International Journal of Research in Engineering, Science and Management
Volume 5, Issue 6, June 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

Applied Trends in Phishing Attacks

Dhriti Agarwal*
Student, Kirit P. Mehta School of Law, Narsee Monjee Institute of Management Studies, Mumbai, India

***Abstract*: Human workings and behaviours around the world are undergoing great modification and beneficial progress as a result of rapid and unending technological advancements. The use of technological improvement has truly redefined human efficiency, making profit centres all over the world. However, technology, like most other problems linked with great inventions, has its own drawbacks. Using ordinary technologies such as the internet, the globe is woefully connected these days. Internet connectivity comes with its own set of concerns. In this student, the researcher will conduct the necessary study and due diligence to comprehend the most prevalent practice of a new type of problem and crime, namely, cyber-based crimes. Due to advantageous economic and technological conditions, phishing scams have grown in popularity in recent years. Technical resources required to carry out phishing attacks are easily available from both public and private sources. Non-technical criminals can now access several technical resources that have been streamlined and automated. For a wider group of less sophisticated offenders, phishing becomes both economically and technically viable, which acts as a curse to the society that remains. In this paper, the researcher discusses one of the most common methods of cybercrime, phishing.**

***Keywords*: Phishing, Cybercrime, Trends, Psychology.**

1. Introduction

Earlier, phishing was commonly identified as the use of electronic mail messages that were designed to look like messages from a trusted party such as a bank or auction site or other faithful commercial organisations. These messages usually solicit the user to take some form of an action and show a sense of urgency, for example threats of account suspension, which motivates the users to take the given action.

Lately, new social engineering approaches, that deceive users, include the offer to fill out a survey for an online banking site with a monetary reward, and email messages that claim to form hotel reward clubs that ask users to verify card information that a customer may store on a website for reservation purposes. Phishing methods have evolved to become more technically deceiving to investigations and recently, the definition of phishing has grown to encompass a wider variety of crimes, both; electronic and financial. Other than the omnipresence of the aforementioned, a significant increase in malicious programs that specifically targets user account information has also been observed. These programs, once installed in the user's devices, use a variety of techniques to spy and collect more account information.

When a cybercriminal makes contact with a user via mail or phone, a cyber offence occurs. Attackers gain victims' confidence and act as agents working for consumer service, obtaining users' passwords and bank information. The criminal fetches more information about the victim by getting into their social media. Once this information is obtained, it can either be sold on the internet or the victim can be scammed further.

Attackers have choices using which they can steal data. First, from the main server, second, from the backup server, which holds a full copy of the main server, third, while the data is in transition between two points, and fourth from a web page, which shows the data to the end user. It does not matter what method is chosen as there is a great chance that the attack will go unnoticed if the information is not immediately released. Think of conventional crime versus a cybercrime. A conventional crime, robbery for example, will be immediately noticed the next time the money is counted. Stealing data is different. All the information is still on the server and it may seem untouched as there might be copies of the data made. Organisations and individuals suffer substantial losses in the form of lost customers and stolen or compromised confidential information.

2. Literature Review

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139-154.

Phishing attacks have become one of the most prominent attacks faced by internet users of any kind. Here, attackers collect sensitive data of the client by the use of spoofed emails and fake websites. This paper provides a thorough study of phishing attacks by the use of a number of literature reviews of AI techniques for the detection of cyber-attacks. It has also analysed the current practices in the area of phishing.

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.

This study, from 2021, has taken into consideration the framework that helps detect phishing attacks in order to mitigate new age cyber-attacks. Unaware and untrained users end up as the main targets for the simplest methods of stealing credentials, identities, and other personal details that are sensitive to an individual. The authors have presented a new, privacy-aware framework that helps detect attacks against

*Corresponding author: dhriti2411@gmail.com contemporary tactics to achieve the highest-level impact against unsuspecting victims and the Internet of Things and mitigate them.

Rahman, S. S. M. M., Islam, T., & Jabiullah, M. I. (2020). PhishStack: evaluation of stacked generalization in phishing URLs detection. Procedia Computer Science, 167, 2410-2418.

This study has assessed investigations on the malicious URLs sent by cyber criminals to victims. These are sent using various communication mediums. These URLs seem legitimate and genuine and according to a study conducted in June, 2018 a loss of 3 billion dollars takes place annually by phishing attacks. This is one of the main reasons why this topic is given so much importance.

Bhoopal, U. (2021). Phishing Attempts in Cyber Crime. Supremo Amicus, 24, [39]-[50].

This paper has started with looking at some vital statistics about the usage of the internet as a whole, this includes Internet Usage Patterns, Cyber Crimes falling into the broad categories of government institutions, properties and individuals and the kinds of cyber-crimes. Unlike other papers, this study has investigated and given importance to the psychological aspect of the action of cyber-crimes and has highlighted a few cases relating to the subject.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106, 1-20.

This 2018 study has analysed a survey on phishing attacks, especially its types, vectors and technical approaches. The focus is primarily on discussing these approaches and the way these are used in conducting phishing attacks. This paper has also analysed a number of papers to get a clear understanding on how phishing attacks have evolved. The dependence on anti-phishing approaches that detect phishing websites upon visiting a website is not sufficient. An anti-phishing effort is needed to curb the phishing attacks.

3. Research Objectives

The following are the research objectives of this paper:

1) To analyse common phishing techniques used by attackers.
2) To highlight the behavioural aspects behind cyber-crimes and of the ones at the risk of being attacked.
3) To place emphasis on phishing countermeasures.

4. Research Questions

The following are the research questions answered in this paper:

1) What are the phishing techniques used by attackers?
2) What is the psychology behind cyber-crimes and the response of the ones at the risk of phishing?
3) What are some common phishing countermeasures that can be used to curb it?

5. Limitations

This research paper has been limited to the journals, articles and research papers referenced at the end of the paper.

6. Research Methodology

The research work for this paper commenced with reviewing a number of journals, research papers and articles based on the current trends of phishing attacks and how they take place. Only secondary data was used in this study and the material was collected from the internet.

7. Findings

A. Common phishing techniques used by attackers

Today, these mails do not get flagged as spam leading to the individuals being scammed and divulged to give in their information. This is done by the attackers employing phishing techniques to try to steal information.

Link Manipulation: The most familiar method used by phishers is making a link in an email that leads the user to spoofed websites. Common tricks used include misspelt URLs, use of subdomains, making anchor texts for a link appear to be a valid URL when the link actually goes to the phishers' site. Earlier, the '@' symbol was used in the spoofing links, to include a username and password in a web link. Despite the widespread awareness of the issue, also known as Internationalised Domain Names spoofing or a homograph attack, no documented phishing attacks have exploited it.

Website forgery: The deceit does not as victims view websites. JavaScript commands are employed by phishing scams to change the address bar. Accomplished by either overlaying pictures of the actual entity's URL over the address bars or by closing the old address bar and establishing new ones with legitimate URLs. Another technique is using scripts of trustworthy websites against victims. Cross-site scripting attacks are particularly dangerous since they urge the user to sign in at their bank's or service's own web page, where everything from the web address to the security certificates looks to be correct and are impossible to detect without specialised understanding.

Phone phishing: A false website isn't required in every phishing effort. In a 2006 instance, messages purporting to be from a bank instructed users to call a phone number about an issue with their bank account. When consumers dialled the phisher's phone number, prompts instructed them to input their account details and PIN.

B. The psychology behind cyber-crimes and the behavioural response to the risk of phishing

Differences between cyber-crime and traditional crime, both in terms of committing and prosecuting the crime, appear to favour criminals. Current legal structure makes it extremely difficult to identify, apprehend, and convict cyber offenders. Because cyber-crime does not necessitate the perpetrator's physical presence, the attackers can choose where they will be at the moment of the crime. A simple programme can be written at any time and injected into any network. The application can be programmed to run whenever the culprit desires.

The user behaviour that has presented itself as a risky measure has been the reason for the gradual and rapid expansion of cybercrime. Along with that, the statistics that support it, has been a contributing factor in the rise of online scamming and hacks. Cybercriminals use social media or the wider internet to gather information. Because of the nature of the situation, persons working in SMEs are also exposed, that raises the cost of improving the system's security, and the human contact with it makes it much more difficult to manage.

According to a study, there are certain principles used by phishers to be successful at what they do. First, authority. Phishers usually impersonate senior executives in emails. This is because people defer authority. Second, consistency. Humans are often referred to as creatures of habit. This is used by attackers, hoping the recipient overlooks the unusual request that is included in such an email. Third, consensus. A phishing email or message that mentions statistics such as “455 of 600 people have registered for this event” is more likely to be at the risk of phishing than another. Lastly, unity. This is the usage of similarities and same interests to commit a cyber-crime.

C. Phishing countermeasures

In reaction to phishing, solutions have been developed designed to address both technical and non-technical issues. Although there are numerous recommendations for combating phishing, the following are widely used today to either directly combat phishing or minimise phishing-capable threats like malware.

One basic fact that cyber criminals have taken advantage of is the lack of education of two main things; the occurrence of internet related cyber-crimes and online companies' policies and procedures for contacting clients about account information and maintenance issues. When a customer recognises a phishing email or website, he or she can immediately link it to the attempt to steal account information. If malware is discovered on a computer, the typical approach is to follow the instructions for isolating and eradicating the danger, of which users may be unaware, making the link between the activity of attempting to steal account information unclear.

Second is web browser toolbars. The development of toolbars for web browsers that can help identify whether a consumer is browsing a probable phishing site is one of the efforts to safeguard customers against phishing scams. These toolbars mostly work by looking for a database of known FQDNs and IP addresses that have been reported as hosting phishing sites. The phishing site must be already reported in the database for this to work.

Third, strong authentication and authorization. A technique that requires two or more authenticators is known as two factor authentication. It is used in online commerce by giving customers a physical token that generates a constantly changing component for their authentication credentials. The purpose is to safeguard users if an attacker obtains their login credentials through electronic surveillance. The attacker's ability to use the credentials in the future is limited due to the ever-changing component's timeliness.

Last is virus, spyware and spam prevention. Anti-virus, anti-spyware, and anti-spam softwares all help safeguard from phishing frauds. Devices that identify and block harmful code installation and execution are a crucial aspect of a secure home computer environment. These products must be enabled and have up-to-date signatures in the case of anti-virus and anti-spyware products. A significant fraction of modern malware tries to disable anti-virus and anti-spyware software before a detection signature can detect and eliminate it.

8. Discussion and Conclusion

To address the rising capabilities available to phishers, phishing awareness must continue to advance. This awareness should be spread not only among clients, but also among workers of targeted firms and law enforcement officers charged with investigating electronic financial crimes. Customers should be made aware of the growing sophistication and use of technical deception in phishing emails and websites, which makes them hard to detect and even harder to be resolved.

Reduce the return on investment of the activity to the criminal community as part of the plan to combat phishing. By continuing to develop and enforce existing anti-phishing defences, the resources utilised for phishing become scarcer and more expensive, making phishing less profitable.

Even if defences are put in place to stop one method of data theft, criminals have other choices. Understanding the technical capabilities available to these criminals is crucial for designing more effective methods for securing customer information and law enforcement personnel entrusted with catching and convicting phishing scammers.

References

[1] Lynch, J. (2005). Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal*, *20*(1), 259–300.

[2] 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.

[3] Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1-20.

[4] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139-154.

[5] Mihai, I. (2012). Overview on phishing attacks. International Journal of Information Security and Cybercrime, 1(2), 61-70.

[6] Jabbour, K. T., & Devendorf, E. (2017). Cyber Threat Characterization. *The Cyber Defense Review*, *2*(3), 79–94.

[7] Wiggen, J. (2020). The impact of COVID-19 on cyber crime and state-sponsored cyber activities. Konrad Adenauer Stiftung.

[8] Rahman, S. S. M. M., Islam, T., & Jabiullah, M. I. (2020). PhishStack: evaluation of stacked generalization in phishing URLs detection. *Procedia Computer Science*, *167*, 2410-2418.

[9] Lacey, D., Salmon, P., & Glancy, P. (2015). Taking the bait: a systems analysis of phishing attacks. *Procedia Manufacturing*, *3*, 1109-1116.

[10] Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527-565.

[11] Bhoopal, U. (2021). Phishing Attempts in Cyber Crime. Supremo Amicus, 24, [39]-[50].

[12] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

[13] Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review*, *21*(5), 408-414.

[14] Eisenberg, A. K. (2015). Criminal Infliction of Emotional Distress. *Michigan Law Review*, *113*(5), 607–662.

[15] Warikoo, A. (2014). Proposed methodology for cyber criminal profiling. *Information Security Journal: A Global Perspective*, *23*(4-6), 172-178.

[16] Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pp. 37-44.