The Many Faces of Phishing: Leveraging Multi-Factor Authentication as a Holistic Defense Strategy

Felipe Trinidad Pilier, Faneeza Geronimo, Le Fang, Angel Rivera

I. PROBLEM BACKGROUND

Human error has historically been one of the most significant attack surfaces in the cybersecurity field. It does not matter how strong an encryption method is used or how well-guarded assets are; if the users authorized to access sensitive information forfeit credentials, the associated systems are vulnerable to compromise. The success of social engineering lies in exploiting human psychology rather than exploiting technical vulnerabilities.

Social engineering has five stages: reconnaissance, pretexting, exploitation, execution, and exit. In the initial stage, reconnaissance, the attacker gathers information about the target. This target can range from an individual to an entire organization. The goal of this stage is to perform the necessary due diligence to develop a strategy for the attack. One example of this would be to search in an organization's website to find the contact information of its employees. The next stage is pretexting, where the attacker establishes contact with the target under a made-up identity. The attacker then creates a scenario to coerce the target into forfeiting sensitive information. This specific process is called staging. The attacker impersonating an organization's information technology support department and claiming they need access to a restricted area is an example of pretexting. After a situation is staged, the attacker can move onto the exploitation stage. At this point, the attacker has already created a situation designed to put the victim under pressure. From here, the attacker will engage with the target and perform the script they have written. The general goal of this step is to coerce the user into giving important information, such as credentials. In email phishing, this will be clicking on a malicious link. In vishing, this will be telling the attacker their information. We will discuss both of these attack methods in this paper. This stage is very volatile as it will entirely depend on how convincing the attacker has been and how thoroughly they completed the previous steps. If the attacker is successful in exploitation, they then have access to the restricted assets and can begin their attack. The execution involves stealing data, installing malware, or gaining unauthorized access to systems. The final step in social engineering is the exit phase. In this phase, the attacker will attempt to erase traces of their presence to avoid detection until the target does not realize what happened, which is too late. This may involve disguising the attack itself, disabling logs, and deleting the communication traces.

In this paper, we will be examining social engineering and its eventual lead to phishing. We will also propose a holistic approach to tackle all types of phishing simultaneously.

II. PHISHING

Over the years, technology has advanced radically and taken over our lives, from what we watch to our phone communication, social media, guarding our bank accounts, etc. Almost everything in today's world needs a password to be accessed; therefore, we assume that it is being protected. Unbeknownst to the primary user, our passwords are not the only thing we need to be protected from the cyber criminals out there today. There are many different forms of threats that can take place to collect information and eventually uncover a user's password and cause havoc in their lives for years to come. According to Rick Walsh and Emilee Rader, over 65 billion usernames and passwords were sold to a website known to many in May of 2024 [1]. Not only does this compromise the user for the specific webpage, but it also compromises other accounts due to a high statistic of 1 in 10 people reusing their passwords across various sites. Companies have introduced multifactor authentication to combat issues with protecting accounts, but phishing is still terrorizing the nation. It is essential to understand how phishing evolved as a form of threat to sensitive data to gather an understanding of the different forms of phishing and the impact it has had on users over the years. It is also important to understand how to prevent and mitigate the nuisance of phishing and all of its subparts. Furthermore, learning about future trends in phishing can help a user or a company stay safe from these attacks.

The term phishing coined in the late 1970 's, derived from the idea that the attackers were fishing for the users' passwords and credentials on the web but was made more apparent in 1996 when a hacking

group used the attack method to gather America Online (AOL) usernames and passwords [2]. Over 2.4 billion accounts were compromised, and multiple different forms of data were exposed in the data breach.

When it comes to defining what phishing is, there are many different definitions that exist, therefore causing several issues when scientists are conducting research and comparing data. According to researchers at Khalifa University, UAE, phishing is categorized as a social engineering attack that exploits the weakness in system processes caused by system users [3]. The most common type of phishing is known as deceptive, where the attacker creates an email that impersonates a legitimate company email and then aims to gather the receiver's personal information. The attackers usually conduct preliminary research to see what companies the user is associated with to create then and execute the email. Once the email is sent, the user sees no difference at a quick glance and logs in; the login information is then routed to the attacker to use at his own will [4]. Similarly, smishing, detected in the earlier parts of the 2000s, is when attackers send messages to the users via SMS or text message and trick the users into clicking on links that can either download malware onto their devices or collect personal data via the user entering the data into what they believe are legitimate websites.

Many companies have now implemented technology that can detect these phishing emails before they are released to the employees and have stressed the usage of multi-layered defense systems that, as the name suggests, add an extra step of security before authentication. As the research grows, companies are also extending their training to employees to teach them to spot out capricious information in the email to be aware of future attacks [5]. Common services used to detect threats are FireEye and CrowdStrike which help organizations anticipate future threats as well as understand the threat in different forms. Other tools like Webroot and Scaler block access to commonly known websites that are categorized as malicious and prevent the user from clicking on the links. Some IT departments even use programs like PhisMe and IRONSCALE to allow the employees to self-report once trained or a suspicion is raised. Organizations are also taking an extra step and utilizing antivirus and anti-malware software such as McAfee, Symantec, and Bitdefender, which can detect and possibly protect a device from unknowingly downloaded malware.

Moving forward, many companies are doing extensive research to attempt to stay ahead of phishing in all forms. Many researchers are integrating AI and machine learning to explore gaining leverage on future attacks by gathering and analyzing trends to predict user behavior. Tools that utilize AI and machine learning can analyze a large amount of data faster than a human can. However, the accuracy is still taken into account due to user error as well as AI not being able to detect new forms that have not been previously detected.

III. VISHING

One of the most prevalent issues regarding unauthorized access to confidential information is voice phishing, also known as vishing. Vishing is a category of phishing attacks that relies on an attacker utilizing voice messaging systems or phone calls. Much like conventional email phishing, vishing aims to deceive a target into forfeiting their credentials or sensitive information. The setup for a phishing attack is similar to other social engineering-based attacks. The attacker creates and presents a scenario to put the target into a vulnerable state to coerce them into disclosing sensitive information. Voice phishing opens avenues that are ordinarily not accessible through other means. One of the most prominent examples of this is the ability to disguise your voice to sound like someone familiar to the target. Social engineering thrives on the principle of sounding as convincible as possible. Elderly, children, and users unfamiliar with security controls are the most susceptible to these kinds of attacks. While this type of scam seems simple at face value, it has constantly evolved with the rest of technology to become more convincing and pose an even more significant threat.

One of the most common vishing scenarios we have encountered has been a call to our cell phone from an attacker claiming an issue with our car’s extended warranty. This is an example of wardialing, where a massive number of automated phone calls are made to the respective number of targets. These calls are less elaborate but do the job of sending someone a message attempting to put them in an urgent scenario. Another common vector of vishing comes from malware on the target’s computer. An executed malware may run a program that will block other programs on a user’s computer. It may also display a message indicating that the computer’s operating system has been compromised and provide a phone number to contact for troubleshooting. This almost certainly leads to an attacker impersonating the operating system’s IT support. The visher, in this case, will likely use a combination of automated replies and their own voice to minimize the work they have to do to get the target credentials. According to Josh Fruhlinger, who created a foundational article explaining vishing and common

situations created using it, vishing attacks may also be designed to target a particular person. This technique is known as spear vishing, similarly named to the method for email-based phishing. This type of attack requires the threat actor to have prior knowledge of the target. This information can involve details such as full name, date of birth, phone number, and home address. This can be likely found on the dark web after the events of a data breach. This highlights the importance of safeguarding the data user's provide online, especially sites that request personal information.

With all of this information in mind, it should be easy for an experienced individual to avoid falling for these scams. However, vishing has evolved since its first documented instance in the early 1990s. Vishing has become more formidable as time has gone on, and the rise of artificial intelligence has contributed greatly to it. As said before, common phishing scenarios involve an automated voice to minimize the work an attacker needs to put in. One such case where this was successfully used was when Sofia Niño de Rivera fell victim to a vishing attack in September 2024. She was approached by attackers on the phone impersonating bank employees, telling her that she was a victim of fraud. By the end of the conversation, her savings and her checking accounts were emptied of their funds. The attackers were so thorough in their plan that they instructed Sofia to accept the multi-factor authentication. Through her personal judgment, she deemed they were legitimate employees guiding her through a fraud case. The scam involved disabling the bank application facial recognition MFA, removing the need for "something you are" for authentication. Sofia shared her experience through a video on TikTok and garnered a considerable impression on her audience. From her experience, we are able to learn a lot about the formidable threat of vishing.

Vishing can also be used elaborately to disguise the threat actor as someone the target is familiar with. Through different methods, an attacker is able to spoof someone's phone number. This means that they can artificially imitate their number. When a phone call is made to someone in a modern phone's contact list, it checks the incoming phone number and cross-references it with the list of numbers in the user's contacts. If there is a match, the caller ID will show up as the user entered it when creating the contact. As such, if a friend in your contact list has their number spoofed, a fraudulent call disguised as that number will show up as your friend. This will allow for the pretext that a familiar person is calling the target. By extension, the target will lower their guard. Due to the rise of generative artificial intelligence, an accurate voice clone of any given person may be created after listening to a short sample of their voice. With these two techniques, an attack may be conducted, making it seem like a familiar individual is contacting you and will even sound like them.

Phishing and vishing are becoming more formidable as technology advances. We must utilize strong authentication methods to ensure the safety of users around the globe.

IV. MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is a security method that requires users to provide more than one form of authentication to access an account, such as a password and a code sent to a phone, making it tougher for unauthorized users to gain access to sensitive information. It's a critical tool in the arsenal of identity and access management, ensuring that a simple username and password aren't the only gates guarding our digital accounts. MFA is also known as two-step verification. It's an additional layer of security that can help prevent unauthorized access to accounts, even if a password has been compromised. For example, if a user is attempting to log in from an unfamiliar location or device, the system may require additional authentication steps to verify the user's identity. MFA increases security by requiring users to provide a combination of two or more authentication factors, such as:

- A password or time-based, one-time password
- A code sent to their email or SMS verification code
- A personal identification number (PIN)
- A cryptographic identification device
- A token or hardware key
- A biometric factor like fingerprint, voice, or facial recognition
- An answer to a personal security question
- A push notification

When we log in our digital accounts, MFA might ask for something more from the mentioned factors, a code from an app, an answer to a personal question, a push notification from third-party apps, or even a quick biometric check like a fingerprint or facial scan. By adding these extra verification steps, MFA goes a long way in preventing unwanted access, safeguarding against data breaches, account takeovers, and a host of other malicious actors. What's more, location can also be used as an additional factor to increase the security of online transactions. For example, the location of the user and the location of the fraudster will differ during online transaction fraud.

Figure 4-1: Multi-Factor Authentication (MFA) Procedure

Multi-factor Authentication (MFA) has many benefits, including:

- Enhanced security- MFA adds an extra layer of security by requiring multiple forms of verification, making it much harder for unauthorized users to breach accounts.
- Reduced phishing attacks- even if an attacker obtains a user's login credentials, they won't be able to access the account without the additional form of authentication.
- Compliance- MFA is an important step in making sure to have strong data protection mechanisms in place, as per legal requirements.
- Protects against password fatigue- MFA ensures that cybercriminals cannot steal simple or repeated passwords.
- Easy to adopt and use- MFA is simple to use while still providing excellent protection against attacks.
- User confidence- Users feel more secure knowing their accounts are protected by multiple layers of security.

In addition, the tendency to use Multi-Factor Authentication (MFA) has been increasing significantly in recent years, driven by the growing recognition of cybersecurity threats, remote work, cloud adoption, social engineering awareness and the need for stronger protection measures. As mentioned above, phishing and smishing are both types of cyberattacks aimed at tricking individuals into revealing sensitive information, while MFA is designed to go against these malicious attacks especially during the pandemic on 2020. In a 2024 JumpCloud survey of over 1000 SME IT professionals, 83% of respondents said that they required employees to use MFA to access all their resources. A similar survey found that:

- 95% of employees using MFA do so via a software program, such as "Duo Mobile".
- The likelihood of MFA usage increases with organization size. In companies with over 10,000 employees, 87% use MFA.
- The likelihood of MFA usage is 78% for business with 1,001 to 10,000 employees.

Another report from "Multi-Factor Authentication Market" depicts that, due to increasing cyber-attacks and security issues, more and more companies and businesses are shifting towards MFA systems to overcome cyberattacks and secure their private data. The tendency can be described as the following graph:

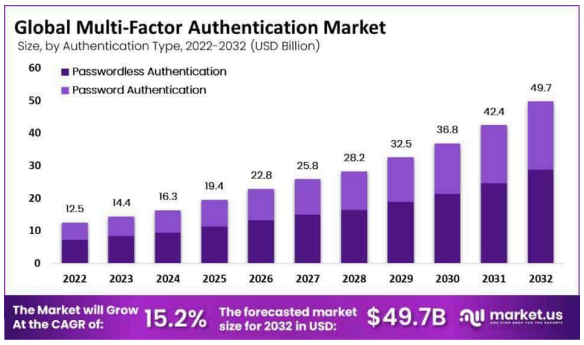

Figure 4-2: MFA Market Tendency

The trend towards MFA adoption is expected to continue as the cybersecurity landscape evolves. Organizations that proactively implement MFA not only enhance their security posture but also foster trust with their users. As threats become more sophisticated, MFA will likely become a standard practice rather than an optional security measure. This can be considered more effectively to be integrated and streamlined to build a more holistic approach to prevent malicious actors from attacking.

V. IMPLEMENTATION

Multi Factor authentication (MFA) has become a popular first line of defense to address and protect organizations from the enormous threat of phishing in the cybersecurity world. MFA certainly brings a layer of protection to phishing threats but also comes with some of its own obstacles. It first requires an organization to follow through with educating employees, addressing human factors, acclimating to the changes in cyber threats, and being compliant with the policies and procedures implemented.

A major problem in implementing MFA is the degree of technical difficulty. Using MFA in older or more vintage systems can be hard, because these systems most of the time are incompatible with new MFA formalities and practices. The problems with systems being incompatible yields wasted time, unnecessary expenses, and straining the infrastructure. Being proactive in fixing technical hurdles is key in making sure the systems remain protected throughout the process of implementing MFA [15] [17]. Not addressing these concerns leads to loop holes in the protections system and processes

that allow attackers the chance to manipulate vulnerabilities.

Another important role that makes it difficult to implement MFA implementation is the human factor. Employees in a workplace find it to be a bit bothersome to take the extra time to download extra applications and receive codes to assist them in completing the “Sign on” process. Most of the time, MFA requires a user to set up an external device or account to verify their identity, and this step is completely ignored. This is why user/employee education is important. It is common for companies and organizations, in conjunction with human resources and information technology departments, to organize training and brief online classes that employees are required to attend and complete to be compliant with retention requirements. The implementation and requirements of this training help against phishing [16] [17].

Phishing attacks are growing in abundance and innovation, prompting the MFA structure to stay up to date with the most recent threats. Cyber-attack culprits are coming up with new ways to jump directly over MFA by deploying man-in-the-middle (MITM) attacks and SIM swapping. Less sophisticated forms of MFA are more susceptible to attacks. An example of this is text-message authentication, which can be targeted. Once the attacker has intercepted a text message, the content of the message is compromised. This has forced organizations to switch to a stronger form of MFA, known as Fast ID Online (FIDO) authentication, which uses cryptography protection procedures, making it much more difficult for attackers to accomplish their mission [14] [15].

Following best practices is crucial for successful implementation. Businesses should not exclusively rely on text message-based authentication. Instead, they should integrate various forms of MFA, such as biometric verification and hardware tokens, to provide better protection against phishing attacks. Additionally, MFA should be implemented for every user in the workplace instead of just focusing on areas that are prone to attacks because attackers can use any compromised account for additional access [15] [17]. Email filtering, encryption, and thorough monitoring are all layers of protection in addition to MFA that protect a system on a holistic level.

Additionally, it is essential to routinely reassess security standard operating procedures as phishing continues to change and tactics get stronger. Companies should periodically update MFA systems and educate users about the latest innovations attackers use for phishing so they can continue to be effective. It could be hard for a business or a company to run and complete its business goals without secure cyber infrastructure [16]. A company can be non-tech related and still be a target of attack, like a hospital or social service agency whose sole purpose is to save people's lives. The employees of these kinds of companies will only be able to do their jobs if their systems are protected.

In conclusion, phishing remains a significant threat, but MFA offers protection against these attacks. However, implementing MFA comes with challenges. Organizations need to consider technical issues, human factors, and the constant change tactics that attackers use. When addressing these obstacles and implementing the best practices, companies will lower the risk of attacks and have a robust cybersecurity infrastructure. Today, the battle against phishing is a hard-fought one that is sometimes won and lost, but proactive measures like implementing MFA can be a vital practice for protecting sensitive information.

References

[1] Wash, R., Rader, E., Berman, R., & Wellmer, Z. (1970, January 1). *Understanding password choices: How frequently entered passwords are re-used across websites*. USENIX. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash

[2] Gupta, B.B., Tewari, A., Jain, A.K. et al. Fighting against phishing attacks: state of the art and future challenges. Neural Comput & Applic 28, 3629–3654 (2017). https://doi.org/10.1007/s00521-016-2275-y

[3] M. Khonji, Y. Iraqi and A. Jones, "Phishing Detection: A Literature Survey," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013, doi: 10.1109/SURV.2013.032213.00009.

[4] Kadlak, Aditya & Sharma, Shabnam. (2018). Study on Phishing Attacks. International Journal of Computer Applications. 182. 27-29. 10.5120/ijca2018918286.

[5] Eka Putra, Fauzan & Ubaidi, Ubaidi & Zulfikri, Achmad & Arifin, Goffal & Ilhamsyah, Revi. (2024). Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study. Brilliance: Research of Artificial Intelligence. 4. 413-421. 10.47709/brilliance.v4i1.4357.

[6] Hatice Ozsahan, David Worthington. “2024 Multi-Factor Authentication (MFA) Statistics & Trends to Know.” *JumpCloud*, 15 Aug. 2024, jumpcloud.com/blog/multi-factor-authentication-statistics.

[7] Kinzer, Kelsey. “What Are the Different Factors of Multi-Factor Authentication (MFA)?” *JumpCloud*, 14 June 2023, jumpcloud.com/blog/different-factors-of-multi-factor-authentication-mfa.

[8] Figure 4-1 MFA Procedure https://umanitoba.ca/information-services-technology/information-security-compliance/um-multi-factor-authentication

[9] Figure 4-2: MFA Market Tendency https://market.us/report/multi-factor-authentication-market/

[10] Figueiredo, João, et al. "On the Feasibility of Fully AI-Automated Vishing Attacks." *arXiv.Org*, 20 Sept. 2024, arxiv.org/abs/2409.13793.

[11] "Device, System, and Method of Detecting Vishing Attacks." Targeted News Service (TNS), 25 Sept. 2024. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=edsgin&AN=edsgcl.810002891&site=eds-live.

[12] "The Bank Calls You for an 'Emergency' and You Lose All Your Money? Vishing' Is the New Phone Scam That Sofía Niño de Rivera Was Subjected to." ContentEngine Noticias Financieras (English), 20 Sept. 2024. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=edsgii&AN=edsgcl.809603981&site=eds-live.

[13] "Sofía Niño de Rivera Denounces the Theft of All Her Savings by Vishing: 'Anyone Can Fall into Fraud.'" ContentEngine Noticias Financieras (English), 21 Sept. 2024. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=edsgin&AN=edsgcl.809624235&site=eds-live.

[14] Cybersecurity & Infrastructure Security Agency (CISA), "Multi-Factor Authentication (MFA)," CISA, 05-Jan-2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[15] D. Robb, "How to Prevent Phishing Attacks with Multi-Factor Authentication," TechRepublic, 23-Sep-2023. https://www.techrepublic.com/article/how-to-prevent-phishing-attacks-with-mfa/.

[16] JumpCloud, "Human Challenges of Multi-Factor Authentication (MFA)," JumpCloud, 19-Oct-2023. https://jumpcloud.com/blog/human-challenges-mfa/.

[17] MojoAuth, "9 Best Practices for Multi-Factor Authentication (MFA)," MojoAuth. https://mojoauth.com/blog/9-best-practices-for-mfa/.