BOOK CHAPTER | Phishing in Deeper Waters

A Review of Phishing Attacks

Mughele, Ese Sophia (PhD)
Department of Computer Science
University of Delta
Agbor, Delta State, Nigeria
E-mail: smughele@gmail.com

Abstract

Phishing is a type of cybercrime that involves tricking the user or victims into supplying sensitive and confidential information to the attacker. Some will steal the victims' login credentials or account information. Phishing attacks are carried out through fraudulent emails, text messages, and phone calls. The attacker could then use the information to perpetrate crimes such as financial fraud and identity theft. The goals of this paper are to raise awareness of phishing strategies, educate internet users about these attacks, and advocate the adoption of phishing prevention techniques, as well as to inform professionals about viable phishing prevention techniques.

Keywords: Phishing, Attacks, review, Security, Cybercrimes, Cyberspace

Introduction

Phishing is the act of impersonating a trustworthy person in an internet discussion in order to get sensitive data such as usernames, passwords, and credit card details. Communication that appears to come from well-known social media platforms, auction sites, and online communities payment systems, or an IT administrator is frequently used to deceive the unwary public. Links to malware-infected websites may be included in phishing emails. Social Engineering is exemplified via phishing. Phishing is primarily used in email hacking; in email phishing, the hacker sends a link to the user via email containing, for example, bank account information or other personal information; the user then goes to that link and fills out all of the information requested, and the hacker obtains all of the user's information.

Phishing begins with an email or other form of communication intended to aid in the victim's attack. The communication is made to appear as if it was sent by a trusted sender. If the victim is duped, he or she will provide personal information to a spam website. Malware may also be downloaded onto the computer of the target.

Citation: Mughele, E.S. (2022). A Review of Phishing Attacks
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

The goal of phishing is to steal data, money, or personal information by using a false website. The simplest way to avoid coming into contact with a phishing website is to recognize bad URLs in real time. The domains of phishing websites can be used to identify them. They are usually linked to a URL that has to be registered (low-level domain and upper-level domain, path, query). Using distinguishing attributes extracted from words that constitute a URL based on query data from various search engines such as Google and Yahoo, the recently obtained status of intra-URL relationship is utilized to evaluate it. The name of the game is phishing. It is defined as an organization's customer deception in communicating with their confidential information in an undesirable manner

.

Literature Review

A review of the relevant literature is included in this section. Several studies have been conducted on phishing attacks and anti-phishing attack techniques. Chiew et al. (2018) offered a detailed and technical overview of current and past phishing techniques. Through their research, they claimed to have gained a deeper understanding of the sorts, nature, and features of current and prior phishing techniques. The survey found that, as a result of growing technology and the widespread use of cloud computing and mobile devices, anti-phishing tactics are in high demand, particularly in sectors where technology is significantly involved. Browser vulnerabilities and phishing websites are responsible for a large percentage of phishing attacks.

Benavides et al., (2020) conducted a systematic evaluation of the literature on how to defend against phishing attempts using cutting-edge machine learning techniques. The article emphasized the importance of awareness sessions, focused blacklists, and machine learning (ML) techniques as three ways to combat phishing attempts, which are becoming more widespread these days. Deep learning (DL) is the most rising and efficient machine learning technique, according to the study, out of all the other approaches.

Amro (2018) discussed the different forms of phishing assaults that can occur on mobile devices, as well as prevention and anti-phishing strategies. They also outlined key precautions to take in order to defend mobile systems from phishing attacks. Current anti-phishing techniques, according to the report, have significant flaws that make them less effective at spotting phishing attacks.

Stafford (2020) discussed the causes and effects of phishing attacks on people, as well as how people become victims of such attacks. Humans become victims of phishing as a result of their own personality traits and practices, such as narcissism, gullibility, and regular email use, according to the study. From the findings, spear phishing is the most targeted of all the phishing strategies. Athulya et al. (2020) highlighted many phishing attacks, as well as the current phishing strategy adopted by phishers and certain anti-phishing techniques. The document educates readers about phishing attacks and strategies, and encourages them to use anti-phishing techniques. The study proposed a phishing detection approach that aids in the efficient detection of phishing websites.

Types of Phishing Attacks

In this section, consist of a brief description of the different types of phishing attacks

Deceptive Phishing

Deceptive phishing refers to messages requiring users to confirm account information, requesting users to re-enter their information, fictitious account charges, unwanted account changes, new free services requiring immediate action, and a variety of other malicious sites that are sent to a large number of recipients in the hopes that the unsuspecting will react by clicking a link to or signing onto a bogus site where their private information can be collected.

Malware-Based Phishing

This refers to phishing scams that infect consumers' computers with dangerous software. Small and medium companies (SMBs) who are not always able to keep their software applications up to date may get malware as an email attachment or as a downloadable file from a website for a specific issue.

Key loggers and Screen loggers

This sort of virus monitors keyboard input and sends the necessary data to hackers through the internet. They are installed as a small program in users' browsers and execute automatically when the browser is launched, as well as in system files as device drivers or screen monitors.

Session Hijacking

This is concerned with monitoring the users' activity until they sign into the account or transaction and create their critical data. The infected program will then carry out illicit acts such as money transfers without the user's awareness.

Web Trojans

They gather information from the user and send it to the phisher. This normally occurs when a user logs in for the first time.

Hosts File Poisoning

When a user types in the URL to visit a website, hackers will seek up the host names and send a phony address that seems identical to the actual website, allowing their personal information to be stolen.

Data Theft

Personal Computers will be used to store sensitive information. The victims will take these data without the user's knowledge. User information, such as passwords, social security numbers, credit card numbers, other personal information, or other private company information, is commonly used. Thieves benefit from stealing confidential conversations, design documents, legal opinions, employee-related records, and so on, and selling them to people who aim to shame or harm the company financially, or to competitors.

DNS-Based Phishing ("Pharming")

The hosts file is simply modified in DNS-based phishing. Hackers will return a counterfeit address in this assault, and communications will be forwarded to the fake website. Users are ignorant of this and will provide sensitive information, which will be hacked by hackers who are most likely not even located in the same nation.

Content-Injection Phishing

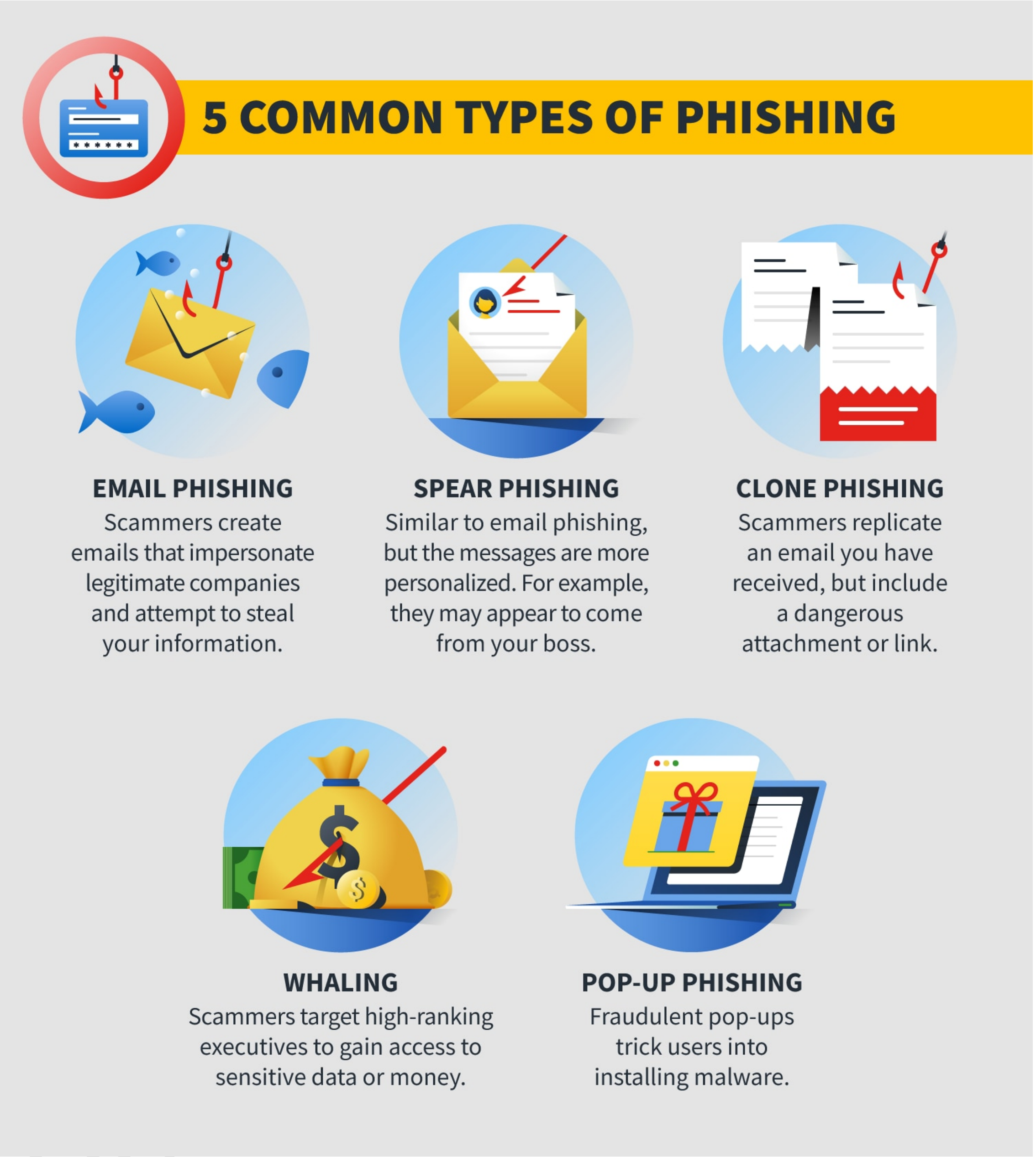
In this type of attack, hackers substitute the actual material on the website with bogus content, leading the user to provide sensitive information.

Man-in-the-Middle:

A hacker will be placed between the user and the website in this scenario. When a user provides personal information, hackers steal it without causing any inconvenience to the user. Hackers will use this information when the user is no longer engaged on the system.

Search Engine Phishing

Phishers will develop false product web sites, have them indexed by search engines, and then wait for unsuspecting clients to enter their personal information during an order, sign-up, or balance transfer. Such pages typically advertise products or services at prices that are almost too good to be true. Figue 1, shows a diagramatic illustration of the types of phishing attacks



5 COMMON TYPES OF PHISHING

EMAIL PHISHING
Scammers create emails that impersonate legitimate companies and attempt to steal your information.

SPEAR PHISHING
Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.

CLONE PHISHING
Scammers replicate an email you have received, but include a dangerous attachment or link.

WHALING
Scammers target high-ranking executives to gain access to sensitive data or money.

POP-UP PHISHING
Fraudulent pop-ups trick users into installing malware.

Figure 1: Types of Phishing Attacks
Source: https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

Existing Preventing Methods for Phishing Attacks

This section provided a brief on the on some existing techniques for preventing to handle all of the aforementioned subcategories of phishing attacks in the preceding section. These preventive techniques provided in this study used several technologies with an additional technique to educate internet users, both individuals and organisations. On the other hand, the tactics employed to resist phishing assaults are examined in detail, along with their pros and downsides. Figure 2, shows how phishing attack is launched on an organization (Suganya, 2016).

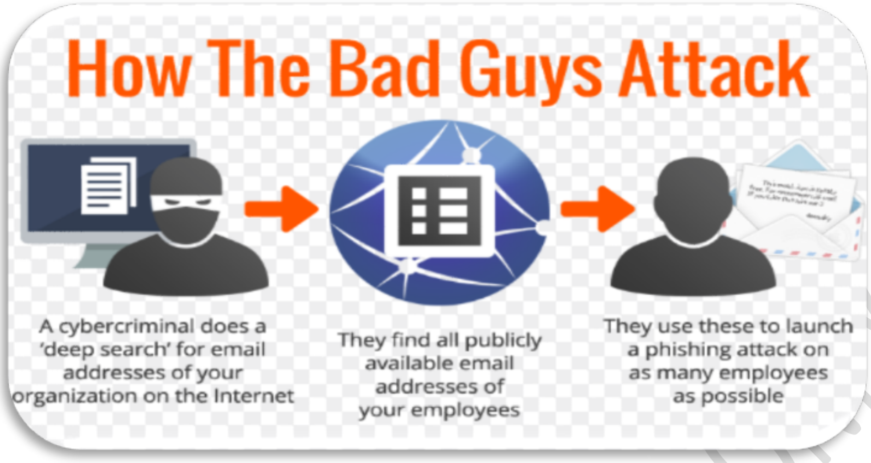

How The Bad Guys Attack
A cybercriminal does a 'deep search' for email addresses of your organization on the Internet
They find all publicly available email addresses of your employees
They use these to launch a phishing attack on as many employees as possible

Figure. 2: How The Bad Guys Attack
Source: https://www.keepnetlabs.com/ironscale/

Blacklist check
A list of dangerous website links is compared to the suspicious URL. "Zero day attacks" are possible with this strategy. Furthermore, when tactics such as routing through an alternate domain name and URL obfuscation are used, this strategy fails.

Heuristics
It utilizes heuristics such as domain registration data (owner, age, and country), the number of links to other well-known sites, image hashes, third-party cookies, and user reviews. The majority of heuristics applied are intuitive, resulting in a greater proportion of false positives.

User polling
Based on user votes, it determines if the URL is phished. However, it is ineffective against modern phishing attacks and is subjective, because the solution does not include any polling, it reduces uncertainty. Figure 3, illustrates how an organization can overcome phishing attack.

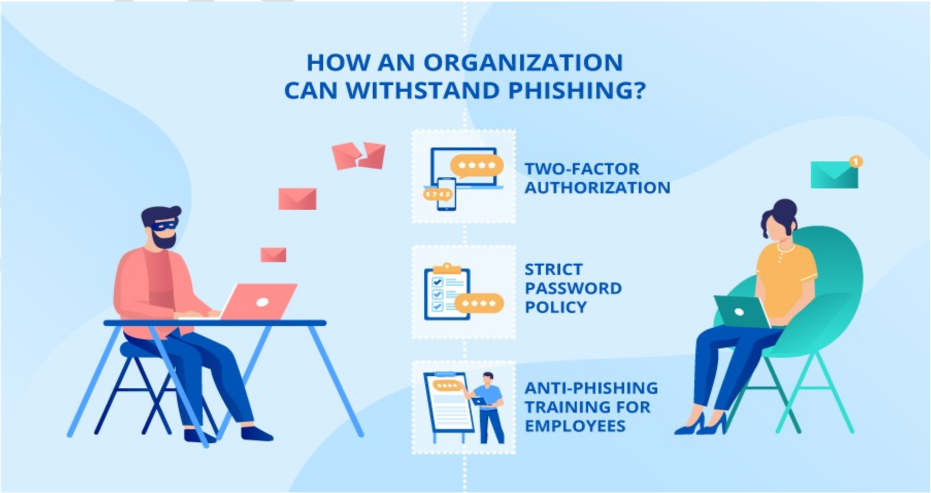

HOW AN ORGANIZATION CAN WITHSTAND PHISHING?
TWO-FACTOR AUTHORIZATION
STRICT PASSWORD POLICY
ANTI-PHISHING TRAINING FOR EMPLOYEES

Fig. 3: How Organizations Can Stop Phishing
https://www.scnsoft.com/blog/prevent-phishing-attacks

Working with third-party certification authorities and reputation services

This necessitates the use of an additional interface, which is vulnerable to phishing. The system handles phishing detection entirely on the server side, without the need of any third-party services. Another strategy for detecting a phishing URL is to employ page rank methodology, domain analysis, URL type analysis, and word analysis. However, it has been discovered that these processes cause false positives.

Conclusion

Phishing attacks may be extremely damaging to both individuals and businesses. It is a dangerous situation in which phishers are constantly trying to come up with new ways to manipulate their victims. Anti-phishing and anti-spam software should be used by online users to protect them when harmful messages are delivered to their computers. Anti-malware software is similar to anti-spam software in that it is developed by security researchers to detect even the most evasive malware.

Detecting identity theft and phishing emails is a major challenge which has also received a lot of attention from cyber security experts. It is unaffected by the growing trend of outsourcing e-mail. It may be difficult to do cross-managerial log analysis and communication. To put it another way, other electronic transactions will become a threat as well. From now on, it is recommended that serious effort be done on these issues before rash attacks occur. All critical Internets banking activity should be protected by a command. Furthermore, advanced Information and Communication Technologies such machine learning algorithms using optimization methodology, will also help combat phishing attacks on the cyberspace.

References

1. Amro B. (2018) “Phishing Techniques in Mobile Devices,” arXiv, pp. 27–35, 2018, doi: 10.4236/jcc.2018.62003.
2. Athulya, A. A., and K. Praveen. (2020) "Towards the Detection of Phishing Attacks." 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). IEEE, 2020.
3. Benavides .E, Fuertes W, Sanchez S. and Sanchez M. (2020) “Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review”, vol. 152. Springer Singapore, 2020.
4. Chiew K. L, Yong K. S, and Tan C. L (2018) “A survey of phishing attacks: Their types, vectors and technical approaches,” Expert Syst. Appl., vol. 106, pp. 1–20, 2018, doi: 10.1016/j.eswa.2018.03.050.
5. Keepsnetlabs.com (2021) https://www.keepnetlabs.com/ironscale/
6. scnsoft.com (2022) https://www.scnsoft.com/blog/prevent-phishing-attacks
7. Stafford .C.D. (2020) Weakest Link: Assessing Factors that Influence Susceptibility to Falling Victim to Phishing Attacks and Methods to Mitigate. Diss. Utica College, 2020.
8. Suganya .V (2016) International Journal of Computer Applications (0975 – 8887) Volume 139 – No.1, April 2016
9. https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html