social Engineering Toolkit (SET) it is easier to understand and use. Geared towards educational purposes, penetration testing, and ethical hacking, Zphisher offers a simple user interface and a broad selection of pre-designed phishing templates. This extensive collection, encompassing various social media platforms like Facebook, Twitter, and Instagram, facilitates the simulation of diverse phishing attacks with relative ease. Zphisher organizes the execution of phishing attacks through automation [16], encompassing the creation of phishing pages, server hosting (local or external), and captured credential management. This automation significantly reduces the time and effort required by the attacker.

*C. **URL Shorteners and Redirection Services***

URL shortening services address the challenge of long website addresses by generating compact aliases. These shortened URLs retain the functionality of their original counterparts, directing users to the intended destination upon clicking. This technique proves particularly valuable for recommending links within environments with limited character space, such as social media platforms, short messaging services, mobile phones, and microblogging platforms [17].URL shortening and redirection services play a significant role in social media phishing by masking the true destination of a URL, making it easier for attackers to deceive targets. These services can transform long, suspicious URLs into short links, thereby increasing the likelihood that users will click on them. URL shortening services address the challenge of exchanging lengthy URLs within environments with limited character space. With compelling social engineering tactics, shortened URLs can be easily embedded in phishing messages sent via social media, making the message appear more credible.There are various platforms that aid in the creation of short URLs which criminal actors employ in phishing unsuspecting individuals.

- TinyURL:TinyURL addresses the challenge of long website addresses. It condenses long URLs into concise, manageable, user-friendly links, facilitating easier sharing and management. TinyURL also provides permanent short links, ensuring that they don’t expire. These functionalities make TinyURL a popular choice within marketing, social media, and content sharing spheres. It’s also able to track link analytics in its paid version and also provide bulk short URLs. For example, along URL https://securelist.com/phishing-kit-market-whats-inside-off-the-shelf-phishing-packages/106149/ becomes https://tinyurl.com/5n9aby57, the first URL containing 89 characters and clearly reading out the destination, becomes a 24 character URL with a destination that isn’t fully distinguishable by just looking at the URL. Many phishers take advantage of such services as they lead to the same destination but become ambiguous and victims are unable to predict where they are being redirected to unless such links are clicked upon.

COUNTERMEASURES:

The paper [18]proposes a model called PhishAri, which is designed for automatic real-time phishing detection on Twitter. The model utilizes various machine learning classification algorithms to evaluate and classify tweets as either 'phishing' or 'safe.' The authors conducted a performance evaluation of different algorithms and ultimately developed a classification model that incorporates features specific to URLs and Twitter.The PhishAri model has limitations, including its current inability to detect phishing tweets from private Twitter accounts, as it relies on public user data. Additionally, while it achieves a high accuracy of 92.52%, it does not reach 100%, leaving room for false negatives. The model's performance can also be affected by external factors such as the response times of the Twitter API and WHOIS repository, as well as internet bandwidth.

Faris et. al[19]discuss two primary approaches for phishing web page detection: a rule-based method and several machine learning models. The rule-based method employs predefined rules to efficiently identify phishing sites, emphasizing speed and accuracy. In contrast, the authors tested three machine learning algorithms, Support Vector Machine (SVM), Decision Tree, and Gaussian Naïve Bayes (GNB), to evaluate their effectiveness in improving detection accuracy. While these machine learning models achieved high accuracy, they did not significantly outperform the rule-based method and required more computational resources. The authors concluded that a combination of URL and HTML features, along with the rule-based approach, offers a more effective solution for phishing detection, balancing efficiency and performance.The paper identifies several limitations of the models discussed, particularly the machine learning approaches, which, despite achieving high accuracy, do not significantly improve upon the rule-based method. These models require substantial computational resources for training and application, making them less efficient. Additionally, the reliance on feature selection is critical, as the effectiveness of both machine learning and rule-based methods hinges on the quality of the features used.

The paper presents an integrated machine learning model for URL phishing detection, highlighting several key techniques. It employs Naïve Bayes and Support Vector Machine classifiers for initial detection tasks. Additionally, it utilizes Artificial Neural Networks (ANN), specifically Feed-Forward Backpropagation and Levenberg-Marquardt algorithms, for classifying URLs as phishing or legitimate. The study also incorporates Fuzzy Inference Systems (FIS), particularly the Mamdani method, to enhance detection through social facet filtering. Furthermore, it discusses the application of rule-based methods and various machine learning techniques, including logistic regression, Markov models, decision trees, and random forests, which are prevalent in the industry for identifying phishing attacks. This comprehensive approach aims to improve the accuracy and effectiveness of phishing detection systems in real-time scenariosThe model presented in the paper has several limitations, including its reliance on predefined heuristics and features, which may not capture all phishing tactics due to the evolving nature of phishing attacks. Additionally, the performance of the model can be affected by the quality and diversity of the training data, potentially leading to false positives or negatives. The complexity of the model may also pose challenges in real-time implementation, as it requires significant computational resources and may not adapt quickly to new phishing techniques without regular updates [20].

CONCLUSION :

In conclusion, social media phishing represents a significant and evolving threat in the digital landscape, capitalizing on the trust and interactivity inherent in these platforms. As cybercriminals continue to refine their tactics, it is imperative for both users and social media companies to adopt proactive measures to combat these threats. This paper has highlighted the various forms of phishing attacks, including account takeovers, impersonation, and malware distribution, which exploit the vast amounts of personal information shared on social media.

To effectively mitigate the risks associated with social media phishing, a multifaceted approach is necessary. User education and awareness campaigns are essential to empower individuals to recognize and respond to phishing attempts. Additionally, the implementation of robust security features, such as multi-factor authentication and effective reporting mechanisms, can significantly enhance user protection. Continuous monitoring and the integration of advanced technologies, including machine learning, will further bolster defenses against emerging phishing tactics.

Ultimately, the fight against social media phishing requires collaboration between users, social media platforms, and cybersecurity experts. By fostering a culture of vigilance and employing comprehensive countermeasures, we can create a safer online environment that protects users' privacy and security in an increasingly interconnected world. As the landscape of social media continues to evolve, ongoing research and adaptation will be crucial in staying ahead of cyber threats and ensuring the integrity of digital communication.

REFERENCES :

[1] Harsha, “Project Report on ‘Social Media,’” Master of Commerce, Punjabi University, Patiala, 2020.

[2] T. Aichner, M. Grünfelder, O. Maurer, and D. Jegeni, “Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019,” *CyberpsycholBehav Soc Netw*, vol. 24, no. 4, pp. 215–222, Apr. 2021, doi: 10.1089/cyber.2020.0134.

[3] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Front Comput Sci*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[4] E. B. Blancaflor, A. B. Alfonso, K. Banganay, G. Dela Cruz, K. Fernandez, and S. Santos, “Let’s go phishing: A phishing awareness campaign using smishing, email phishing, and social media phishing tools,” in *Proceedings of the international conference on industrial engineering and operations management*, 2021.

[5] E. Fletcher, “Social media a gold mine for scammers in 2021,” FTC - Consumer Protection. Accessed: Feb. 25, 2022. [Online]. Available: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021

[6] Z. Bu, Z. Xia, and J. Wang, “A sock puppet detection algorithm on virtual spaces,” *Knowl Based Syst*, vol. 37, pp. 366–377, Jan. 2013, doi: 10.1016/j.knosys.2012.08.016.

[7] X. Zheng, Y. M. Lai, K. P. Chow, L. C. K. Hui, and S. M. Yiu, “Sockpuppet Detection in Online Discussion Forums,” in *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE, Oct. 2011, pp. 374–377. doi: 10.1109/IIHMSP.2011.69.

[8] F. Sullivan, “The Utilization of Sock Puppets in Cyber Intelligence Operation,” Utica College, New York, 2014.

[9] J. Nordine, “Osint Framework,” 2016.

[10] K. Schwarz and R. Creutzburg, “Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego,” *Electronic Imaging*, vol. 33, no. 3, pp. 45-1-45–23, Jun. 2021, doi: 10.2352/ISSN.2470-1173.2021.3.MOBMU-045.

[11] D. Kennedy, “Social Engineering Toolkit.”

[12] N. Pavković and L. Perkov, “Social Engineering Toolkit — A systematic approach to social engineering,” in *2011 Proceedings of the 34th International Convention MIPRO*, 2011, pp. 1485–1489.

[13] G. Sonowal, *Phishing and Communication Channels*. Berkeley, CA: Apress, 2022. doi: 10.1007/978-1-4842-7744-7.

[14] T. Rayat and htr-tech, “zphisher,” 2023, *github*: 2.3.5. Accessed: Mar. 20, 2023. [Online]. Available: https://github.com/htr-tech/zphisher

[15] F. Castaño, E. F. Fernañdez, R. Alaiz-Rodríguez, and E. Alegre, “PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification,” *IEEE Access*, vol. 11, pp. 40779–40789, 2023, doi: 10.1109/ACCESS.2023.3268027.

[16] H. McCalley, B. Wardman, and G. Warner, “Analysis of back-doored phishing kits,” in *Advances in Digital Forensics VII: 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31–February 2, 2011, Revised Selected Papers 7*, Springer, 2011, pp. 155–168.

[17] “An efficient Security Solution for Dealing with Shortened URL Analysis,” in *Proceedings of the 8th International Workshop on Security in Information Systems*, SciTePress - Science and and Technology Publications, 2011, pp. 70–79. doi: 10.5220/0003579800700079.

[18] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, “PhishAri: Automatic realtime phishing detection on twitter,” in *2012 eCrime Researchers Summit*, IEEE, 2012, pp. 1–12.

[19] H. Faris and S. Yazid, “Phishing web page detection methods: URL and HTML features detection,” in *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, IEEE, 2021, pp. 167–171.

[20] H. J. Parker and S. V Flowerday, “Contributing factors to increased susceptibility to social media phishing attacks,” *S Afr J Inf Manag*, vol. 22, no. 1, pp. 1–10, 2020.