**PHISHING AND ANTIPHISIHING TECHNIQUES**

**EMMANUEL JOSEPH WAKAWA**

**(ST/CS/ND/20/455)**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**august, 2023**

**PHISHING AND ANTIPHISIHING TECHNIQUES**

**EMMANUEL JOSEPH WAKAWA**

**(ST/CS/ND/20/455)**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE**

**august, 2023**

**Abstract**

*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.*

**Keywords:** Phishing, phishing steps, phishing types, Anti-phishing tools.

**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 Diaz (2020). 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 & 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).

**Literature Review**

Phishing victims often do not realize that they have been tricked. The first phase in combating phishing problem is the detection of a phishing attack. We classify these detection methods in two categories: human detection and machine detection.

All technology users are not the same. Some are more knowledgeable about security issues and some think longer before they click on a suspicious link. Users may receive training at work but otherwise most internet users are not particularly knowledgeable. Within an organizational setting common operational procedure, knowledge sharing, and double verification processes can reduce problems. Most technology workers are not familiar with the user interaction model of the information systems that they use. Hence it becomes easier for the phishing attackers to mimic the web interface of some familiar webpage and lure the user to enter their private information that is then transmitted to the attackers (Hanus *et al.,* 2021).

An overview of phishing education is presented in Biswal *et al*. (2021. This work focuses on context aware attacks and introduces a strategy for educating users by combining phishing IQ tests and class discussions. However not all potential victims have the advantage of formal classroom training and simply presenting the information in an email or a webpage is of limited effectiveness

To explore the effectiveness of embedded training, researchers conducted a large-scale experiment that tracked workers' reactions to a series of carefully crafted spear phishing emails and a variety of immediate training and awareness activities. Based on behavioral science findings, the experiment included four different training conditions, each of which used a different type of message framing. The results from three trials showed that framing had no significant effect on the likelihood that a participant would click a subsequent spear phishing email and that many participants either clicked all links or none regardless of whether they received training. The study was unable to determine whether the embedded training materials created framing changes on susceptibility to spear phishing attacks because employees failed to read the training materials (Naaz, 2020).

Anti-Phishing Singh et al. (2015) is an online game that teaches users good habits to help avoid phishing attacks. It was designed according to learning science principles. During a study participant who played the game were better able to identify fraudulent web sites. Again, however, such training approaches are only useful if potential victims take the training.

Another study reports findings from a multi-method set of four studies that investigate why we continue to fall for phishing attacks. The study found that phish are becoming more effective and that the use of logos in a phish email makes it more convincing.

Hale *et al.* (2015), examined another game based approach that seeks to incorporate learning techniques and combines the realism of in-the wild approaches with the training features of testing. This work proposes a three phase experiment to test the approach on a customized Cyber Phishing simulation platform.

**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 (Hanus *et al.,* 2021). It is possible to send a message that appears to be from anyone anywhere saying whatever the sender wants it to say.

## 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 (Biswal *et al*., 2021). The shadow copy is funneled through attackers’ machine. 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. 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.

## 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 (Diaz et al., 2021). 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.

## 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 (Jampen, 2020). 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.

**Typical Process of Phishing**

Kiren *et al.* (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 (Naaz, 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 (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 (Biswal & Subhendu, 2021). A man-in-the-middle attack uses Trojan horses to intercept personal information.

**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 (Kiren *et al*., 2020). 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”. 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.

**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.

**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.

**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.

**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

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

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.

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

Hale, M., Gamble, R. & Gamble, P. (2015). Cyber Phishing: A Game-Based Platform for Phishing Awareness Testing, *In: 2015 48th Hawaii International Conference on System Sciences IEEE,* 15(2), 5260–5269.

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

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.

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

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.

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

Singh, Y., Maravi, S. & Sharma, S. (2015). Phishing websites detection through supervised learning networks, *In: 2015 International Conference on Computing and Communications Technologies (ICCCT),* 13(1), 61–65.

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