A Study of Phishing And Countermeasures

John Odi Etta
MSc. Cyber Security &pen Testing

Middlesex University.

Abstract

In the world today, cybersecurity is a major challenge and Phishing is one of the most common cybersecurity threats and cybercrime plaguing the internet space. Phishing though seems harmless on the onset is behind some of the biggest cyberattacks ever recorded. It basically involves luring unsuspecting internet users into willingly giving out sensitive and confidential information to an attacker and sometimes the attackers can collect the required information themselves by monitoring the victim's machines with key loggers. This information may include credit card details, login credentials, bank details, etc. but not limited to these few. Attackers can also target specific organizations and individuals within such organizations for corporate espionage, and other malicious intentions. The oldest and most commonly used phishing attack is the email phishing attack which occurs by an attacker sending out deceptive or malware-laden emails to victims compelling them to act on the email received. Over the years, phishing has evolved and attackers are getting more and more sophisticated in their schemes. The question now is "is there adequate security at present to completely deal with the issue of phishing?" This paper presents a concise study of phishing attacks and several countermeasures that can be implemented to mitigate phishing.

Keywords: Phishing, deceptive phishing, malware phishing, Countermeasures.

INTRODUCTION

Phishing first reported in 1996 was a term used to describe an event of theft of America Online (AOL) passwords and accounts by hackers. At the time it simply referred to that event. But as time went on, the concept of phishing also evolved. Present-day phishing involves the use of several attack vectors such as emails, SMS, social media, voice calls, malware, and man-in-the-middle attacks to lure victims and have them disclose personal information [1],[4]. The concept of phishing started off as emails being sent to unsuspecting victims to deceive and have them reply to such malicious mails with their legitimate information as requested by the mail. Even today, this is still the most common and widely used medium to conduct a phishing attack.[1] Phishing establishes a significant point of interest in terms of security for Internet Service Providers (ISPs), email service providers, browser vendors, domain registrars, cloud service providers, and law enforcement agencies. To enable them to mitigate these attacks, an array of solutions has been proposed, comprising of both technical and non-technical approaches to address the different levels that constitute a phishing attack. At the first level, emphasis is on preventing phishing emails from reaching the end users by applying email filtering techniques, detecting and blocking, or completely removing phishing websites [2],[5]. Similarly, on the client-side which is browser-based, existing solutions focus on providing better user interfaces, such as browser plugins or addons, that inform users about the reputation of a target website and notify them as soon as they are redirected towards a potentially malicious page. Finally, the last line of defense relies on proper education to help users gain basic knowledge in recognizing phishing emails and sites [2] [6].

Regardless of the impressive efforts in mitigating phishing attacks, the issue of phishing is far from being completely eradicated as a report by the Anti-Phishing Working Group (APWG) shows that the number of phishing sites is still on the increase and phishers are getting more advanced and sophisticated in their schemes [2][15]. In order to fully understand the concept of phishing, security researchers in Academia, Law enforcement, and corporate society have put in tremendous effort in research to mitigate the issue of phishing mostly from the technical point of view which comprises how attackers are able to gain access to vulnerable servers, how phishing toolkits work and the remote analysis of existing phishing sites based on available datasets such as stamptraps and phishing blacklists to provide actual statistics on the effectiveness of phishing attacks and proffer solutions [2].

This paper deals with related works in section II, which reviews previous research carried out on issues bordering around phishing attacks and ways to mitigate them. Section III describes the methodology used in the gathering and analysis of materials considered suitable for this research, Section IV provides extensive details of the techniques and methods employed for an effective phishing attack to be carried out and some countermeasures. Section V critically analyses the most effective countermeasures as discussed in section IV and finally the paper is concluded in section VI with a bit of a recommendation on future works.

II. RELATED WORKS

In spite of the fact that various studies have been carried out on the issue of phishing and its mitigation, there is still more work to be done in this regard as there is little to no standard mitigation against phishing. Mitigation and phishing countermeasures are for the most part dependent on how much knowledge victims have on phishing techniques and their ability to identify a phish. Xiao Han et al propose a sandboxed technology, inspired by APWG's Global Phishing Survey which indicated that 71.4% of domains that hosted phishing sites were compromised domains. The sandboxed technology was designed to neutralize a phishing toolkit while keeping it in operation for the entire duration. The approach was further designed to ensure the victim's privacy without interfering with the attack process [2] [15]. Similarly, (Antonio San Martino and Xavier Perramon 2009) propose a mutual multifactor authentication, which if

properly implemented, helps to detect and prevent phishing attacks. Such authentication process comprises key exchange, server authentication, and user authentication to provide security [3]. However, Ahmed Aleroud & Lina Zhou in their research suggest a multi-dimensional taxonomy that is not limited to traditional phishing channels such as e-mails and spoofed websites but explores other phishing channels like mobile apps, social networks, instant messaging, etc. to address phishing environments, techniques, and corresponding countermeasures and also identify the characteristics of phishing attacks on emergent communication media [4]. The research revealed several frontiers of countermeasures that were not considered in earlier research; such as human users, otology, and search engine-based countermeasures.

III. METHODOLOGY

Research for this work was carried out by extensively going through research repositories and databases that have works relating to phishing, its environments, how phishing is conducted, why people fall for phishing scams, and countermeasures. They include Elsevier, Google Scholar, ACM Digital Library, ResearchGate, IEEE Xplore, and other websites. The materials obtained from these sources were carefully examined and analyzed to aid in the production of this paper in areas bordering around the study of phishing and countermeasures with sections on the evolution of phishing, how phishing actually works, various media through which phishing can be carried out, types of phishing scams and how to identify a phish line.

A total of 11 papers with similar problem statements were selected to be used to shed more light on the issues identified herein and how to mitigate them. Subsequently, it was discovered that a very important aspect in the fight against phishing has for the longest time been overlooked or paid little to no attention to. This is the human factor in phishing attacks. From the analysis of this previous research on phishing, it was concluded that for any phishing attack to be successful, there has to be a human input [4], which can also be viewed in two ways. First, with adequate knowledge of phishing and the ability to identify a phish Link, the human in this case can prevent a phishing attack. The second is that the human has little to no knowledge of phishing and cannot identify a phish Link. In this case, the human unknowingly becomes a facilitator in the attack process. This then brings us to a conclusion that the human factor plays a very important role in mitigating phishing attacks. A fundamental question, therefore, has been put forward; How can the human factor be harnessed as the last line of defense against phishing attacks, bearing in mind the evolution and sophistication in modern phishing techniques?

IV. PHISHING METHODS AND TECHNIQUES.

Phishing has been categorized into two categories; deceptive phishing and malware-based phishing [5]. These depend on three distinct components employed to facilitate a successful attack. The components to execute a phishing attack include a medium, a vector, and the technical approach to be employed [7]. The phishing medium refers to the method through which the attacker can communicate with the victim, and it is also the first thing to be considered for an attack as it defines the vector and technical approach to be applied in a specific attack. Some media that can be explored in phishing include; voice interactions, short message service (SMS), and the internet. Phishing vectors depend largely on the medium being used by the attacker as represented in Fig1.

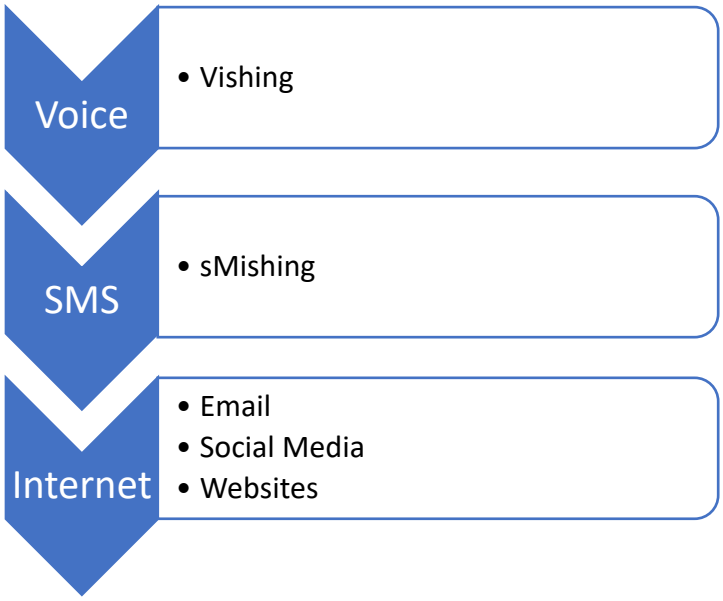

Fig 1.

DECEPTIVE PHISHING

Deceptive phishing technique is associated with the use of social engineering schemes, which largely employ the use of fraudulent email claims that seem to originate from a legitimate domain, individual, company or bank as the case may be [5]. Subsequently, with a link contained in the email, the attacker attempts to lure and redirect victims to a fake website that has already been designed for the purpose of fraudulently collecting personal, financial, and sometimes corporate information from victims and transmitting same to the attacker.[5],[16] All forms of deceptive email phishing attacks generally follow a specific lineup of events that leads to a successful attack. Fig2 distinctively outlines the basic steps involved for a successful deceptive phishing attack [6]:

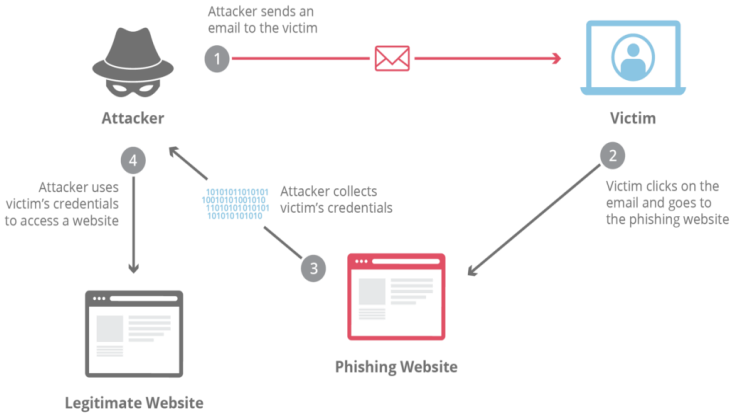

Fig 2.[20]

- The attacker sets up a phishing website for the attack.

- The Attacker sends emails with a sense of urgency or call for action that requires the recipient to click on a link.
- The victim is deceived by the email into clicking the link which then redirects to the phishing website and takes action that makes them vulnerable to confidential information compromise.[6]
- Victim's personal information is transmitted from a phishing server to the phisher.
- Attacker makes use of the information of the victim on a genuine website and impersonates the victim's identity to gain access [6], [13][17].

Deceptive phishing comprises mostly the use of emails to prey on or lure victims into divulging sensitive information. some examples of phishing emails are given below;

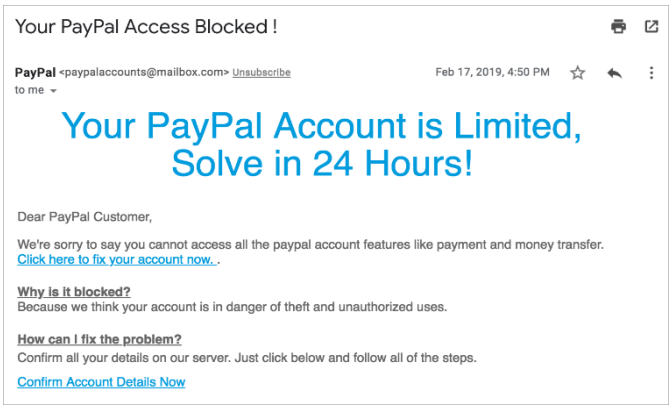

Fig 3.[18]

In the above figure, we see an example of a phishing email on a user's PayPal account, stating that the account has been blocked due to the danger of theft and unauthorized use, A link that suggests the solution has also been provided.

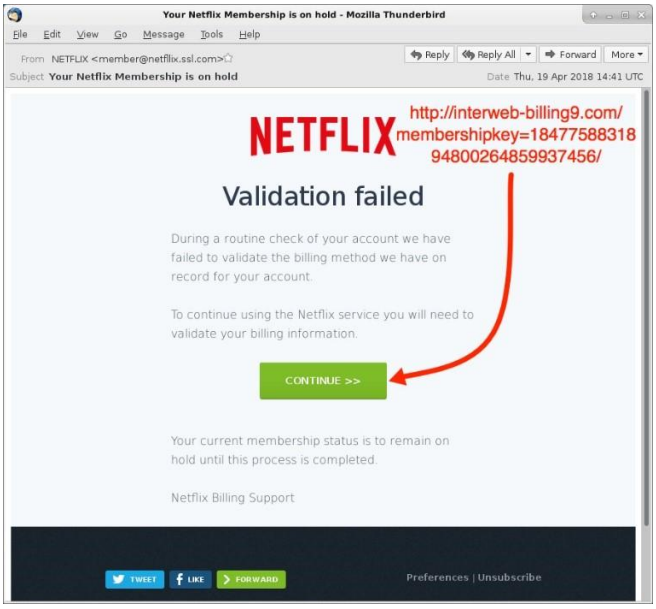

Fig4[19]

In Fig4, we see a similar email sent to a Netflix user explaining why this user's membership had been placed on hold. The e-mail further suggests the user validate their billing information to continue enjoying Netflix services.

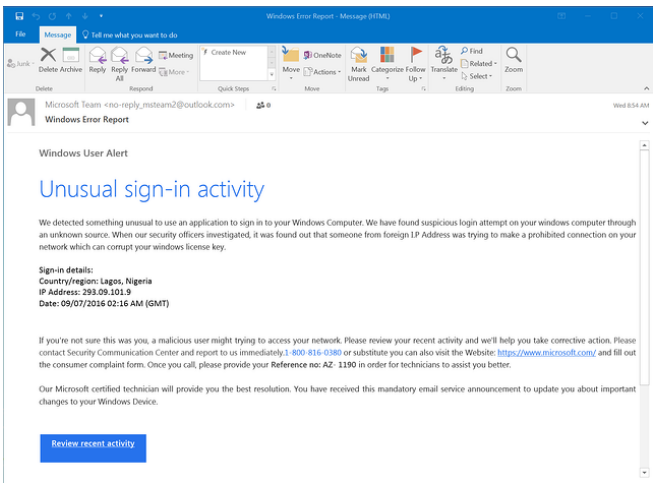

Fig 5.[18]

The second category of phishing as earlier stated is malware-based, which includes the application of technical schemes that depend on malicious scripts or malware as remote access tools to gain access via a backdoor to the user system either by downloading an email attachment or after the user clicks on an embedded email link [5]. These malicious codes which may be viruses' worms, keyloggers, spyware, ransomware, and sometimes adware can also detect and use already existing security vulnerabilities in the user's computer to monitor and collect the information directly [5] [8] [16].

Examples of malware phishing are given below;

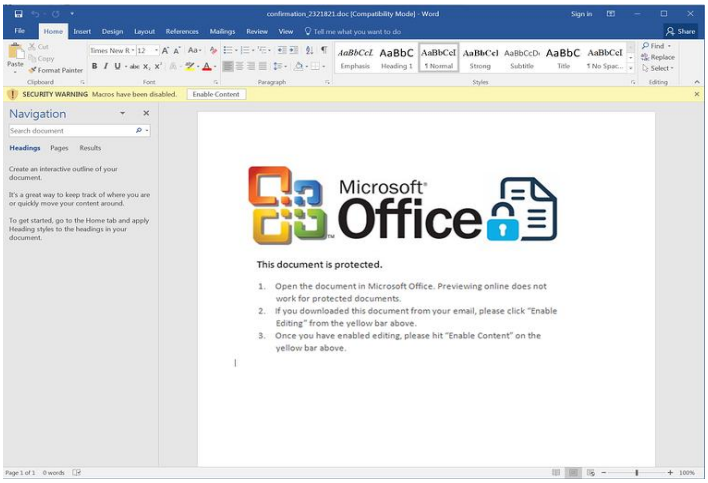

Fig 6[18]

It can be seen here that the document looks like a legitimate Microsoft Word document. But it has a malicious macro (executable script or program) attached. Which when enabled delivers its payload on the victim's machine.

PHISHING COUNTERMEASURES.

In the campaign against phishing, several countermeasures have been proposed to mitigate the issue of phishing. Countermeasures and anti-phishing techniques can be classified into three main categories: server-side anti-

phishing, browser-side anti-phishing, and online training anti-phishing strategies.

Server-based schemes refer to those requiring server authentication to defend against phishing attacks [6][8].

An apparent direct authentication approach is for clients to verify the credential presented by a web server, and such credential is usually issued by a trusted third party which provides assurance on its bearer's identity [6]. Similarly, the implementation of some security standards to determine the origin of an email and detect email spoofing further adds another level of security on the server-side against a phishing attack. One of such is the Sender Policy Framework (SPF) which integrates Simple Mail Transfer Protocol (SMTP) to reject emails from fake addresses and adds a list to DNS records that include all servers that are authorized to send emails.[10],[12] And the second, DomainKeys Identified Mail (DKIM), which basically refers to how an email server digitally signs outbound mails, ensuring that an email originated from a specific domain and has not been tampered with in transit [12.

Client-side browser-based countermeasures against phishing attacks include the utilization of anti-phishing plug-ins or addons in Web browsers, enabling the browser to regulate web page's visual behaviors to detect phishing [6]. Some browsers come with a form of anti-phishing mechanism already preinstalled. Browser side anti-phishing techniques based on existing plug-ins are roughly categorized by four distinct approaches: Blacklist-based, Visual-clue-based, Webpage-feature-based, and Information-flow-based phishing detection mechanism [6],[13].

Anti-phishing education emphasizes the use of online training materials, testing, and situated learning as end-user education minimizes user vulnerability to phishing attacks and further backs up the technical countermeasures of phishing. It is observed that most successful phishing attacks are facilitated by human error and the inability of users to detect or suspect a phish; nonetheless, existing phishing detection training does not provide complete protection against current sophisticated attacks, but it goes a long way in providing users and potential victims some basic knowledge of phishing and how to identify phishing emails. [6],[14]. Interactive solutions like PhishMe use immersive educational methods to coach employees to recognize phishing attacks. And Wombat which is a tool that assesses employee vulnerability to attack and further motivates them to require training by periodically sending mock phishing emails to test their susceptibility levels can be used to promote anti-phishing education [16]

CRITICAL ANALYSIS

Social engineering techniques basically rely on human interaction and most often than not, deception or exploitation of human nature using tricks aimed at coercing victims to agree to and do things they would not have done normally. By exploiting victims' limited security knowledge or awareness and sometimes weaknesses, phishers deceive other unsuspecting internet users into divulging their sensitive information or download attachments that can inject malicious software onto their systems to grant the attacker unsolicited access [4]. Here, we will consider some client-side anti-phishing tools the extent to which they can detect or protect users against phishing, and their inherent limitations.

Tools	feature	limitation
Google Safe Browsing	Makes use of a blacklist of phishing URL to identify a phish site.	Unable to recognize phishing sites not present in the blacklist.
SiteAdvisor	Protection against spyware and adware attacks	Unable to detect a phishing site if it is not rated in the SiteAdvisor database.
Netcraft Toolbar	Assess phishing probability of sites to determine the age of domain registration.	Might not recognize new phishing sites unless it is already flagged in its database.
PILFER	Makes use of machine learning-based approach to classify emails as a phishing or legitimate e mail.	Not many parameters are used in the classification process
Pshark	Detects phishing emails, locates host server, and reports server to the administrator.	Does not have an email filtering technique and cannot stop an initial phishing email.
PhishWHO	Phish site detection using identity keywords extraction and target domain finder.	Does not recognize visual website cloning.

From the table above, an inference can be drawn regarding the fact that no single tool or technique can be used to adequately and conclusively stop phishing attacks (cybersecurity in general) but by the application and implementation of a combination of these tools and other countermeasures, phishing can be properly checked.

CONCLUSION

In recent times Phishing has become a very common method for attackers and other malicious internet users to collect all sorts of sensitive information ranging from organizational information, financial records, and personal individual data from unsuspecting users [1],[11]. Phishing also involves the use of social engineering techniques where

the attacker collects sensitive information by tricking the victim into providing the required information, instead of extracting it directly from a computer system [1]. This is and will remain a major challenge in the cyber security sphere for a while as phishers are getting more innovative in their schemes. Another difficulty faced in mitigating phishing attacks is the ability to distinguish phishing websites from legitimate sites as these attackers come up with more innovative and sophisticated ways to evade detection. A recent development seen on newer phishing sites is the use of SSL by phishers to make their sites seem more genuine.[7] Therefore more effort should be put into mitigating the ever-evolving threat phishing poses on cyber security.

REFERENCE

1. Anders Persson "Exploring Phishing Attacks and Countermeasures" Master Thesis in Computer Science Thesis No: MCS-2007:18 September 2007
2. Xiao Han, Nizar Kheir, & Davide Balzarotti. 2016. PhishEye: Live Monitoring of Sandboxed Phishing Kits. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 1402–1413. DOI: https://doi.org/10.1145/2976749.2978330
3. Antonio San Martino & Xavier Perramon" Phishing Secrets: History, Effects, and Countermeasures" International Journal of Network Security, Vol.11, No.3, PP.163–171, Nov. 2010
4. Ahmed Aleroud, Lina Zhou," Phishing environments, techniques, and countermeasures: A survey, Computers & Security", Volume 68, 2017, Pages 160-196, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.04.006
5. Chawla, M. and Chouhan, S.S., A Survey of Phishing Attack Techniques. International Journal of Computer Applications, 975, p.8887.
6. H. Huang, J. Tan and L. Liu, "Countermeasure Techniques for Deceptive Phishing Attack," 2009 International Conference on New Trends in Information and Service Science, 2009, pp. 636-641, doi: 10.1109/NISS.2009.80.
7. Rana Alabdan "Phishing Attacks Survey: Types, Vectors, and Technical Approaches" Future Internet 2020, 12, 168; doi:10.3390/fi12100168
8. Website Security Store "Malware-Based Phishing Attacks 101: What is Malware Phishing"? July 30, 2021 web security. https://websitesecuritystore.com/blog/what-is-malware-phishing-attack/
9. T.Y MEZQUITA 2019 https://cyberhoot.com/cybrary/phishing/
10. Christian Kirsch "Get Off the Hook: 10 Phishing Countermeasures to Protect Your Organization" Sep 11, 2015 https://www.rapid7.com/blog/post/2015/09/11/phishing-countermeasures-to-protect-your-organization
11. Purkait, Swapan. (2012). Phishing counter-measures and their effectiveness - Literature review. Information Management & Computer Security. 20.10.1108/09685221211286548.
12. Hong, Jason. (2012). The State of Phishing Attacks. Commun. ACM. 55. 74-81. 10.1145/2063176.2063197.
13. H. Huang, S. Zhong and J. Tan, "Browser-Side Countermeasures for Deceptive Phishing Attack," 2009 Fifth International Conference on Information Assurance and Security, 2009, pp. 352-355, doi: 10.1109/IAS.2009.12.
14. Alkhalil, Z. Hewage, Nawaf, L. Khan ,I (2021) "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy". Front. Comput. Sci.3:563060. doi:10.3389/fcomp.2021.563060.
15. Xiao Han "Measurement and Monitoring of Security from the perspective of a service provider" Ph.D Thesis TELECOM ParisTech Computer science and Networking. Sep 2017
16. V. Suganya" A Review on Phishing Attacks and Various Anti-phishing techniques" International Journal of Computer Applications (0975–8887)Volume 139 – No.1, April 2016 20
17. Okesola, J.O. Adewole, O.A. Sorunke I. I "Understanding Phishing and Phishing Techniques in Client-Side Web-Based Systems" A Quarterly Publication of the Faculty of Science, Adeleke University, Ede, State of Osun, Nigeria http://www.jasra.adelekeuniversity.edu.ng/
18. https://www.knowbe4.com/phishing
19. https://www.malware-traffic-analysis.net/2018/04/20/index.html
20. https://www.cloudflare.com/learning/access-management/phishing-attack/