**PHISHING AND ANTIPHISHING TECHNIQUES**

**by**

**BLESSING BULUS**

**st/cs/Hnd/19/019**

**BEING A SEMINAR PAPER**

**PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY,**

**FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**DECEMBER, 2021**

**Abstract**

*Now a days one of the highly used techniques to pursue online stealing of data and to do fraudulent transactions is phishing. Phishing is a form of online identity theft that aims to steal sensitive information such as online passwords and credit card information. It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials. To stop phishing many detection and prevention techniques has been made with their own advantages and disadvantages respectively, but phishing has not been eradicated completely yet. This seminar paper has shown phishing and its types in detail and reviewed some of the phishing and anti-phishing techniques. Also, the seminar paper recommended techniques that can be used to prevent phishing attacks for both individuals and organizations.*

**INTRODUCTION**

Internet has changed the life of human significantly and it has dominated many fields including e-Commerce, e-Healthcare etc. Internet increases the comfort of human life; on the other hand it also increases the need for security measures too. For example all web browsers and servers take almost every care to make guarantee the safe business through internet. Still they are vulnerable to attacks such as phishing. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. Phishing is not limited to the most common attack in which targets are sent spoofed (and often poorly spelt) messages imploring them to divulge private information. Instead and as recently documented both in academic and criminal aspects, phishing is a multi-faceted techno-social problem for which there is no known single silver bullet. As a result of these insights, an increasing number of researchers and practitioners are attempting to quantify risks and degrees of vulnerabilities in order to understand where to focus protective measures (Taylor, 2020).

The Phishing technique and attack is a method to access sensitive and restricted information of end users by using social engineering and technology. Phishing has been declared as the number one approach used by the attackers to exploit the privacy of the internet user (Naaz, 2021).

Most of the people who become victims, are those who do not have knowledge about phishing attacks. Phishing attacks on IOT devices and machines are also growing rapidly. Many security mechanisms are followed to minimize this problem but attackers are always forming ground-breaking ideas to crack undisclosed information and identities using advance technologies (Hanus, 2021).

The most common method in phishing is sending scam emails to victims. These emails are sent through the accounts which are the replicas of government authorized agencies, digital banks, electronic payment sites and digital markets like flipkart. These replicas and fraud websites gains the sensitive data from the end users through many ways (McAlaney and Hills, 2021).

These websites send the account update links, account verification emails and sometimes send prize winning messages like “congratulations you have won $10,0000, click on the link below to process” to end users by using social engineering techniques to deceive the internet users. They make them believe that those emails are coming from authorized organizations (Hanus, 2021).

Phishing can also be done through fake phone calls for example; the person calling you present himself from any bank and ask you for your bank account details and credentials like credit card number, ATM pin code, OTP (onetime password), usernames and passwords. Anti-phishing working group (APWG) reported that, 90% of the phishing outbreaks are held through HTTPS on which the data of user and browser is found. It also reported that, in the 3rd quarter of 2020, the most targeted sector is web email sites and Software-as-a-Service. To minimize the phishing effects and its consequences on the users, everyone should be aware of the phishing techniques. The comprehensive analysis of phishing attacks and techniques can help security developers and policy makers to develop better safety techniques and approaches (Diaz, 2020).

**Classification of Phishing Attacks**

Phishing

attacks

Email, IM

Email

IM,IRC,e

tc

Phone,mail,etc

Exploit Based

Figure 1: Phishing attacks (Hadlington, 2021).

1. Spooled e-mails are sent to a set of victims asking them (usually) to upgrade their passwords, data accounts, etc (Hadlington, 2021).
2. MSN, ICQ, AOL and other IM channels are used to reach the victims. Social engineering techniques are used to gain victim’s sensitive information (Hadlington, 2021).
3. Calling the victims on the phone, classic social engineering techniques are used by phishers (Hadlington, 2021).
4. Another kind of attack is based on internet vulnerabilities. This approach is usually used to automatically install dialers (Hadlington, 2021).

**TYPES OF PHISHING**

Kiren andSunil(2020), presented a review on different types of phishing attacks and detection techniques. Also, they presented some mitigation techniques of phishing. The paper proposed that 100% accuracy to detect phishing can be made possible by using machine learning approach among all other anti-phishing approaches.

Rana (2020), presented a review and comprehensive examination of the modern and state of the art phishing attack techniques to spread awareness of phishing techniques among the reader and to educate them about different types of attacks. Phishing has spread beyond e-mail to include VOIP, SMS, Instant messaging, social networking sites and even multiplayer games. Below are some major categories of phishing.

**Clone phishing**

Clone phishing is a type of phishing attack where hacker tries to clone a web site that is victim usually visits. The clone web site usually asks for login credentials, mimicking the real websites. This will allow the attackers to save these credentials in a text file, database record on his own server, then the attacker redirects his victim to the real websites as a authenticated user (Rana, 2020).

## Spear phishing

Spear phishing targets at specific group. So instead of casting out thousands of e-mails randomly spear phishers target selected groups of people with something in common. For example, people from same organization (Naaz, 2020).

## Phone phishing

This type of phishing refers to messages that claim to be form a bank asking users to dial a phone number regarding problems with that bank accounts. SMS phishing is a variation for phone phishing. The end-users receives sms telling him that he has successfully subscribed to a service (Adam, 2021).

If he wants to unsubscribe the service he should visit the website now the end users visit the websites and provide sensitive information.

## DNS-Based Phishing (Pharming)

Pharming is an attack aiming to redirect a website traffic to another bogus site. Pharming interfere with the resolution of domain name to an IP address so that domain name of genuine web site is mapped onto IP address of rogue website (McAlaney and Hills, 2020).

If we are typing the domain name www.barclays.co.uk in the address bar, it is redirected to www.google.co.uk.

## Man-in-the-middle-attack

A man-in-the-middle attack often refers to an attack in which an attacker secretly intercepts the electronic messages given between the sender and receiver and then capture, insert and modify message during message transmission. A man-in-the-middle attack uses Trojan horses to intercept personal information (Biswal and Subhendu, 2021).

**Typical Process of Phishing**

In a typical phishing attack, phishers send a large number of spooled emails to random number of internet users that seem to be coming from a legitimate organization. Email urges to provide sensitive information. By clicking on the link provided in the mail, user is directed to a bogus site implemented by the attacker (Hadlington, 2021).

**PHISHING TECHNIQUES**

Various techniques are developed to conduct phishing attacks. The phishing techniques are described as follows.

## Email spoofing

Email spoofing is used to make fraudulent emails appear to be from legitimate senders so that recipients are more likely to believe in the message and take actions according to its instructions. Email spoofing is possible because Simple Mail Transfer Protocol does not include an authentication mechanism. To send spoofed emails sender inserts commands in headers that will alter message information. It is possible to send a message that appears to be from anyone anywhere saying whatever the sender wants it to say. Fig 8 shows the example for e-mail spoofing (Hanus et al., 2021).

## Web spoofing

A Phisher could forge a website that looks identical to a legitimate website so that the victims may think this is the genuine site and enter the personal information which is collected by the phisher. Web spoofing creates a shadow copy of the World Wide Web. The shadow copy is funneled through attackers’ machine. (Biswal & Kumar, 2021).

Modern web browsers have built in security indicators that can including domain name highlighting and HTTPS indicators. They are often neglected by careless users. Modern web browsers display a padlock icon when visiting an HTTPS web site of Hyper Text Transfer Protocol and HTTPS, Transport Layer Security, provides encryption and identification through public key infrastructure (Biswal & Kumar, 2021).

Web browsers examined the certificate presented by the web browser. The certificate considered as invalid if any of the following situations occurs, the certificate is expired, the certificate is not signed by root CA, the certificate is revoked by CA otherwise the website host name does not match the subject name in the certificate (Biswal & Kumar, 2021).

## DNS Cache Poisoning

DNS cache poisoning attempts to feed the cache of local DNS resolves with incorrect records. DNS runs over UDP and easy to spoof the source address of the UDP packet. For example, attacker wants his IP address returned for a DNS query, when the resolver ask NS1.google.com for www.google.com. The attacker could reply first, with its own IP (Diaz, Alejandra & Anupam, 2021).

## Malware

Malware is a software used to disrupt computer operation gather sensitive information. It can appear in the form of code, scripts, active content and other software. Malware includes viruses, worms, trojan horses, key loggers, spyware, adware. Client security products are able to detect and remove malware and other potentially unwanted programs. But phishers can make malware undetectable. Key strokes, screen shots, clipboard contents and program activities can be collected and send this information to phishers by e-mail, ftp server or IRC channel (Jampen, 2020).

**ANTI-PHISHING TECHNIQUES**

AntiPhish is based on the premise that for inexperienced, technically unsophisticated users, it is better for an application to attempt to check the trustworthiness of a web site on behalf of the user. Unlike a user, an application will not be fooled by obfuscation tricks such as a similar sounding domain name. AntiPhish is an application that is integrated into the web browser. It keeps track of a user’s sensitive information and prevents this information from being passed to a web site that is not considered “trusted” (Kiren et al., 2020).

In general anti-phishing techniques can be classified into following four categories (Rana, 2020).

**Content Filtering-** In this methodology content/email are filtered as it enters in the victim’s mail box using machine learning methods, such as Bayesian additive Regression Trees or Support Vector Machines (Rana, 2020).

**Black Listing-** Blacklist is collection of known phishing Web sites/addresses published by trusted entities like Google and Microsoft’s black list. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites (Rana, 2020).

**Symptom-Based Prevention-** Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected (Rana, 2020).

**Domain Binding-** It is a client’s browser-based techniques where sensitive information is bind to a particular domain. It warns the user when he visits a domain to which user credential is not bind (Rana, 2020).

**CONCLUSION**

Phishing attacks are still successful because of many inexperienced and unsophisticated internet users. The last years have brought a dramatic increase in the number and sophistication of such attacks. This paper provides a broad survey of various phishing types which are used by attackers to steal the sensitive information. This study clearly shows that phishing techniques enables the attackers to steal the information efficiently. Our future work is to compare various types of anti-phishing techniques and choose the best one for further research.

**RECOMMENDATIONS**

The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy. The following are the recommendations the seminar paper puts forward.

1. Organizations should establish corporate policies and communicate them to consumers and also provide a way for the consumer to validate that the E-mail is legitimate.
2. Stronger authentication at web sites to monitor the Internet for potential phishing web sites.
3. Implement good quality anti-virus, content filtering and anti-spam solutions at the Internet gateway.
4. Automatically block malicious/fraudulent E-mail and detect and delete malicious software.

# REFERENCES

Hadlington, L. (2021). The “human factor” in cybersecurity: Exploring the accidental insider. *Research Journal of Artificial Intelligence Applications in Security, 2(32),* 45-75

Naaz, S. (2021). Detection of Phishing in Internet of Things Using Machine Learning Approach." *International Journal of Digital Crime and Forensics (IJDCF)*, 13(2), 1-15.

Adam, K. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims & Offenders,* 16(3) (2021), 316-342.

Hanus, Y., Andy, W. & James, P. (2021). Phish Me, Phish Me Not. *Journal of Computer Information Systems,* (20), 1-11.

McAlaney, J. & Hills, P. (2020). Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking,” Frontend Development Journal, 11(2), 1–13, doi: 10.3389/fpsyg.2020.01756.

Biswal, C. & Kumar, P. (2021). Cyber‐Crime Prevention Methodology. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications* (2021): 291-312.

Diaz, A., Alejandra, T. & Anupam, J. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), 53-67.

Jampen, D. (2020). Don’t click: towards an effective anti-phishing training. A comparative literature reviews. *Journal of Human-centric Computing and Information Sciences,* 10(2), 1-41.

Kiren, D. & Sunil, N. (2020). "Different Types of Phishing Attacks and Detection Techniques: A Review." *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*. IEEE.

Rana, A. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future of the Internet, 12(10), 1–39, doi:10.3390/fi12100168.

Taylor, P. (2020). "A systematic literature review of blockchain cyber security." *Journal of Digital Communications and Networks,* 6(2), 147-156.