IJARSCT

ISSN (Online) 2581-9429

Impact Factor 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, July 2022

Phishing: A Way of Attacking the Privacy

Mr. Rahul Ramesh Ghodekar[1] and Prof. Sudeshna Roy[2]

Student, Bharati Vidyapeeth, Navi Mumbai, India[1]

Assistant Professor, Bharati Vidyapeeth, Navi Mumbai, India[2]

Abstract: *The Internet provides a fantastic platform for ordinary people to communicate. Criminal minds have figured out a means to steal personal information without having to meet the person and with the least danger of getting detected. It's known as phishing. Phishing is a significant threat to the ecommerce sector. Customers' trust in ecommerce is shattered, and electronic service providers suffer significant financial losses as a result. As a result, understanding phishing is critical. This document educates readers on phishing assaults and anti-phishing the recipient, the auction site will have a good yield. Anti-phishing strategies and online security rules have been recommended by both academia and industry practitioners in order to protect customers' interests. Some commercial anti-spam and anti-phishing products block email from "blacklisted" sites that they claim deliver spam and phishing emails, but allow email from software. Because of the obvious usability issues "whitelisted" sites that they claim are known not to send it. This strategy appears to be anticompetitive because it unfairly discriminates against smaller and lesser-known sites.*

Keywords: Email Phishing, SMS Phishing, Website Phishing, SPF, DMARC.

I. INTRODUCTION

PHISHING is the act of attempting to obtain sensitive information from a victim by impersonating a trustworthy third party in an electronic conversation, which could be a person or a reputable corporation. The goal of a phishing assault is to persuade recipients to reveal sensitive information such as bank account numbers, passwords, and credit card numbers. For example, a phisher may pose as a significant banking institution or a well-known online retailer. Despite knowing little to nothing about with security toolbars, their performance may suffer as a result. The examination of usability is critical for the future. Today, five common antiphishing toolbars are in use: Internet Explorer 7.0's built-in phishing prevention, Google Toolbar, Netcraft Anti-phishing toolbar, and Spoof Guard. In addition, Antiphishing IEPlug is an Internet Explorer plug-in. A lot of usability concerns may be discovered based on the heuristic usability evaluation.

II. LITERATURE REVIEW

During a phishing attack, the attackers utilize digital deceit to trick their victims into divulging personal information. The success of the deception is determined by the attackers' ability to imitate real services and connections, as well as the user's ability to recognize and/or respond correctly to what is phoney and what is authentic. For example, a phishing email may have evident spelling errors, indicating that it is not legitimate. However, if these spelling errors go undiscovered before the receiver clicks, the assault will be successful. We want to better understand the present status of user-centered phishing research, covering a wide range of methodological techniques and potentially significant attack attributes, because the user plays such a crucial role in phishing attempts. Users might provide interview comments on a prototype's usability, for example, as part of more traditional research approaches. However, we're also interested in more passive ways that can tell us a lot about what consumers are and aren't paying attention to when they're confronted with a phishing assault. Alsharnouby et al., for example, used eye tracking techniques to collect data on user attention to site authenticity. Their findings revealed that gaze time on browser elements had a beneficial impact on the capacity to detect phishing websites, while the technical skill of the participants had no bearing on the detection strategy they used. Visual deception can fool even sophisticated users, according to Dhamija et al., who discovered that a good phishing website tricked 90 percent of their participants. Given their research of participants' tactics for detecting a phishing website, they argue that standard security indicators are ineffective. Such studies aid in establishing the efficacy of human centered phishing research, as well as justifying our focus on the current status of user studies in the phishing literature.

DOI 10.48175/IJARSCT-5701

III. TYPES OF PHISHING ATTACKS

Due to a lack of setup on their email, attackers/phishers send legitimate links to victims via valid email, which allows anyone to use their email and drop the email in the victims' email box. There are following types of Phishing Attacks which leads to information leakage of victims. A. Email Phishing B. Sms Phishing C. Website Phishing Following is the Detail Explanation about all the Phishing Attacks.

3.1 Email Phishing

The most prevalent sort of Phishing assault is email phishing, in which the attacker sends legitimate-looking material by faking the sender's identity. This email is written with a sense of urgency, in which the attacker informs the recipient that their account has been compromised and that they must enter their information in order to change their password. Users become panicked and trust the email as a result of this type of communication, and they become phishing victims.

3.2 SMS Phishing

Smishing Attack is another name for SMS Phishing. Smishing is a type of attack in which the attacker sends a text message to the victim's phone. Malware is downloaded into the phone device when the attacker clicks on the link in the message, and the victim's phone is hacked.

3.3 Website Phishing

Website phishing is an attack in which the attacker uses the same look character from Latin or any other word format to fake the look of a website's url. The url of the website that the victim will view is the same as the actual website. After visiting the rogue website, the victim would be forced to give the attacker their credentials.

IV. ANTI-PHISHING TECHNIQUES

As a response to the above-mentioned phishing attack, we have discovered some manual antiphishing techniques that will assist in keeping people informed and protected from such attacks.

1. In a [1] Email Phishing Attack, the attacker spoofs the organization's legitimate email address and sends an email to the victim from the fake email account. Because this email address is authentic, the recipient will be unaware of the sender's malevolent intent. When a user receives an email with the subject ”Reset password” or ”Change account details,” the user should check the sender email to see if it is a real email. If the email id is valid, the user should verify the ”mailed by” section to see if the email was sent from a valid server or if the email sender page was hosted on a free hosting server.It will be required for businesses to activate SPF and DMARC records on their domains so that attackers are unable to use their email address in an email phishing assault. If a business owner or developer wants to see if their domain name is vulnerable to email phishing attacks, they should go to the following website and enter their domain name. https://mxtoolbox.com/.
2. In a [2] Sms Phishing Attack, the attacker sends a malicious link to the victim's mobile phone over text message, and when the victim clicks on the link, malware is downloaded to the victim's device. People do not have to click on any link that comes from an unknown person or a sms provider in order to avoid becoming a victim of the attack. Any prize or a communication from the bank are examples of messages. If the message contains any financial information, recipients must contact the bank immediately to validate the message.
3. 3.In a [3] Website Phishing Attack, an attacker creates a website that seems identical to the real. Facebook.com is the original website URL, and the malicious website will be faceboook.com. Where the extra 'o' will be added, but the victim did not look at the address because he was in a rush and ended up submitting the credential to the attacker website. This type of Phishing attack can also be carried out via an IDN Homograph attack, in which the attacker utilises a UNICODE character to offer the identical URL to a website that the user can readily trust. If a random individual sends the link, the user must copy the website address into notepad, where Unicode characters such as 'apple.com' will be converted to 'XN 80ak6aa92e.com'.

DOI 10.48175/IJARSCT-5701

V. CONCLUSION

Phishing assaults are one of the oldest types of cyber-attacks, costing billions of dollars each year (Moore and Clayton, 2011; Tian et al., 2018). The Federal Bureau of Investigation assessed in 2018 that companies in the area of Business email hacks cost the world 12 billion in 2018 (DigitalinformationWorld.com, 2019). In the field of secure computing, preventing phishing attacks is a top goal and a serious difficulty. While researchers and practitioners frequently offer technical solutions to address phishing-related issues, our analysis of phishing research suggests that social solutions that focus on users themselves could provide an important, missing piece of the complete toolkit available to combat these attacks. Only 13.9 percent of relevant published papers on phishing from 2004 to 2018 included any kind of user focused study, and these studies primarily focused on usability or testing of tools developed by the researchers rather than exploring how different types of users approach and make sense of phishing attempts, according to the ACM Digital Library. A lot of this research left out key information on the people who took part in the study. Based on our review of published phishing research to date, we see support for the potential usefulness of user studies in this field of study, as well as for better reporting and recruiting techniques in future studies.

REFERENCES

[1]. Phishing with Unicode Domains - Xudon Zheng

[2]. Bart, Y., Shankar, V., Sultan, F., and Urban, G. L. (2005) Are the drivers and role of online trust the same for all web sites and consumers? A large-scale empirical study, Journal of Marketing, 69, 4, 133-152.

[3]. Dunham, K. (2004), Phishing isn't so sophisticated: scary!, Information Security Journal, Volume 13, No. 2, pp 2- 7.

[4]. Rakesh Verma, Narasimha Karpoor, Nabil Hossain and Nirmala Rai - Automatic Phishing Email Detection based on Natural Language Processing Techniques, Research Gate, 2016.

DOI 10.48175/IJARSCT-5701