Phishing Detection Approach on Social Media Networks

Daryoosh Mansoory[1], Ashiqullah Alizai[2], Abdullah Hamidi[3]

[1]*Network Department, Computer Science Faculty, Herat University, Herat, Afghanistan*
[2,3]*Database Department, Computer Science Faculty, Herat University, Herat, Afghanistan*

Abstract: **Internet technology is so extensive today. As an example, from online social networking to online banking, it's made people's lives easier. One in all the foremost important problems with the net technology is unwanted spam emails. The well-disguised phishing email comes in as a component of the spam and makes its entry into one's inbox quite frequently nowadays. Here the various aspects of phishing attacks and some possible defenses as countermeasures are analyzed. Phishing could be a special form of network attack where the attacker creates a reproduction of an existing website to fool users in to submitting personal, financial, transaction or password data to what they think is their service provider's website. Phishing is also a range of online fraud that aims to steal sensitive information like online passwords and master card information. To protect internet users against phishing, different anti-phishing techniques are proposed. During this paper we've reviewed various phishing and anti-phishing methods for detecting and preventing phishing attack.**

Keywords:- **Phishing, Information Technology, Anti-phishing, techniques, Social networking**

I. INTRODUCTION

The world is roofed and ruled by technology. However, this technology may betray you when it's vulnerable and will result in loss of essential data. A serious challenge and important issues in Information Technology and also the IT world is that the information security and protection of information. This involve the safety and data of the companies and also the government, your computer, tablet and cellphone that contain important and sensitive information that hackers and other criminals would like to have them.

1. Masse [9] points out that protection of sensitive information is vital in our modern society. Despite the increasing awareness of the threats to information security, there continues to be information security violations.

Banu and Banu [2] statement that phishing could be a sort of online fraud that aims to steal sensitive information like online passwords and MasterCard information. Phishing attacks use a mixture of social engineering and technology spoofing techniques to steer users into making a gift of sensitive information that the attacker can won't to make financial profit. Normally phishers hijack a banks sites and send emails to the victim so as to trick the victim to go to the malicious site so as to gather the victim checking account information and card number.

As Suganya [11] expresses that these days' attacks have become major issues in networks. Attacks will poke into the network infrastructure and collect the knowledge needed to cause vulnerability to the networks. Security is required to stop the info from various attacks. Attacks may either active attack or passive attack. Phishing emails contain link to the infected website. Phishing email direct the user to the infected website where they're asked to enter the non-public information, in order that the web site will hack the knowledge regardless of the user enters. Phishing email is sent to sizable number of individuals and therefore the phisher will count the proportion of individuals who read that email and entered the knowledge. Many internet users are attacked by phishing and therefore the attacker become success to steal the sensitive and private data through a fake email and link.

Biju, Jacob and Choing [3] denote that one in every of the largest problems with the web technology is that the unwanted spam emails. The well-disguised phishing email comes in as a part of the spam and makes its entry into one's inbox quite frequently nowadays. While phishing is often considered a consumer issue, the fraudulent tactics the phishers use are now intimidating the company sector additionally. Phishing is that the act of sending forged emails and pretend websites to users in an endeavor to scam them into surrendering personal information that ends up in fraud. Typical phishing email is distributed too many potential victim's mailboxes, and frequently comes with a clickable link. The phishers (attackers) may use deceptive sender address, genuine-looking logo and fraudulent web links in such emails.

Damodaram [6] introduces that phishing is an act of attempting a victim for fraudulently acquires sensitive information by impersonating a trustworthy third party, which might be someone or a reputed business in a transmission. The target of phishing attack is to trick receivers into divulging sensitive information like checking account numbers, passwords and MasterCard details. As an example, a phisher may misrepresent himself as an outsized banking corporation or popular on-line auction site will have an inexpensive yield, despite knowing little to nada about the recipient.

As a result, a phisher could target many forms of wind, including user names and passwords, master card numbers,

checking account numbers, and other personal information. Where several suspected Internet users, called phishers, post a friendly e-mail for other users, aiming at acquiring sensitive information from a victim fraudulently, by acting as an acquaintance. A standard phishing attack is (for a phisher) to get a victim's authentication information appreciate one website (that is corrupted by the attacker) and so use this at another site. This can be a meaningful attack on condition that many computer users reuse passwords – whether in verbatim or with only slight modifications. During this research every kind of phishing along the prevention methods are explained and also the way the way to be secure and save from a phisher inside the network.

II. STUDY PURPOSE

The aim of this review research is to achieve a better understanding of the threat named phishing attack, nefarious attacks aimed towards the human element of the target.

Suppose a person receives a phone call from someone claiming to be from a computer support company, your ISP or perhaps tech support of a company. They may ask you to test to determine if you've got certain files on your computer and walk you thru on a way to find them. Once they need tricked you into believing your computer is infected, they're going to pressure you into going to an internet site and buying their security software or ask you to grant them remote access to your computer so that they can fix it. However, the software they're selling is really a computer virus. If you get and install the software, not only have they fooled you into infecting your computer, but you furthermore may just paid them to try to it. If you give them remote access to your computer to repair it, in reality, they're visiting take over and infect it.

III. PHISHING

Chouhan and Chawla [4] survey that the word 'Phishing' initially emerged in 1990s. The early hackers often use 'ph' to interchange 'f' to get new words within the hacker's community, since they sometimes hack by phones. Phishing may be a new word produced from 'fishing', it refers to the act that the attacker appeal users to visit a faked Web site by sending them faked e-mails (or instant messages), and silently get victim's personal information like user name, password, etc. This information then are often used for future target advertisements or perhaps fraud attacks.

Almomani, Samer, Meulenberg and Eman [1] exposes that the act of sending an e-mail to a user falsely claiming to be a longtime legitimate enterprise in a shot to scam the user into conceding personal information that will be used for identity theft. The e-mail directs the user to go to an internet site where they're asked to renew personal information, like passwords and master card, social insurance, and checking account numbers that the legitimate organization already has. One among the first aims of phishing is to dishonestly do fraudulent financial transactions on behalf of users using a forged email that contains a URL pointing to a fake web site.

Rami, Thabtah and McCluskey [10] have revealed that phishing may be a relatively new web-threat, it's a large impact on the commercial and online transaction sectors. Social engineering and technical tricks are commonly combined together so as to start out a phishing attack. Typically, a phishing attack starts by sending an e-mail that seems authentic to potential victims urging them to update or validate their information by following a URL link within the e-mail.

IV. PHISHING TECHNIQUES

According to Rami, Thabtah and McCluskey [10] phishers use different tactics and strategies in designing phishing websites. These strategies can be categorized into three basic groups those are:

- *Mimicking attack:* during this attack phishers typically send an email to victims asking them to verify, update or validate their credentials by clicking on a URL link within the e-mail which can redirect them to a phony webpage.
- *Forward attack:* This attack starts once a victim clicks on the link shown within an email. He then redirected to an internet site asking him to submit his personal information.
- *Pop-up attack:* Another method utilized by MITM technique is urging victims to submit their information by means of well-designed pop-up window.

V. TYPES OF PHISHING

Dakpa and Augustine [5] statement that there are common forms of phishing such as:

- Email Phishing: Phishing scam on the online starts with an email message that looks like a political candidate communication from a reliable source sort of a bank, a master card company or a reputable online store.
- Spear Phishing: It targets specific individuals instead of an outsized group of people. Attackers often research their victims on social media and other sites. That way, they'll customize their communications and appear more authentic.
- SMS Phishing: SMS phishing, or “smishing,” could also be a kind of phishing that capitalizes on the world’s addiction to text messaging and instant communications.
- Phone Phishing: Vishing” is “voice phishing” (phishing over the phone), then you’re be correct. A vishing attack occurs when a criminal calls your phone to undertake to induce you to provide personal or financial information.

VI. PHISHING FUNCTIONALITY

Damodaram [6] points out that an individual who engaged in malware activities is termed a phisher. The strategy utilized by phishers is typically to create fraudulent websites, the same as the real website by mimicking the HTML code containing the identical images, text and sections.

The phishing attack lifecycle are often decomposed in:

- Planning: Typically, phishers start planning for his or her attack by identifying their victims, the knowledge to be achieved and which technique to use within the attack.
- Setup: The phisher creates the attack code/message and sends to the target user.
- Attack: A malicious message arrives at the target site. The ignorant target reads the message and takes some action which makes him or her susceptible to an information compromise.
- Collection: As soon because the victim takes an action making him vulnerable to an information theft, he's then urged to submit his credentials through a trustworthy-looking webpage. Normally, the fake website is hosted on a compromised server, which has been exploited by the phisher for this purpose.
- Fraud: The phisher engages in fraud using confidential information to impersonate the user.
- Post-Attack: The user is then prompted for confidential data through a well-known and trustworthy looking web interface.

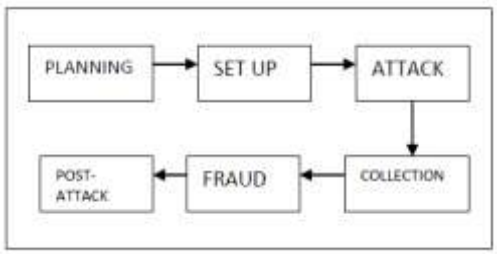

Fig 2: Steps in Phishing, adapted from [6]

VII. PHISHING PREVENTION

Guedez [7] points out that phishing prevention refers to a comprehensive set of tools and techniques that will help identify and neutralize phishing attacks before. This includes extensive user education that's designed to spread phishing awareness, installing specialized anti phishing solutions, tools and programs and introducing variety of other phishing security measures that are aimed toward proactive phishing protection while providing mitigation techniques for attacks that do manage to breach security.

According to Hadnagy and Fincher [8], there are list of Anti-Phishing tools which can be used for phishing prevention purpose:

- Mail-Secure: Mail Secure's Anti-Phishing module combines several layers and technologies to detect and block. Phishing attempts.
- Security Tool Bar – Netcraft: It provides web server and web hosting market-share analysis, including web server and software system detection.
- ESET Security: ESET Smart Security incorporates anti-spam and a bidirectional firewall altogether with traditional anti-malware features of ESET NOD32 Antivirus.
- Browser Integrated Tools: It usually relies on a blacklist, which contains the URLs of malicious sites, to see whether a URL corresponds to a phishing page or not.
- Using Anti-phish and Dom Anti-phish Techniques: AntiPhish may be a browser plug-in that keeps track of sensitive information.
- PhishMe: PishMe may be a SaaS solution that utilizes immersive education methods to coach employees to recognize and avoid phishing attacks.
- Wombat: With this tool, you'll assess your employees' vulnerability to attack and motivate them to require training by sending them mock phishing e-mails.
- PhishLine: PhishLine is an enterprise SaaS solution that gives real-world social-engineering and phishing simulations together with online security awareness training, risk-based surveys, and detailed, risk-based reporting and metrics.
- Social-Engineer Toolkit: SET provides a mechanism for assessors to check the effectiveness of their education and awareness program.
- Phishing Frenzy: Phishing Frenzy is an open source Linux based Ruby on Rails application that's leveraged by penetration testers to manage e-mail phishing campaigns.

VIII. PHISHING IMPACTS

Stolen data can have many uses. Master card information will be accustomed purchase goods and services, ATM card information may well be accustomed duplicate ATM cards and use them for withdrawal of money. Account information will be accustomed steal information or to be ready to act as another user online.

IX. MISTAKES ABOUT PHISHING

According to Dakpa and Augustine [5] the most common mistake of people which leads to phishing attacks are:

- People clicking on the links in emails
- Individuals who don't close the browser after logging out.
- Spamming as a result of forwarding emails.
- Those who don't use Internet email security.
- Failing to erase disk drive when selling computer.

X. CONCLUSION

This study has been that specialize in the phishing attack along the way a way to prevent those attacks anywhere. Internet facilitates reaching customers everywhere the world with none market place restrictions and with effective use of e-commerce. As a result, the quantity of consumers who depend on the net to perform procurements is increasing dramatically. Many numerous dollars are transferred through the net daily. This amount of cash was tempting the fraudsters to hold out their fraudulent operations. Thus, Internet-users were prone to differing kinds of web-threats. Hence, the suitability of the net for commercial transactions becomes doubtful.

Phishing may be a style of web-threats that's defined because the art of mimicking a web site of an authentic enterprise planning to acquire private information. Typically, a phishing attack starts by sending an e-mail that seems authentic to potential victims urging them to update or validate their information by following a URL link within the e-mail. Predicting and stopping phishing attack may be a critical step toward protecting online transactions.

As a result, identifying phishing websites is performed manually. By this suggests, the Internet-user analyses the webpage and supported the extracted information he takes a choice on the web site legitimacy. Therefore, we believe that a successful phishing detection model should be able to adapt its knowledge and structure in an exceedingly continuous, interactive way in response to the changing environment that characterizes phishing websites.

10.1 Suggestions

The subsequent list of recommendation to the general public internet users to be safe from any phishing attack, those advices are classified as what to try to and what no to do:

10.1.1 What to do

- Protect your computer with anti-virus software, spyware filters, email filters, firewalls, and Anti-Phishing toolbar & confirm that they're regularly updated.
- Ensure that your Internet browser is up to date and security patches applied.
- Always make sure that you're employing a secure website when submitting master card or other sensitive information via your browser.
- Regularly check your bank, credit and charge account credit statements to make sure that everyone transactions are legitimate.

10.1.2 What NOT to do

- Don't assume that you just can correctly identify an internet site as legitimate just by staring at its general appearance.
- Always check the spelling of the URLs in email links before you click or enter sensitive information.
- Don’t use the links in an email to urge to any online page, if you think the message may not be authentic.
- Avoid filling out forms in email messages or pop-up windows that enkindle personal financial information.
- Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media.

REFERENCES

[1] Almomani, A., B, G., Samer, A., Meulenberg, & Eman , A. (2013). A Survey of Phishing Email Filtering Techniques. IEEE Communications Surverys & Turorials, Vol. 15, No. 4, PP.7-15.
[2] Banu, N., & Banu, M. (2013). A Comprehensive Study of Phishing Attacks. Tiruchirappalli: IJCSIT.
[3] Biju, I., Jacob, S., & Chiong, R. (2006, 1). Analysis of Phishing Attacks and Countermeasures. Germany: IBIMA, Bonn.
[4] Chouhan , S., & Chawla, M. (2014). A Survey of Phishing Attack Techniques. Bhopal: International Journal of Computer Applications, Vol. 93, No. 3, PP. 1.
[5] Dakpa, T., & Augustine, P. (2017). Study of Phishing Attacks and Preventions. Karnataka, Bangalore.
[6] Damodaram, R. (2016). Study on phishing attacks and antiphishing tools. Tamil Nadu, India.
[7] Guedez, A. (2017). The best in anti-phishing tools: Phishme vs Wombat features and results comparison. Retrieved from gb-advisors.com: https://www.gb-advisors.com/anti-phishing-tools/
[8] Hadnagy, C., & Fincher, M. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails. Canada: Wiley.
[9] Massé, E. (2018, 1 25). Accessnow.org. Retrieved from Data protection: why it matters and how to protect it: https://www.accessnow.org/data-protection-matters-protect/
[10] Rami, M., Thabtah, F., & McCluskey, L. (n.d.). Tutorial and Critical Analysis of Phishing Websites Methods.
[11] Suganya, V. (2016). A Review on Phishing Attacks and Various Anti Phishing Techniques.