Solutions to Phishing Attacks

Sem Pisey **Tha Rithyvuth**

School of Computer Science, Cambodia Academy of Digital Technology
sempisey1414@gmail.com tharithyvuth7@gmail.com

Abstract

Phishing attacks have emerged as a pervasive and persistent threat in the digital era, targeting individuals, organizations, and even governments with fraudulent attempts to deceive and extract sensitive information. These attacks, often disguised as legitimate communications or websites, can lead to severe consequences such as identity theft, financial loss, and reputational damage. To mitigate these risks, a range of countermeasures have been developed. User education plays a critical role in raising awareness about the threat of phishing and empowering individuals to recognize and report phishing attempts. Technological advancements have led to the development of sophisticated anti-phishing tools, including email filters, web filters, and browser extensions, which employ algorithms and heuristics to detect and block phishing attempts. Additionally, policy frameworks have been established to deter attackers through legal and regulatory measures. However, phishing attacks continue to evolve, necessitating a multi-faceted approach that combines user education, technological innovation, and policy enforcement. Continued research, collaboration, and vigilance are essential to stay one step ahead of attackers and protect the digital landscape from the pervasive and evolving threat of phishing attacks, ensuring a safer and more secure environment for individuals, organizations, and society as a whole.

1 General Introduction

In today's digital landscape, the Internet plays an increasingly vital role in online commerce and business activities. However, the inadequate security measures in Internet technology, coupled with the potential for significant financial gains, serve as strong motivations for attackers. As online services gain popularity, Internet security risks have experienced an exponential increase. These risks encompass any malicious and undesirable events that can occur within various applications, which may have vulnerabilities that facilitate the realization of threats. Such risks can lead to the interception and hijacking of sensitive personal data over unprotected Internet connections. The focus of this paper centers around website phishing.

Website phishing attacks typically initiate with an email that arrives in the user's mailbox, masquerading as a seemingly legitimate and well-known entity. Often, these emails claim urgent action is required from the user and direct them to a deceptive web page that solicits private information, such as passwords. However, it is important to note that these web pages are not associated with the actual bank or legitimate entity.

One common characteristic shared by all phishing sites is their malicious intent to deceive users into believing that they are legitimate websites. As a result, the detection of phishing pages essentially becomes an authentication challenge between users and servers. In web applications, user authentication is typically required before granting access to requested resources. The level of user authentication can vary, ranging from simple to robust, depending on the security policies implemented for the service or resource. For instance, a web forum may only necessitate a plain-text password-based authentication, while online banking platforms require the utilization of certificates and public key infrastructures.

The structure of this paper is organized as follows. In Section 2, focuses on literature review which is about academic papers, and publications related to phishing attacks. Section 3 focuses on the solution of phishing attacks in-

cluding preventing phishing, detecting phishing and stakeholder training. In section 4 is the recommendation for future work based on the current state of research. Lastly, concluding remarks are provided to summarize the key findings.

2 Literature Review

Phishing attacks have become a pervasive and ever-evolving threat in the digital landscape, targeting individuals, businesses, and organizations of all sizes. These attacks aim to deceive users into providing sensitive information such as usernames, passwords, and credit card details through fraudulent websites and emails. To combat this growing menace, extensive research has been conducted to develop effective anti-phishing solutions that can detect and prevent these attacks, safeguarding users' personal and financial information.

One notable contribution in the field of anti-phishing solutions is the work of E. Kirda and C. Kruegel, who introduced Antiphish [1]. Their research focused on developing a tool that can detect and block access to phishing websites. Antiphish utilizes advanced algorithms and analysis techniques to identify fraudulent sites accurately. By proactively blocking access to these malicious websites, Antiphish provides users with an additional layer of protection against phishing attacks. The authors evaluated the effectiveness of their tool through real-world phishing attack scenarios, demonstrating its ability to mitigate risks and enhance user security.

Building upon their previous research, E. Kirda and C. Kruegel further explored the topic of protecting users against phishing attacks in their publication in The Computer Journal [2]. They addressed the challenges posed by these attacks and proposed a defense mechanism centered around detecting and blocking phishing websites. Their approach involved comprehensive website analysis and the use of intelligent algorithms to identify fraudulent sites with a high degree of accuracy. The authors collected empirical evidence through extensive datasets of real-world phishing attacks, validating the effectiveness of their proposed approach. This research contributes to the ongoing efforts to develop robust anti-phishing solutions and enhance the overall security posture against these attacks.

In a study by S.H. Apandi, J. Sallim, and R.M. Sidek [3], the authors provided a comprehensive review of different types of anti-phishing solutions. They classified phishing attacks into two categories: social engineering and malware-based phishing attacks. The paper delved into two primary types of anti-phishing solutions: phishing prevention and phishing detection. While prevention measures aim to minimize the occurrence of phishing attacks, detection techniques focus on identifying and mitigating phishing websites. The authors emphasized the significance of phishing detection, highlighting the usefulness of academic phishing detection/classification schemes in identifying and thwarting phishing attempts. They also suggested further research in leveraging deep learning techniques to enhance the accuracy of phishing detection, thereby improving the overall effectiveness of anti-phishing solutions.

Another aspect of combating phishing attacks involves preventive techniques and countermeasures. M. Badra, S. El-Sawda, and I. Hajjeh [4] explored this topic in their paper presented at the 3rd International ICST Conference on Mobile Multimedia Communications. They provided an overview of various techniques employed by attackers and discussed the impact of phishing attacks on individuals and organizations. The authors proposed a range of preventive measures and countermeasures to mitigate the risks associated with phishing attacks. These measures included user education and awareness programs, as well as the implementation of technical controls such as email filters, firewalls, and secure communication protocols. By promoting user education and implementing preventive measures, organizations can significantly reduce the likelihood of successful phishing attacks.

Similarly, M. Adil, R. Khan, and M.A.N.U. Ghani [5] focused on preventive techniques in their paper titled "Preventive techniques of phishing attacks in networks." Presented at the 2020 3rd International Conference on Advancements in Computational Sciences, their research explored authentication, encryp-

tion, and user awareness as preventive measures to enhance network security and thwart phishing attacks. The authors emphasized the importance of implementing robust authentication mechanisms and encryption protocols to ensure secure communication channels. Furthermore, they stressed the significance of user awareness programs to educate individuals about phishing techniques and empower them to identify and avoid phishing attempts effectively.

Another notable contribution in the literature is the chapter on phishing attacks and countermeasures by Zulfikar Ramzan [6], which is part of the Handbook of Information and Communication Security. Ramzan provides a comprehensive overview of phishing attacks, starting with an examination of the underlying ecosystem that enables these attacks to occur. The chapter delves into the techniques employed by phishers and sheds light on the specific brands they target, as well as the variations and adaptations of traditional phishing attacks. Furthermore, Ramzan discusses proposed countermeasures to combat phishing, evaluating their relative merits and effectiveness in countering these threats.

Another noteworthy study on the state of phishing attacks is conducted by J. Hong [7] in the Communications of the ACM. Hong's research provides valuable insights into the current landscape of phishing attacks. The paper emphasizes the tactics employed by attackers and highlights the detrimental impact of phishing attacks on both individuals and organizations. To address these challenges, Hong discusses preventive measures and countermeasures that can be employed to mitigate the risks associated with phishing. These measures include user education and awareness programs, as well as the implementation of technical controls such as email filters, firewalls, and secure communication protocols.

Overall, the reviewed literature highlights the significance of developing robust anti-phishing solutions to protect internet users from falling victim to phishing attacks. The studies discussed in this review cover a wide range of aspects related to anti-phishing solutions, including the development of specialized tools, detection algorithms, preventive measures, and user awareness programs. These research efforts collectively contribute to enhancing the knowledge and understanding of phishing attacks and provide valuable insights for mitigating the risks associated with them.

3 Solution

We propose that there are three ways in which the solution to phishing can be approached: detect phishing attacks before they reach the user, detect once the user has reached the phishing site, or train users to detect or prevent them by themselves. Each option has its own benefits and downsides, but the best method is an approach utilizing a mix of all three. Phishing is evolving every day to avoid detection and bypass these defenses, so by taking on all three we increase the chances that they will be found and stopped. Figure 2 shows our approach and the proposed anti-phishing solution framework.

Step 1 – Prevent phishing: Phishing can be stopped before it reaches the user either by blacklisting or blocking phishing sites or by filtering out phishing emails. The first method is carried out by looking at the URLs and the sites that they claim to be, either manually or automated through the use of machine learning. Although this may catch some sites, there is little hope of catching all of them, since a phisher can easily just make a new site once one is taken down.

The second method can be seen as more effective, because if successfully carried out it will stop the user from ever being exposed to the link for the phishing sites. There are many successful spam filters used by email servers, but few phishing filters due to its more complex nature. Filters for phishing are being designed using machine learning techniques as well. In ‘Classification of Phishing Email Using Random Forest Machine Learning Technique’ the authors discuss the characteristics used for classifying phishing emails. Some examples of these are the use of URLs containing an IP address,

non-matching ‘href’ attributes and link text, the number of dots contained within a domain name and checking the domain names against the email sender. There are also a few simple keywords that the pro- gram looks for, such as ‘urgent’, ‘update’, ‘suspend’ and ‘verify’. The result of their experiment showed an accuracy of 99.7% with a very small false positive rate of about 0.06%. This indicates this method is a very effective method of combating phishing, even more so since the machine learning technique can evolve with the evolving phishing attacks.

Step 2 – Detect phishing: Since attackers use sophisticated methods to ensure that phishing emails and websites reach vulnerable users, a method is sought to either identify possible phishing sites or indicate to the user to avoid malicious sites (or avoid giving malicious information in these emails or sites) even if they have received (and opened) a malicious email. Many web browsers already have defenses in place against phishing sites, which will either have a passive indicator or an active indicator. Active indicators will have pop-up windows with a warning that the site they are on is a suspected forgery or that it is not considered safe, while passive indicators do not interrupt the user’s task.

As expected, many users would ignore or simply not notice the passive indicator and active indicators were much more effective. However, some users trust that the sites they are going to are what they expect because they were originally sites they trusted. To combat this, applying a verification system for sites that are trusted and secure can be helpful. If users see that verification every time they visit the genuine site, they are more likely to notice its absence on the fake website. The provision of the certified identification and branding attracts the eye and helps assure the user that they are on the correct site.

Step 3 – Stakeholder training: Training users to avoid falling for phishing scams is the third approach in our solution methodology. Most existing general phishing training is broad and does not combat the current more advanced phishing attacks, plus it depends on users actually engaging with and reading the material. Emailing warnings or material about phishing generally does not work because most users have been conditioned to disregard such emails and believe that they know how to protect themselves.

In our solution, we propose anti-phishing training methods using games or embedding training systems into an email server. Researchers are working on such games. For example, one of the most successful examples of the game format is ‘Anti-Phishing Phil’, a micro game that helps teach users to identify suspicious URLs and other components of phishing scams. This approach is both engaging for the user as well as informative, but users must still go to this program for themselves.

The other method, embedded training, can be useful because by sending mock phishing emails, users who are not trained in avoiding phishing scams will be trained by default. In the report ‘Protecting People from Phishing: the design and evaluation of an embedded training email system’, the authors outline a system that would send mock phishing emails which, if users opened and followed the link, would direct them to a page notifying them what was wrong with the email and what they should look for in the future to avoid being phished. Another approach was to use a comic to outline some key tips to help users avoid compromising their personal information. Both groups performed better than the control group, which only received security notice emails. This is a useful method because if the user is using the email server and clicking on the bait emails, then they will encounter the training email and become more aware of the risks, turning a premium phishing victim into an educated user.

4 Recommendations for future work

Phishing is increasing in complexity and is becoming harder to identify for cyber-security professionals. On the other hand, phishing is also becoming more complicated for attackers due to the increase in online security in recent years. Phishing is also getting more complicated for victims because new methods of attack make it harder for the layperson to distinguish phishing activity from normal activity.

We believe that the best defense to protect against phishing on a widespread scale would be to incorporate the pro- posed anti-phishing solution framework described in the previous section into email provider servers, such as Gmail, Yahoo and Hotmail. This would ensure that even those not experienced with computers and phishing risks are still protected at the most basic level. It would be even more effective if these servers also incorporated embedded training systems into their email services, because then the users will become more educated on how to protect themselves in the future, which will lead to a society of aware users and make it very difficult for phishers to successfully launch attacks.

5 Conclusion

Phishing is becoming an ever-growing threat to users as the attacks evolve and become more difficult to distinguish. The criminals who carry out these attacks are increasingly hard to catch. To combat these challenges, we have proposed a three-pronged approach. The use of a filtration system helps lessen the number of phishing emails that reach the user, decreasing the chances that they will be phished. The user interface model provides users with warnings when the site they are visiting is not trusted, therefore defending against the chance that a convincing email has led them to a phishing site. Finally, by engaging users with educative games or embedded training, the users themselves can start to practice methods of preventing phishing.

Even though attackers keep updating phishing tactics and it's becoming a more complex task to prevent and detect phishing, staying up to date with machine learning-based automated defenses in these three categories in our proposed solution approach will be able to help keep phishing under control.

References

[1] E. Kirda and C. Kruegel, "Protecting users against phishing attacks with antiphish," *29th Annual International Computer Software and Applications Conference (COMPSAC'05)*, pp. 517--524, 2005.

[2] E. Kirda and C. Kruegel, "Protecting users against phishing attacks," *The Computer Journal*, vol. 49, pp. 554--561, 2006.

[3] S. H. Apandi, J. Sallim and R. M. Sidek, "Types of anti-phishing solutions for phishing attack," *IOP Conference Series: Materials Science and Engineering*, vol. 769, p. 012072, 2020.

[4] M. Badra, S. El-Sawda and I. Hajjeh, "Phishing attacks and solutions," *3rd International ICST Conference on Mobile Multimedia Communications*, 2010.

[5] M. Adil, R. Khan and M. A. N. U. Ghani, "Preventive techniques of phishing attacks in networks," *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)*, pp. 1-8, 2020.

[6] Z. Ramzan, "Phishing attacks and countermeasures," *Handbook of information and communication security*, pp. 433-448, 2010.

[7] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, pp. 74-81, 2012.