Framework´s Study for Cybersecurity Education Applied for Phishing

Fernando Padilha Farah [1]; Everson Denis [2];

[1] Scholarship Student of the GCSP – IMT (EEM/CEUN-IMT);
[2] Mentor of the GCSP-IMT (EEM/CEUN-IMT).

Abstract. This paper concerns cybersecurity in the world and the main types of cybersecurity threats, with a focus on Social Engineering and Phishing. The purpose is to carry out the analysis of two frameworks that list guidelines for simplifying security policies so that organizations fully understand their specific risks and can develop curative and preventive measures accordingly. Phishing analyses are proposed with the ATT&CK Matrix for Enterprise framework considering tactics, techniques, sub-techniques, and subsequently, mitigation proposals. Proposals for future work applying cybersecurity frameworks are presented, focusing on business viability.

Keywords. *CyberSecurity, Mittre Att&ck, Mitre Engage, Nist, Social Engineering, Phishing.*

Introduction

Information security is directly related to the protection of a set of information, in the sense of preserving the value they have for an individual or an organization. The basic properties of information security are confidentiality, integrity, availability, authenticity and non-repudiation. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative (Netacad 2022).

Failure of cybersecurity measures: business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability (Wef 2021). Global Risks Horizon (Figure 1) revealed that cybersecurity flaws were indicated as the fourth biggest risk for the short term and that private and government actors are likely to engage in more dangerous and sophisticated cyberattacks soon. Therefore, it is essential that organizations look to the future in a pragmatic way, understanding the importance of having secure processes that follow the evolution of the technologies used.

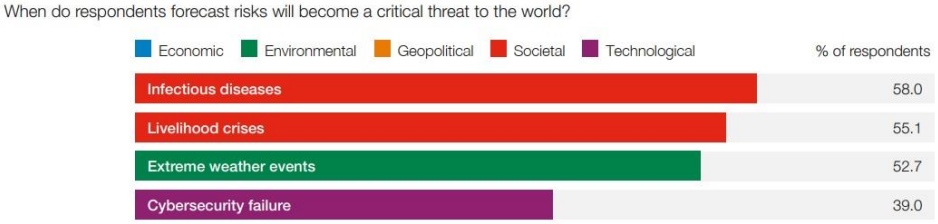

Figure 1: Global Risks Horizon (Wef 2021).

In today's connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning. Main types of cybersecurity threats (Netacad 2022):

- Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber attack. You can help protect yourself through education or a technology solution that filters malicious emails.
- Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.
- Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.
- Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

The area within CyberSecurity that most needs direct interaction from people, which is, therefore, more fragile to cyber awareness, is Social Engineering as "any act that influences a person to take an action that may or may not be in his or her best interests" (Christopher H 2018). There are many types of Social Engineering attacks (Mitnick K & Simon W 2005) characterized as a set of characteristics that seem common when attackers are faced with an unexpected situation, such as in assertiveness techniques (making sure something needs to happen or some information needs to be passed), urgency (usually rushing people helps them to act without thinking), compassion (showing targets that there is a great need for something to happen, if not something bad can happen to them, for example, "if something isn't done, my boss might fire me"), data collection (the more information is known about the target, the easier it is to convince him) and improvisation (in real situations nothing goes as planned, so you have to be quick to adapt to new problems and obstacles.) Always appealing to the human side and impact of people.

Apwg (2021) mentions that "preying unsuspecting victims, tricking them into believing they are dealing with a trusted and legitimate party using deceptive email addresses and email messages", as well as highlighted that in In the first half of 2022 (Figure 2), there were more than 2.1 million phishing attacks, thus reaching a new record.

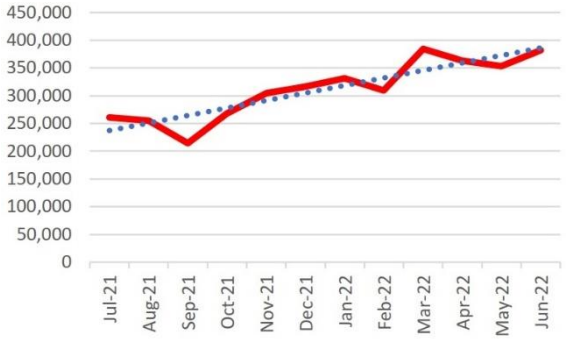

Figure 2: Phishing Attacks, 3Q2021 – 2Q2022 (Apwg 2021).

Organizations today need to establish a secure network that is both proactive and reactive to cyberattacks. Reactive security focuses on reducing the gravity of an attack and containing the damage. A proactive strategy hardens the security of the organization so risks from an attack are minimized. Although most organizations have some proactive and reactive strategies in place, they might have implemented these without fully understanding their own unique exposure to risks. Implementing cybersecurity frameworks can help. They can list guidelines for streamlining security policies so organizations fully understand their specific risks and can develop curative and preventive measures accordingly. There are two popular cybersecurity models that are used by organizations across industries: the National Institute of Standards and Technology (Nist 2022) and MITRE Adversarial Tactics, Techniques, and Common Knowledge (Mitre Att&ck 2022) frameworks.

The Nist Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. The NIST framework can be divided into three components:

1. The framework core: This instructs how to implement uniform defense techniques and comply with industry standards. The five steps of the organization's cybersecurity risk are: Identify, Protect, Detect, Respond, Recover (Figure 3).

Figure 3: The Cybersecurity Framework - Version 1.1 (Nist 2022)

2. Framework implementation tiers: This NIST component helps organizations assess their security maturity level, referred to as implementation tiers, based on the following factors: Risk management process, Integrated risk management, External participation.

3. Framework profile: This component helps organizations define and align their security outcomes, like revisions of the security policy and improvements to the security design, with the associated risks (identified at the "core" stage), and the security maturity level they're currently at (identified in the "implementation tier" stage). Organizations can set this as a "current profile" and then create "target profiles" to determine the maturity levels they aspire to be at. This approach to understanding the current security posture helps organizations address the different risks the organization faces and invest in appropriate security solutions. Since its introduction, NIST has been widely implemented as a security standard to enhance security postures. (Figure 4).

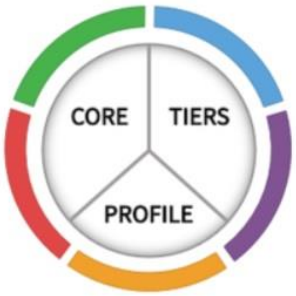

Figure 4: Voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk. (Nist 2022), (Intel 2014).

The MITRE ATT&CK framework (Mitre Att&ck 2022) was developed in 2013 to provide organizations with a blueprint for any possible type of cyberattack. It is one of the most multi-dimensional frameworks available for understanding cyberattacks. The ATT&CK framework's foundation is built on publicly accessible research on cyberattack techniques, threat intelligence on attacks, and reports of security incidents. It also lists ways organizations can mitigate these attacks. The MITRE ATT&CK framework is structurally a matrix that explores tactics, the "why" of a cyberattack, and techniques, the "how" of a cyberattack. ATT&CK analyzes the tactics, the malicious goals that attacker wants to accomplish, and the techniques, the processes used to achieve those goals. ATT&CK features 14 tactics that cover possible attack goals, and the multiple techniques attackers might employ to achieve each tactic (Figure 5).

Figure 5: ATT&CK Matrix for Enterprise V12.1. (Mitre Att&ck 2022).

While they share the goal of empowering organizations to defend themselves, the approach they take is different. NIST (Nist 2022) helps companies achieve required security outcomes by outlining best practices blended with compliance laws. ATT&CK (Mitre Att&ck 2022) helps companies understand their adversaries better, test their network for vulnerabilities, and set up counter measures.

Objectives

The technical nature of ATT&CK serves as a good reference for determining signals or activity logs, analyzing, detecting and mitigating threats. For the phishing technique, the ATT&CK framework will be very useful for a more targeted and detailed analysis of this application. There is a Phishing analysis proposal with the ATT&CK Matrix for Enterprise framework (Mitre Att&ck 2022) considering tactics, techniques, sub-techniques and, in the sequence, mitigation proposals.

Development

Under Initial Access, there are 9 techniques. Some of the techniques have sub-techniques, such as Phishing (Figure 6).

Figure 6: ATT&CK Matrix for Enterprise - Phishing: Sub-techniques. (Mitre Att&ck 2022).

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source. The 3 sub-techniques of Phishing are Spearphishing Attachment, Spearphishing Link and Spearphishing via Service.

In the case of Spearphishing Link, Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email

attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

Procedure Example (Spearphishing Link - Wizard Spider): is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals (Dhs/Cisa 2020), (Hanel A 2019), (Podlosky A & Hanel A 2020). A technique used was “Account Discovery: Domain Account”: Wizard Spider has identified domain admins through the use of "net group ‘Domain admins’" commands (The Dfir Report 2020).

Results and Discussion

Based on the technique "Phishing: Spearphishing Link" and "Wizard Spider" phishing emails were sent containing a link to an actor-controlled Google Drive document or other free online file hosting services (Dhs/Cisa 2020, Podlosky A & Hanel A 2020), as shown in figure 7.

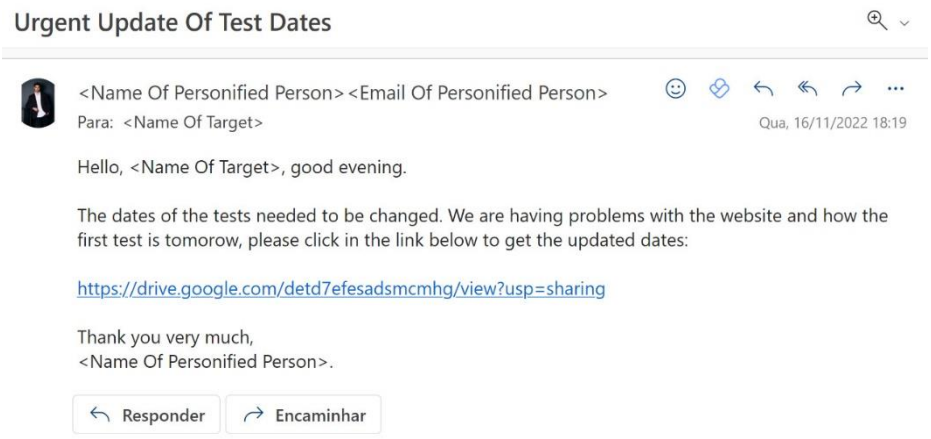

Figure 7: Phishing: Spearphishing Link. (Mitre Att&ck 2022).

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging User Execution. The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack"). (Cisa 2019). Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to Steal Application Access Tokens (Hacquebord F 2017). These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls (Microsoft 2021).

As shown in figure 7, when the link accessed by the visitor, there is a redirection to the fake google page. SetToolKit (The Social-Engineer Toolkit - SET) which is an open source Python based tool aimed at penetration testing around Social Engineering (Set 2022). The Social Engineering Toolkit allows phishing attacks to be performed against the victim. By using SET, one can create phishing pages of many websites such as Instagram, Facebook, Google, etc. SET can use a URL or IP for the victim, once the victim opens this URL, he/she will see a legitimate web page of a real website, which is actually a phishing page. As soon as he/she enters his/her identification password, the hacker gets the identification password on the terminal screen. This is how the phishing attack using SET works (Figure 8).

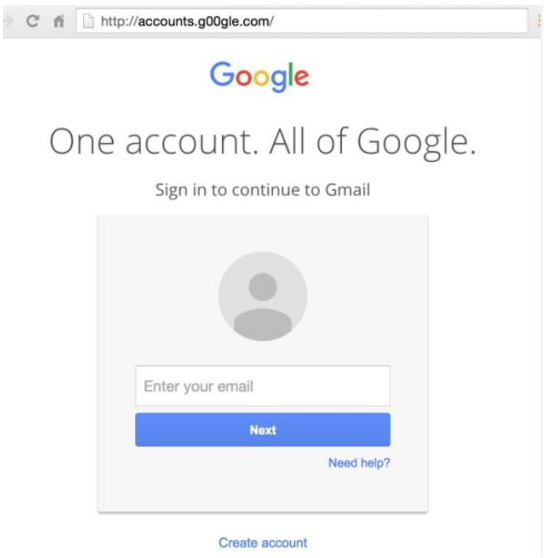

Figure 8: Social engineering toolkit by creating google phishing page with changed URL. (Kali 2022, Set 2022).

To mitigate the risks related to the phishing techniques employed, as well as other similar techniques, here are some strategies to minimize possible threats (Table 1).

Table 1 - Techniques Addressed by Mitigation (Mitre Att&ck 2022):

Mitigation	Description
Audit	Audit applications and their permissions to ensure access to data and resources are limited based upon necessity and principle of least privilege.
Restrict Web-Based Content	Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain and integrity of messages. Enabling these mechanisms within an organization may enable recipients to perform similar message filtering and validation.
User Account Management	Azure AD Administrators apply limitations upon the ability for users to grant consent to unfamiliar or unverified third-party applications.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails with malicious links which includes phishing for consent. Additionally, users may perform visual checks of the domains they visit. Phishing training and other cybersecurity training may raise awareness to check URLs before visiting the sites.

Conclusion

In this article, two frameworks applied to cybersecurity were analysed. For the phishing technique, the ATT&CK framework proved to be very useful for a more targeted and detailed analysis of this application. Some examples of Phishing analysis were carried out, as well as an application based on the ATT&CK Matrix for Enterprise framework (Miter Att&ck 2022) considering tactics, techniques, subtechniques and mitigation proposals.

Following the project, real tests are expected in a company applying cybersecurity frameworks (Nist 2022), (Mitre Att&ck 2022), (Mitre Engage 2022), with a focus on business viability.

References

Apwg 2021. The Anti-Phishing Working Group, Phishing Activity Trends Report, viewed 06 November 2022, https://apwg.org/trendsreports

Christopher H 2018, Social Engineering: The Science of Human Hacking, p. 7. John Wiley & Sons, Indiana.

Cisa 2019, Security Tip (ST05-016): Understanding Internationalized Domain Names, https://www.cisa.gov/uscert/ncas/tips/ST05-016

Dhs/Cisa 2020, Ransomware Activity Targeting the Healthcare and Public Health Sector, viewed 06 November 2022, https://www.cisa.gov/uscert/ncas/alerts/aa20-302a

Hanel A 2019, Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware, viewed 06 November 2022, https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Hacquebord F 2017, Pawn Storm Abuses Open Authentication in Advanced Social Engineering Attacks, https://www.trendmicro.com/en_us/research/17/d/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks.html

Intel 2014, The Cybersecurity Framework in Action: An Intel Use Case, viewed 06 November 2022, https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf

Kali 2022, The Most Advanced Penetration Testing Distribution, viewed 10 December 2022, https://www.kali.org/

Microsoft 2021, Microsoft delivers comprehensive solution to battle rise in consent phishing emails, https://www.microsoft.com/en-us/security/blog/2021/07/14/microsoft-delivers-comprehensive-solution-to-battle-rise-in-consent-phishing-emails/

Mitnick K & Simon W 2005, The Art of Intrusion. PEARSON: Prentice Hall, São Paulo.

Mitre Att&ck 2022, It´s a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, viewed 06 November 2022, https://attack.mitre.org

Mitre Engage 2022, Framework for planning and discussing adversary engagement operations, viewed 06 November 2022, https://engage.mitre.org/

Netacad 2022, Cisco Networking Academy - Understanding Defense, viewed 06 November 2022, https://www.netacad.com/pt-br/courses/cybersecurity/cyberops-associate

Nist 2022, NIST Cybersecurity Framework, viewed 06 November 2022, https://www.nist.gov/cyberframework

Podlosky A & Hanel A 2020, WIZARD SPIDER Update: Resilient, Reactive and Resolute, viewed 12 December 2022, https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

Set 2022, The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around Social-Engineering, viewed 12 December 2022, https://www.kali.org/tools/set/

The Dfir Report 2020, Ryuk’s Return, viewed 12 December 2022, https://thedfirreport.com/2020/10/08/ryuks-return/

Wef 2021, World Economic Forum, The Global Risks Report, viewed 06 November 2022, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf