PHISHING ATTACKS:RAISING AWARENESS AND DEFENDING

ABSTRACT

Phishing is a type of social engineering attack that can be used to steal sensitive and important information and details from unsuspecting entities, either organizations or individuals. This document describes how phishing attacks are carried out, what protection techniques are needed to counters such attacks, and uses his MINDSPACE framework at the University of Bournemouth to test such attacks. It gives you an overview of how to increase your awareness. That is, protection technology is grouped into three layers . Automated tools, training and skills, and multi-factor authentication. Using the MINDSPACE framework to raise awareness found that approximately 50% of targeted students were unaware of his phishing attack and the tactics used to carry it out .

Keywords— Phishing, MFA, MINDSPACE

I. INTRODUCTION:

The emergence of the internet and its growth rate has been proven to have great benefits for technology and as the internet develops threats also appear. cyberbullying and cybercrime, and one of them is called phishing . Phishing attacks initially started on messaging platforms but later spread to social networking sites, voicemail, messaging, multiplayer games, and even instant messaging, and these are platforms used daily by a large number of individuals many of whom are unaware of the wars. technique used by phishing attackers. 4044 Xiong et al. propose that phishing is a 4044 social engineering attack that transmits a message with the aim of causing 4044 potential victims to take certain actions (such as clicking on hyperlinks or hyperlinks). ineffective, 4044 opening or downloading embedded malware attachments or entering credentials into copied websites) resulting in the victim revealing confidential information from which to benefit to the attacker . Hong suggests that most of the phishing attacks use social rather than technical techniques, and that convey a sense of urgency to get the attention of potential victims. This begs the question, how are individuals aware of the phishing tactics used by these attackers? What protection techniques does know about? This study is intended to educate and inform people about techniques to protect against phishing attacks. This will be achieved through the use of secondary 4044 data and awareness will be enhanced through the use of the MINDSPACE 4044 framework that will help 4044 individuals know and recognize an attack before it occurs.

II. LITERATURE REVIEW:

The effectiveness of the scam can be attributed to its use of social engineering techniques in social media platforms and this to the fact that users of social media platforms share too much personal information about them. attackers perform phishing attacks to exploit the cognitive biases of their potential victims by pretending to be trusted organizations or individuals and sending phishing messages email and social media platforms such as Facebook, Instagram, Twitter and many others to a large number of potential victims. 4244 Ali asserts that various types of phishing techniques can be used to carry out the attacks, and these techniques include: phishing 4244 through compromised web servers, phishing 4244 by means of compromised web servers. using botnets and many other techniques. Banu and Banu also recognize different types of scams used by attackers such as clone scams, online scams, phone scams, DNS scams also known as medicine. It should be noted that each of these 4244 types of phishing attacks have specific techniques 4244 used by attackers, and although a lot of research has been conducted 4244, the problem deals with 4244 This scam is still a concern for many researchers. In 2020, European Union cybersecurity agencies said that there had been a 667% increase in phishing attacks in just a month during the COVID-19 pandemic. During the last quarter of 2019, 4336 74% of phishing websites started using 4334 Secure Hypertext Transfer Protocol (HTTPS) which is used to secure 4334 communication in computer networks and showed that a or the site is safe and secure. In addition, a recent study by the European Union's Cybersecurity Agency found 4244 that 88% of organizations worldwide I have experienced spear phishing attacks. This is also a form of phishing that targets specific entities. Phishing campaigns are changing, evolving rapidly from small to fully automated processes. Most phishing sites

available today use these toolkits, allowing attackers to We make it easy to create the content necessary for an attack and route the stolen data appropriately. In 2018, 32% of the data breaches were initiated by phishing attacks, and 78% of the backdoor installations and uses were also related to his phishing attacks. According to Chaudry et al. In 2014 he was observed by the Anti-Phishing Working Group (APWG) that a record average number of 255,000 malware variants of he were detected. This was due to a phishing attack.

III. HOW PHISHING IS IMPLEMENTED:

Chaudry et al. argue that phishing attacks have both a social engineering and a technical aspect and this is because the attacker uses both social engineering tactics but also requires technical knowledge of the system that a potential victim has in order to get through the security measures the victim will adopt. The social engineering aspect of scams can be classified into three factors; curiosity, fear, and empathy. Curiosity: This is often exploited when attackers send emails containing links to malicious websites or websites. When the user sees the link sent , he is curious to know where it leads. Fear: This tactic is used by attackers to instil fear in the minds of potential victims. An attacker could send an email to a potential victim alerting him to multiple attempts to access his bank account or another online account and asking him to verify his identity by sending a malicious link, thereby causing panic and fear in the victim. Empathy: This is often taken advantage of when an abuser sends messages toying with a potential victim's feelings by impersonating a friend or loved one or even an organization is looking for relief or aid for victims of the earthquake or flood asks the financiers, prompting them to click on any malicious links sent to potential victims. 4244 The technical aspect of phishing generally depends on the type of phishing attack 4244 is being performed although there are some general 4244 technical tricks that most attackers use, such as:

- Email Spoofing: This is done to change the original email sender address in order to lure potential victims.
- Fast Flux: A technique used by phishers to host phishing websites on multiple computers, frequently updates the IP address of phishing websites on their DNS servers. This is so that if one of the phishing sites goes down, another phishing site can easily take its place.
- Phisher commonly uses logos, images and trademarks associated with certain brands and organizations. A attacker could identify it as the sender and sender of the email.
- Phishers can hide and encode website URLs.

IV. PROTECTION TECHNOLOGIES:

Protection against phishing attacks is provided by a variety of tools and techniques:

1. AUTOMATION TOOLS

Various automations for phishing detection:

- such as servers containing links contained in phishing emails. Tools are implemented.
- A database containing blacklisted URLs and domain names. These blacklists are divided into two. Domain/URL Blacklist , which contains domain names and URLs that are blacklisted for malicious intent, and Internet Protocol Blacklist , which is a blacklist that contains blacklisted IP addresses , are configured. increase. Change status .
- Intrusion Detection and Intrusion Prevention The system is also a tool implemented to protect against phishing. These tools are primarily used by organizations and are set up on networks to detect and prevent attacker intrusion .

2. 4844 Training and Knowledge:

Educating users on how to access their information 4844 is a useful technique that can be used to protect against phishing [14]. The publication of online scams by 4244 academic institutions, government organizations and even 4244 NGOs is the most basic but least common approach taken in training and communication. permissions for 4244 users with knowledge of scams. Xiong et al. suggest that procedural knowledge regarding equipping users with skills on how to identify phishing sites is key to improving the effectiveness of phishing alerts, from that makes the user aware of the website.

3. Multi-Factor Authentication (MFA):

4044 Chaudhry et al. suggest that it is necessary to replace 4044 Multi-Factor Authentication which typically involves users entering 4044 of their credentials (username and password) to visit a system or website that has multi-factor authentication systems. Instead of just requiring to enter a username and password, Multi-Factor Authentication requires users to provide at least two verification factors such as facial recognition, fingerprint, or password to use one. times (OTP) to access the system or account online. MFA helps to reduce fraudsters' attempts to gain access to systems or online accounts, making it an effective method and means of providing enhanced security, thus creating a layer of security. additional protection. Three different types of authentication factors are possible in MFA function and they are: What you know: This is authenticated with a password or PIN . What are you: This is authenticated with biometric data such as fingerprints and iris scans. What you have: This is authenticated by the type of device one has, such as a smartphone. It should be noted that no protection technique works 100% but having as many as possible can help attackers work harder.

V. METHODOLOGY:

The MINDSPACE Framework will be used to raise awareness of phishing attacks in the Bournemouth University community through the University Student Union, which will help educate the University community about dangers and impacts of these attacks. MINDSPACE is a framework used to influence behaviour and is used by individuals and organizations to support and improve policy and decision making . As seen in Table 1 side Below, the different factors of MINDSPACE and how they can influence behaviour are briefly explained.

VI. RESULT AND DISCUSSION:

The MINDSPACE framework was introduced to the student federation body at Bournemouth University and they implemented fraud awareness using the framework. Scams approached with prior knowledge of the scam. phishing attacks, although many of them are unable to identify or recognize when an attack is about to begin. It should be noted that notification was contacted and approached by the student union using the MINDSPACE framework regarding phishing attacks indicating that although 50% of the students approached knew about phishing attacks without their knowledge. and do not know about techniques to protect against these attacks and the remaining 50% do not know about phishing attacks, the tactics used by attackers and related protection techniques .

VII. STRENGTHS AND LIMITATIONS:

The MINDSPACE framework has certain strengths including a number:

- Easy to use and very cost effective .
- Provide a timely and direct method of decision making to facilitate behavioural change in individuals and other entities .4344
- It does not need to be used by an expert and can be used by anyone .
- Helps to improve decision making and policy making.

4044 A major limitation of MINDSPACE is that the reflective 4044 system and other potential behaviour-altering factors are often overlooked by the 4044 framework, making it less comprehensive than it should be This study was conducted on an evaluation basis and that makes it subject to bias for further study and analysis.

VIII. CONCLUSION:

Facts and statistics produced by scholars based on research have shown that phishing attacks are steadily increasing and thus have become the cause of concern because many people and organizations are experiencing these attacks on a daily basis and this is due to the lack of user awareness and protection . This shows that to combat these attacks, It is important to raise awareness and implement the right techniques to protect against these attacks. Consistent and up-to-date training can be effective in making individuals aware and less vulnerable to phishing attacks.

REFERENCE:

[1] O. F.W. Onifade and K.J. Adebayo, "Vdetector: Attacking Attackers Against Phishing and Internet Identity Thieves", Information Journal Impact Technology, vol. 11, no. 2, p. 133–144, 2011.

[2] J. A. Chaudhry, S.A. Chaudhry và R.GRittenhouse, «Phishing attacks and defenses», International Journal of Security and Its Applications, vol. 10, no. 1, p. 247–256, janv. 2016, doi: 10.14257 / ijsia.2016.10.1.23.

[3] A. Xiong, R.W. Proctor, W. Yang et NLi, "Integrating Training into Alerts Improves Scam Site Recognition Skills ", Human Factors: Journal of on Human Factors and Socio-Economics, vol. 61, no. 4, p. 577–595, December 2018, doi: 10.1177 / 0018720818810942.

[4] J. Hong, "State of Phishing Attacks", ACM Communications, vol. 55, no. 1, p. 74, January 2012, two: 10.1145 / 2063176.2063197.

[5] ED. Frauenstein and S. Flowerday, "Scam Resistance on Social Networking Sites: A Model of Personal Information Processing ", Computers & Security, vol. 94, p. 101862, July. 2020, doi: 10.1016 / j.cose.2020.101862.

[6] X. R. Luo, W. Zhang and A. Seazzu, " Surveying Fraud Victims with the System-System Model : A Theory and Discovery Framework", Computer & Security, vol.38, p. 28–38, October 2013, doi: https://doi.org/10.1016/j.cose.2012.12.003.

[7] A. Ali, "Social Engineering: Recent and Future Fraud Techniques ", March. 2015.

[8] M. N. Banu and SM. Banu, "An In-depth Study of Phishing Attacks", International Journal of Computer Science and Information Technologies, vol. 4, no. 6, p. 783–786, 2013.

[9] E. D. Frauenstein and S. Flowerday, "Scam Resistance on Social Networking Sites: A Model of Personal Information Processing ", Computers & Security, vol. 94, p. 101862, thg 7 2020, doi: 10.1016 / j.cose.2020101862.

[10] «Ransomware ENISA Threat Landscape EN EN». Chương . Disponible: https://www.enisa.europa.eu/topics/threat-risk management /nace-and-xu hướng / etl-review-folder / etl-2020-444 ransomware.

[11] M. Cova, C. Kruegel and G. Vigna, "There are no free scams: an analysis of 'free' and live phishing kits", in WOOT, 2008, vol. 8, no. 10, p. 1–8.

[12] CCrane, "20 Scam Statistics to Keep You Addicted in 2019", thesslstore.com, July 24, 2019: https://www.thesslstore.com/blog/20-phishing-stosystem-to-keep-you- from- get-hook-in-2019 (accessed November 9, , 2021).

[13] Z. Ramzan, «Phishing attacks and countermeasures», Handbook of Information and Communications Security, 2010.

[14] P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, and IVlaev, "Influential Behavior: The Path of Mental Space ", Journal of Economic Psychology, vol. 33, no. 1, p. 264–277, February 2012, doi: 10.1016 / j.joep.2011.10.009.

[15] M. O'Sullivan, C. Ryan, D. G. Downey and CM. Hughes, "Behavior Change: Finding the Right Balance 4244 for Research and Policy," International Journal of Clinical Pharmacology 4244, Vol. 38, no. 5, p. 1027-1031, July. 2016, doi: 10.1007 / s11096-016-0351-0.

[16] OneLogin, «What is Multi-Factor Authentication (MFA) and how does it work? », OneLogin, 2019. https://www.onelogin.com/learn/what-is-mfa (Consulté 01 décembre 2021)