Social Engineering Attacks: Risks, vulnerabilities and Countermeasures

Nelson Cacheira[1]

[1] ULP – Lusófona University, Porto - Portugal

nelson_cacheira@hotmail.com

Abstract. Never before was the Internet the ground for communications and social interactions. The world is now a digital expansion of our lives, and the way we think and communicate. As digital interactions take ever more space in our personal life, the information given by the users to these platforms are in great jeopardy due to the inherent vulnerability of attacks. It is not uncommon to hear about attacks happening in companies, but it is something that is not taken into account by the common user, because it doesn't affect them. But if cybersecurity isn't taken into consideration, the next attack could be directed at us. Social Engineering should not be avoided or downplayed, and the discussion must be brought to the public eye, and discuss the risks, vulnerabilities, attacks and countermeasures. Attackers can easily take advantage of these vulnerabilities and exploit them for personal gains. Norms have been taking place such as cookie and privacy policies so the websites and corporations are clearer in their practice. The public must be aware of the risk they're facing, and put into practice ways to be safe online. This paper will explain the risks, vulnerabilities and ways to prevent these attacks.

Keywords: Social-Engineering, Cyber-Security, Internet Safety, Awareness, Countermeasures.

1 Introduction

Cyber security has become a new concern in the 2000s. Companies and private individuals are concerned with the leaking of information. The communications channels have widened, even at the workplace, being more popular the BYOD (bring your own device), in which these mobile devices carry around corporate information and have no way to be totally in the control of the companies [1]. Social media is too a great concern, being generally used by all ages and cultures. A study on "User characteristics that influence judgment of social engineering attacks in social networks" show for example, that perceived risk and perceived severity of threats vary between genders, being the women more aware than men [2]. Social engineering isn't only an online

problem. Even before the advent of the Internet, there were social engineering attacks going on. Now it just took to another level. The focus of this study will be on defining Social-Engineering, it's Categories, the hacker's motivations for attacks, the attack phases, types and vectors, to highlight the prevention and some methods anyone can apply to mitigate the problem. The objective is to bring awareness to the problem, and give some insight into what is Social-Engineering.

2 Social-Engineering

"Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion" [3]. The Human factor is maybe the greatest threat to cybersecurity. If a software has programming errors, it is attributed to the Human not programming it correctly, and if there is a breach in security, it is because humans didn't take it into account when designing its defenses. Most of the issues come from people downplaying the importance of knowledge and awareness, trusting the website or application their using, and believing they're good at detecting such attacks [3]. In this chapter will be explained the categories, motivations, phases and types of social-engineering attacks.

2.1 Categories

Hunting. "This approach seeks to execute the social engineering attack through minimal interaction with the target. Once the specified objective is achieved and the security breach is established, communication is likely to be terminated. This is the most frequently used methodology to support cyber-attacks and as a rule, the modus operandi involves a single encounter" [4].

Farming. "Social engineering farming is not often practiced, nevertheless this technique may be used for situational purposes. The attacker aims to establish a relationship with the victim in order to extract information for a longer period of time. Throughout the process, the interaction can change, the target may learn the truth and the social engineer may attempt to bribe or blackmail the target, thus resorting to traditional criminal behavior" [4].

2.2 Hacker's motivation

For any crime, there is a motive worthy of pursuing. Being it the thrill of the moment, or financial games, there are various motives for attacks to take into consideration [5].

Self-Education. Can be only for the thrill of gaining knowledge and beating the system [5].

Financial Gain. Maybe the most thought of motive, blackmail and organized crime [5].

Revenge. Some ex-employees can exploit their known weaknesses of the system to get back at the corporate entity or an individual in the organization [5].

External Pressure. The social engineer can manipulate someone to break security protocols, by blackmailing, ransoming, exploiting moral dilemmas or extremist beliefs. Since there are no victims, just ones and zeros, the victim can be persuaded to commit a crime they wouldn't have in normal conditions [5].

Terrorist and Political Motivated Groups. Attacker can act on religious beliefs or activist values to break havoc and attack a financial and critical information infrastructure [5].

2.3 Social-Engineering Attack Phases

"Any criminal act has a common pattern. Such a pattern is evident with social engineering, and it is both recognizable and preventable." [6] When planning an attack, the social engineer plans his actions ahead. While the target doesn't know, the attacker can have already planned out who the target is, and how to get the information. Attacks of this nature, typically consist of four distinct phases: research, hook, play and exit, as shown in **Fig. 1** [4].

Research. This involves gathering information on the target. A variety of techniques can be used to achieve this, and be used to create a relationship [5]. An experienced social engineer can exploit chance encounters too [4].

Hook. This is when the attacker builds a relationship with the target. This relationship will be exploited an explored to capitalize on the created trust. Sometimes masquerading as a senior member of the organization or as a friend [5].

Play. Here is where the attack takes place, using the information gathered, the attacker performs the attack per se, to disclose or compromise the system [4][5].

Exit. The social engineer has completed his task, preferably without arising suspicion, because these attacks aren't easy to track down [4].

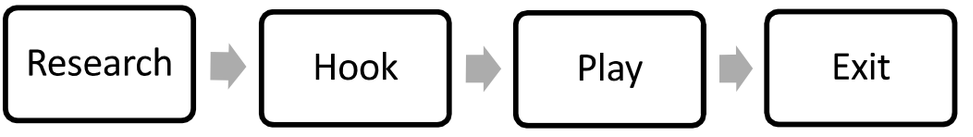

Fig. 1. Social Engineering Phases (4).

2.4 Types of Social-Engineering Attacks

Social Engineering attacks can come from two Operators. One being the Human, and the other Software [3]. Since the dawn of humanity, social engineering tricks have been occurring, especially with street performers and con-artists, but in the digital era, these tricks have taken another form, sometimes more indirect, through channels like e-mail, instant messaging, telephone, social networks, cloud services and websites [3]. **Fig. 2** shows the various ramifications of this, branching from Type, Operator and Channel.

2.4.1 Physical

These are physical interactions, such as eavesdropping, over-the-shoulder and dumpster diving. Can sometimes be the most practical and available method since no IT knowledge is needed to intercept conversations, check on passwords or steal an authentication card [3].

2.4.2 Social. This is the basis for all Social Engineering attacks. From even before the digital era, con-artists would use tricks to persuade into his biddings. These persuasion techniques are used to manipulate and address the curiosity of the victim, even to the point of developing and maintaining a relationship with their future victims, being the most prevalent attacks performed by phone [7]. Can lead to attacks such as baiting and spear-phishing attacks [3].

2.4.3 Socio-Technical. This is an approach that relies on technical knowledge for social engineering attacks. The best example would be the attacks via e-mail or instant messaging. These classic attacks like phishing are not lucrative, being aimed at a large number of people indiscriminately [8]. That is why these Socio-Technical attacks evolved to Spear-Phishing or Wailing, that target specific individuals [3].

2.4.4 Technical. Tools are used to gather and harvest information on future victims through malware or search engines to gather personal information about future victims [3].

2.4.5 Reverse Social-Engineering. There's still this often-overlooked type of attack. In this reverse take on social engineering, the attacker makes the victim think they're a trustworthy entity instead of making the first contact. That could be done by advertising and then assisting previously sabotaged victims [9]. Doors can be opened, and passwords can be given to the attacker directly from the victim, with the objective to help her [3].

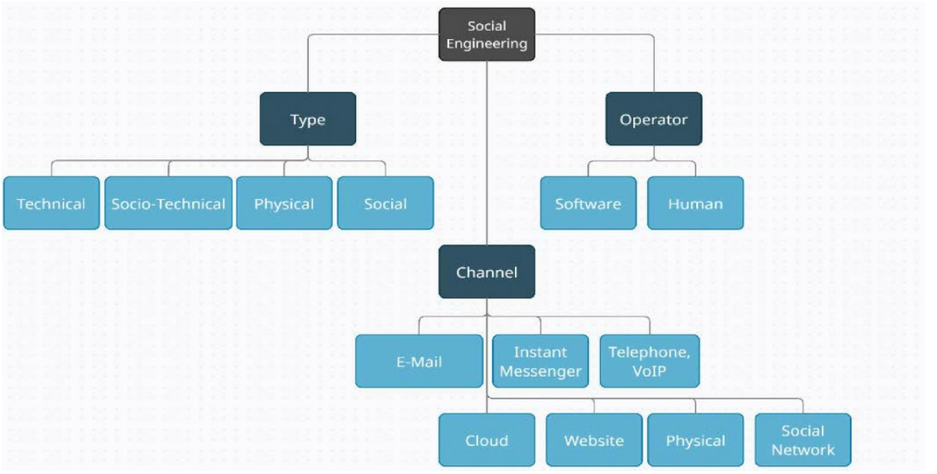

Fig. 2. Social Engineering Taxonomy [3].

3 Attack Vectors

Attacks can take on many forms. From waiting for any unaware victim as a trap, disguised as another person or website, or from directed spear-headed attacks on multi-millionaire corporations for financial or political gains, the creativity and genius of these attacks are ever evolving, always finding new ways to swindle the victims or breaching into high-security websites, as shown in **Fig. 3**. It does come to show the attackers will always be one step ahead.

3.1 Phishing

The act of illegally accessing to the information of the target, often masquerading as a trustworthy entity. Usually targets a large group of victims indiscriminately through various mediums [3].

3.2 Spear-Phishing

Is a targeted Phishing attack, used to hit specific individuals or companies after gathering the victim's information. Usually is meant to hit high-profile victims, with the intent to access the victim's system, to gather for example, company/military/personal secrets. It is highly effective, due to the preparation and focus involved [10].

3.3 Spy-Phishing

Is the act of spying on a victim through unauthorized installed software. The attacker installs a malicious software called spyware, by exploiting website fragilities, trojans,

or via Freeware and Shareware. waits the victim to access a predetermined website to steal log in information [10].

3.4 Dumpster-Diving

Is the act of going through the victim's trash. Has a man's trash can be another man's treasure, often the victims don't realize the problem imposed by their trash. The attacker can find login passwords, security footage, signatures, memos, personal contacts or e-mails [3].

3.5 Shoulder Surfing

The simplest method of gathering info, the eavesdropping. It is the easiest way to gather information, just looking at someone's phone or computer screen [3].

3.6 Advanced Persistent Threat

Refers to long-term, mostly Internet-based espionage attacks conducted by an attacker who has the capabilities and intent to comprise a system persistently [3].

3.7 Reverse Social Engineering

Trust is pre-established between the attacker and the victim. The attackers create a situation in which the victim requires help and then present themselves as someone the victim will consider someone who can both solve their problem and is allowed to receive privileged information. Of course, the attackers try to choose an individual who they believe has information that will help them [3].

3.8 Baiting

Is an attack during which a malware-infected storage medium is left in a location where it is likely to be found by the targeted victims [3].

3.9 Water Holing

Describes a targeted attack where the attackers compromise a website that is likely to be of interest to the chosen victim. The attackers then wait at the waterhole for their victim [3].

Table 1 – Classification of social engineering attacks according to our taxonomy.

		Phishing	Shoulder surfing	Dumpster diving	Reverse social engineering	Waterholing	Advanced persistent threat	Baiting
Channel	E-mail	✓			✓		✓	
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓	✓	✓

Fig. 3. Classification of social engineering attacks [3].

4 Social-engineering Attack Risks

These are some of the greatest examples on how social-engineering attacks have damaged corporations, and brought to the frontline the notions of cybersecurity and its necessity. Not only the corporations are impacted, but also the people affiliated with these companies can have their data stolen. These are some of the risks a breach in security can have [11].

4.1 Yahoo Customer Account Compromise (2013)

Through a semi-privileged worker, 3 billion accounts were compromised, going up for sale on the dark web, being probably the biggest security breach ever [11].

4.2 Sony Pictures Hack (2014)

Due to a movie release satirizing North Korea, allegedly, north Korean hackers aimed to hurt the movie publisher, released several other pictures and a considerable amount of employee data online, making Sony suffer substantial financial losses [11].

4.3 Department of Labor Watering Hole Attack (2013)

A server of the Department of Labor was hacked, through a remote access Trojan named Poison Ivy. The hackers were never found, and it is hard to know the victims unless those victims come forward, because watering holes are websites or resources that look official but are traps set up by the attackers [11].

4.4 Ubiquiti Networks Scam (2005)

Attacker impersonated employees from the companies Hong Kong subsidiary, regarding instructions to changes in payment account details or new vendors to be credited, which, unverified, led to the $47 million in damages, recovering only $8 million, being the rest lost to the hackers [11].

4.5 RSA SecurID Phishing Attack

Attackers sent email with a spoofed address to four employees, purporting to be at a job recruitment website, with an Excel attachment. The files were opened, and a zero-day Flash exploit installed a backdoor access which stole the company's SecurID's two-factor authentications [11].

5 Prevention

The methods, motives and channels of attack are endless, and the battle between attackers and defenders is ongoing. “Most people do not realize just how much information they reveal about themselves, or the organizations that they work for, in the course of their daily discussions” [5]. The importance for cybersecurity is still downplayed, being the costs and complexity high, it is hard to insist on its importance. Sometimes, only when someone or a corporation is attacked, that the awareness. There are a wide range of tools nowadays to prevent against social engineering attacks, but despite these software applications, the number one factor to consider, is the human factor. To be well protected, one must first acknowledge the problem, “know thy enemy” and then act on the issue [12]. “The defense must have several layers of protection so that even if a hacker were able to penetrate one level, there would be other levels at which he/she would be stopped”, and this can be accomplished, among other things, by having software, human, and policy resources on the task [13]. There are three ways to defend against social engineering attacks, according to Douglas Twitchell: Education, training and awareness; Policies; Enforcement through auditing.

5.1 Education, training and awareness

It is not enough just to enforce policies and audit, because if the individuals aren’t taught why they must follow them, it remains hard to enforce it [14]. All staff must understand the necessity of cybersecurity at home and at work, especially when BYOD, and most importantly, their responsibility. Any breach can compromise their personal info or corporate info. This training should begin starting at employment all the way until the end of the employment. This training will make the individual aware of the risks, so he will be reluctant to disclose personal or corporate information, and be on the lookout and alert in case of social engineering signs like rushing processes, name-dropping, intimidation, small mistakes and requesting forbidden information or accesses. Another method could be having a website dedicated to security [12].

5.2 Policies

“The security policy sets the standards and levels of security that can be applied to any network, system or environment” [5]. The anti-social-engineering documentation’s standards cannot be unattainable. Must have a brief and concise list of what they should do, and not what they shouldn’t do, so they aren’t turned off by the policies, and don’t waste too much time reading [12]. Policies must be too reviewed regularly and stay relevant with the times, as security is constant evolving battle between attackers and defenders.

5.3 Enforcement through auditing

An audit is conducted internally or by a specialized entity, with the purpose of making a risk assessment, identifying the people involved, the hardware and software, vulnerabilities, risks, and plan countermeasures accordingly. “Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening” [15]. Auditing will have considerable impact not only in cybersecurity and data protection against hackers, but in increased performance, identifying gaps in the defenses, highlighting and addressing weak spots, delivering an in-depth analysis of internal and external security practices, adding reputational value to the company and assuring employees, clients and vendors [16].

6 Countermeasures

6.1 Use secure and complex passwords

A good password is a password that uses a mix of numbers, capital and lower-case letters, symbols and with no repetitive patterns as these can be cracked easily by brute force [12].

6.2 Use Two factor authentication

Something you have, something you are, and something you know. This is a method where various means are applied simultaneously that only the user has, is and knows, like a card and a password, or a card and a retina scanner [12].

6.3 Remove info from public information databases

The more information someone has on the Internet, the riskier it is. There are ways to disclose private information through previously uploaded data through sites like Facebook or Instagram that depend on their cybersecurity, so the least information you have, the safer you’ll be [12].

6.4 Monitor your data

Look for identity theft and credit card dubious movements. You need to be vigilant to breaches [12].

6.5 Never reveal passwords

Due to dumpster diving and shoulder surfing, it is easy to know someone’s password, but easier it is if someone knows your password. Don’t tell your password to anyone nor dispose of written passwords without destroying them [12].

10.11228/dpsc.03.01.005

7 Conclusion

The information gathered in this article was collected to bring awareness to the cyber-security paradigm. Not only as a study on social-engineering, but on the ways to prevent it, taking into consideration the various attack vectors, motives, phases and types of attacks, and acknowledging the results these breaches had in some of the greatest corporations in the world in the past. From all the new technologies and advances in software and hardware, the most vulnerable component and the one that cannot be changed is the human being. In order to "upgrade" the human factor, one must only learn and be aware, as it is the first barrier between being at risk and being safe. Only then can countermeasures be put into practice to protect from attacks. There are multiple ways to be attacked, and the inevitability of attacks is certain. Only one breach is needed to break a system, but all fronts must be protected.

10.11228/dpsc.03.01.005

References

1. Miller, K., Voas, J., Hurlburt, G.: Byod: security and privacy considerations. IT Professional 14(5):53-55 (2012).
2. Albladi, S., Weir, S.: User characteristics that influence judgment of social engineering attacks in social networks. Albladi and Weir Hum. Cent. Comput. Inf. Sci. (2018) 8:5.
3. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. Journal of Information Security and Applications 22, 113-122 (2015).
4. Barbosa H., Breda F., Morais T.: Social Engineering and Cyber Security. International Technology, Education and Development Conference, DOI: 10.21125/inted.2017.1008 (2017).
5. Chantler, Alan and Broadhurst, Roderic: Social Engineering and Crime Prevention in Cyberspace. Technical Report, Justice. (2016).
6. Allen, M.: Social Engineering – A Means to Violate a Computer System. GSEC (2006).
7. Granger, S.: Social engineering fundamentals, Part I: hacker tactics. SecurityFocus. (2001).
8. Herley, C, Florencio, D.: Phishing as a tragedy of the commons. NSPW'08 (2008).
9. Nelson, R.: Methods of hacking: social engineering. http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html (2008).
10. Pais, R., Moreira, F., Varajão, J.: Engenharia Social (ou o carneiro que afinal era um lobo). Grupo Almedina: Pedro Campos e Pedro Quelhas de Brito (2013).
11. Cybersecurityeducationguides webpage, https://www.cybersecurityeducationguides.org/2017/11/top-5-social-engineering-attacks-of-all-time/ (2017).
12. Kumar, A., Chaudhary, M., Kumar, N.: Social Engineering Threats and Awareness: A Survey. Future Internet 11 (2019).
13. Gragg, D.: A multi-Level Defense Against Social Engineering. SANS Institute (2020).
14. Khonji, M., Youssef I., Andrew J.: Phishing Detection: A Literature Survey. IEEE Communications Surveys & Tutorials 15(4), 2091-2121 (2013).
15. Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J.: A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance. International Conference on Infor-mation Systems and Computer Science (2017).
16. Indusface webpage, https://www.indusface.com/blog/what-is-cyber-security-audit-and-how-it-is-helpful-for-your-business/ (2020/11/16).