Social Engineering: The art of attacks

Nelson Duarte[1[0000-0001-6650-0778]], Nuno Coelho[2[0000-0001-5517-9181]] and Teresa Guarda[3,4,5,1[0000-0002-9602-0692]]

[1] ISLA Santarém, Santarém, Portugal
[2] ISLA Gaia, Santarém, Portugal
[3] Universidad Estatal Peninsula de Santa Elena, Santa Elena, Ecuador
[4] CIST – Centro de Investigación en Sistemas y Telecomunicaciones, Universidad Estatal Península de Santa Elena, La Libertad, Ecuador
[5] Algoritmi Centre, Minho University, Guimarães, Portugal

nelson.duarte@islasantarem.pt, nuno.coelho@islagaia.pt, tguarda@gmail.com

Abstract. The correct management of information systems security is often overlooked in technological measures and management efforts, and although there are now many tools to address security threats, the human aspect has been neglected. This paper discusses the human factors that could potentially lead to intrusions with social engineering. Social engineering is a method used by hackers to obtain access to systems by manipulating flaws in behavior known as mental preconceptions. Social engineering is a risk to security information and must be considered just as important as in technological areas. In this paper we also approach social engineering, taking an introductory brief in its history, what is psychological manipulation and human weaknesses, what are the social engineering attacks, how they use authority and fear establishment, it is also approached how a social engineering attack is executed, providing value monetizing the scam, and identity exploration.

Keywords: social engineering attacks, psychological manipulation, human weaknesses, identity exploration.

1 Introduction

The internet is the largest means of communication available to us today, it is through the internet that we communicate in most diverse ways, using different means of communication. Social networks have become one of the privileged ways for us to get in touch with other people, whether on a personal or professional level. Organizations increasingly expect their employees to be connected to the company, either by devices that the company provides or by their own devices [1]. Decentralized access to online data and services has brought about a paradigm shift in information sharing and an increase in platforms for doing so. People post all kinds of information on social media without realizing that what they are sharing could be used by someone who might want to compromise the security of systems of the company they work for. Although systems are constantly being updated in terms of security, they end up being not very effective when employees are manipulated through social engineering [2]. The expression "knowledge worker" was introduced by Peter Drucker about 50 years ago and still applies to employees where their main characteristic is knowledge. [3].

One of the most powerful tools a hacker has to access privileged information is Social Engineering, where people are manipulated into giving out information they shouldn't. It is a technique superior to most other hacking techniques because it allows them to breach the most secure systems, since users are the most vulnerable part of any system. Social engineering does not require great technical skills and can be performed on a large scale. Social engineering is widely exploited on social networks and sharing platforms, allowing large companies worldwide to fall target to advanced attacks on their computer structures [2].

One can refer to the attack on Google's system in 2011 [4], where it was compromised, the attack on Facebook in 2013 [5], or the attack on the New York Times in the same year where hackers allegedly connected to the Chinese government attacked the computer systems, taking over some passwords [6].

Regarding security and privacy of systems there has been a strengthening of these issues due to the high number of attacks that have been reported in the media, with main focus on attacks by email, which is the main method of communication used for this type of attack by hackers and social engineers, however this awareness in services on the cloud and social networks is still relatively small [7].

The contributions of this paper aim to make an introduction to the history of Social Engineering, what is psychological manipulation and human weaknesses, Social Engineering attacks, how to perform a Social Engineering attack, how to obtain value and how can the attacker benefit from identity exploitation. This article aims to alert companies, employees, public and private entities to the different types of attacks perpetuated through Social Engineering, showing how they are executed, so that the reader can be enlightened and consequently prevent these same attacks that cost companies millions. It is also intended to help other authors in the study and research of this subject.

2 Social Engineering Human Manipulation

Human manipulation in social engineering, in information technology, is the manipulation of the behavior of people to have certain behaviors that could endanger computer systems, whether personal or corporate. Human personality is prone to be manipulated to carry out social engineering attacks [8]. These attacks are mainly aimed at getting an individual to perform certain actions unconsciously, as explained by [9].

2.1 Psychological Manipulation

The goal of psychological manipulation is to get a person to perform a certain action or to reveal confidential information without realizing that they are doing so. people are considered to be the most vulnerable link in an information system, which is why they are also the preferred targets of hackers [10].

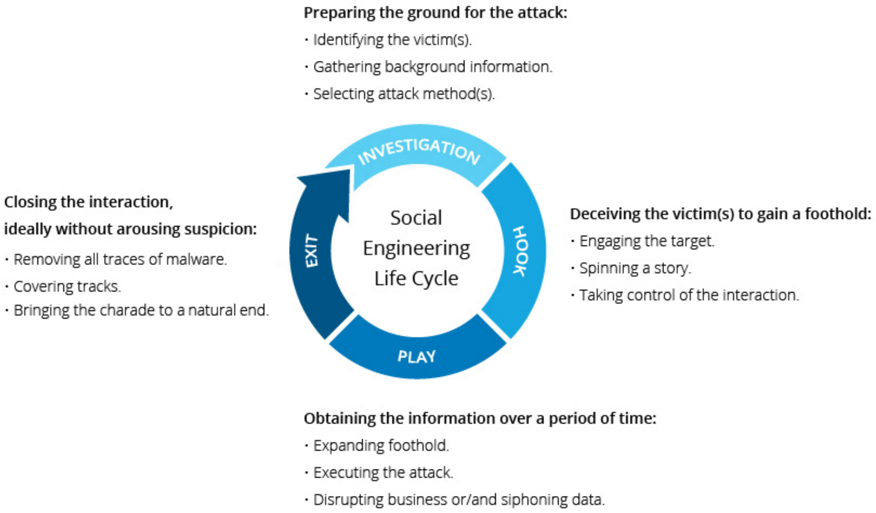
in computer infrastructures there are firewalls that cost companies a lot of money, information systems have implemented access controls with very tight rules about who has access to what and also have antiviruses that block malicious code from entering servers and other devices on the network, but despite the existence of all these security mechanisms we have the human vulnerability, the people who are inside the network and have access to information. this paradox leads us to Social Engineering, where all these security systems can be compromised by a person in the company who has access to confidential information and advanced permissions [11].

2.2 Human Weaknesses

One of the most exploited human weaknesses in Social Engineering is greed, offering something that the person wants or needs. It is common to use emails offering cash prizes by email as a form of phishing, of course then more information will be requested from the user that will allow other types of attacks. Another weakness is fear, where the attacker scares the user and convincingly threatens him to the point of providing privileged information. Curiosity is another form of weakness, people are curious by nature and this curiosity can lead to problems. Facebook is an example of how click-jacking scam schemes can be realized where a video appears with a text that arouses the user's curiosity and when the user clicks on the video, he loses control over his computer [12].

3 Social engineering Attacks

Social Engineering is the art of making someone to compromise computer structures and infrastructure. The Social Engineering life cycle, as referenced in Figure *1*, shows us that attackers first identify potential victims by searching for relevant information and selecting the best attacks, then they try to gain the victim's trust through social engineering schemes, using that information to execute attacks and gain control over the systems, and finally they remove the traces of their interaction so that they cannot be incriminated or related to the attack [2].



Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Figure 1 - Social Engineering Attack Lifecycle

3.1 Reverse Social Engineering

Hackers target people with privileged access to systems and try to contact potential victims indirectly by posing as a credible entity. The goal is to get victims to make contact and ask the attacker for assistance. This approach is called "reverse social engineering" [13] and consists of damage, assistance, and publicity [14]. The first approach consists of sabotaging the organization's computer system, it can range from disconnecting users from the network to manipulating software installed on the victim's computer. hackers may later contact the company saying they can fix the problem. When the hacker is asked for help, the hacker will ask for the victim's password to solve the problem or ask the victim to install a certain program [15].

3.2 The Technical approach

The Internet is one of the main means used for cyber-attacks. Granger [16] tells us that the web is very attractive for hackers to get passwords, since people frequently use the same (mostly very simple) passwords for the various systems they have online. Users are unaware that they are giving out critical information. Hackers use search browsers to get private information from potential targets. Some tools are available that allow attackers to collect information from other resources on the web. one such tool is Maltego [17]. social networks are a valuable source of information for these types of individuals.

3.3 Office communication

The new online communication platforms have dramatically changed the way teams communicate with each other in companies, making it possible to share information at a great speed. Although these platforms are protected with security devices and software, social engineering attacks are still not properly addressed in security plans. In enterprises face-to-face communication has largely been substituted by email and chat applications, creating a new opportunity for hacker attacks. Social engineering attacks initiated from inside accounts or known emails are easier to succeed with a prospective victim. Parsons et al. [18] performed an experiment with 117 participants where they were tested on their ability to distinguish between phishing emails and authentic emails. They found that people with a high level of awareness were capable to detect substantially more phishing emails has shown in Figure *2*, private information obtained across social engineering had direct effects, such as gaining access to bank accounts or indirect consequences such as identity theft [19].

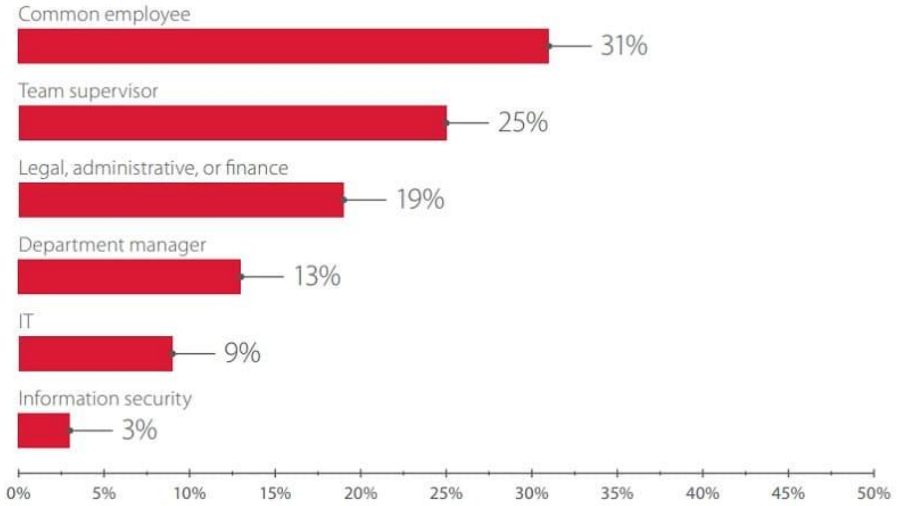


Figure 2 - Phishing attacks on employees by department

3.4 Authority and Fear Establishment

In this kind of attack the hacker uses fear trying to convince the victim that his computer may have a virus, pretending to be a credible entity, like Microsoft, making the victim believe he's being contacted because he's using a Windows operating system and that Microsoft knows what's going on with his computer, establishing authority in this case. As most users have little experience with computers, they become afraid, and that's when the attacker tries to convince the victim that the best solution will be to remotely access his computer to solve the problem. What the hacker really wants is to create authenticity regarding the serious problem that may be on the victim's computer [17]. After gaining control of the victim's computer the blackmailing for value begins.

3.5 Identity Exploration

For identity exploitation there are several tools available on the Internet, some paid and some free, and they are widely used by hackers to obtain information about potential victims. There is a tool called pipl that is a people search engine and allows you to search various sites for data a person has online. It is one of the most powerful tools to find personal and corporate information, emails, phone numbers, files, and posts. In a short time, a hacker can gather enough information to carry out a successful attack. [2]

3.6 Personal Contact

In these types of attacks hackers personally contact the victim, interacting with the victim, to get information that will allow them to perform an attack on the victim or the company where the victim works. This type of information may vary depending on what the hacker wants, usually it will be information related to the target. another way to get information will be to rummage through garbage bins looking for papers that may have been thrown in the trash and may contain relevant information about the company, often employees throw papers away when they should shred them so they cannot be read. these papers may have information about employees, reports about the company and in some cases even information about computer access such as users and passwords. One of the practices of some less informed employees can lead them to write their passwords on papers so that they don't forget them and throw them in the trash absentmindedly. Other types of personal attacks involve stealing or extorting people to get data [20].

3.7 Tailgating

The common characteristic in this type of attack is that the attacker creates a character and invents a false story around the character trying to exploit the victim's basic emotions, sympathy, greed and fear [21]. The technique, basically, consists of following a person with authorized entry into a restricted access location. Less enlightened employees may be easily misled. Employees in less senior positions may fear that they will be denied access by senior managers and the potential (undue) reprisals that will ensue. The social engineer may use a variety of techniques to gain access to the site, such as access, such as using conversation and sympathy to gain the victim's trust in order to provide access, convincing access, convincing them that he has forgotten or lost his card, pretending to be a new colleague at work, using a fake card and excusing himself with a possible malfunction, or pretending to be someone in authority [22].

3.8 Socially Engineered Attacks

One of the most common ways of carrying out social engineering attacks are social approaches. By socially approaching victims, hackers use social-psychological methods to persuade victims. An example of this is the use of authority, or curiosity employed in spear-phishing and baiting attacks. These types of attacks are only successful if the hacker can establish some sort of trust relationship with the victim. Most of these attacks are carried out by phone calls [15].

The majority of attacks in 2018 were aimed at direct financial profit or obtaining sensitive information. However, attacks aimed at data theft often have financial implications: data can be used for stealing money, blackmailing, and can even be sold on the dark web. The graph in Figure *3* shows us the most common reasons for hackers to carry out attacks.

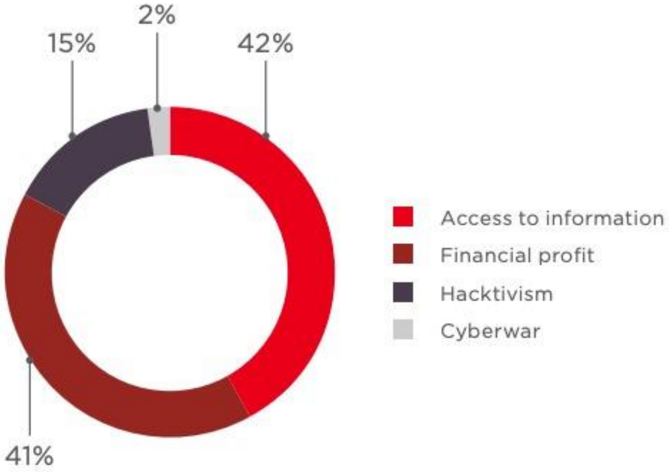


Figure 3 - Most common attacker motives

3.9 Attacks on Social Networks

Although you can get information in traditional ways as mentioned in the previous topic, not all hackers are predisposed to this type of attacks, nowadays; through social networks, you can easily access information about almost everyone. This information can be a starting point to initiate attacks. This kind of information allows you to get phone numbers, emails, places often visited by victims, family members and workplaces [23]. LinkedIn is one such social network, where people post on their profile where they work, in which department and often even the computer equipment the company uses. An employee who posts his or her email address on their profile may be opening the door to a spam or phishing attack that could compromise the company they work for. Phishing is a widely used attack on the Internet, this type of attack can direct victims to fake websites where hackers can try to collect passwords to access the real sites or bank card information. Many of these phishing attacks are very successful because the hacker pretends to be a friend of the victims, which increases his credibility [24].

3.10 Most commonly used Attacks in enterprises

Data provided by PORDATA (2012), indicates the rate of Internet use by companies with 10 or more employees was 98%. Among the various activities carried out through the internet, email processing (sending and receiving) and information search are the most used activities, and in contact with public bodies and financial institutions the internet is the preferred medium. With the growing importance of the use of this medium, attacks have been aimed at exploiting its vulnerabilities. In the use of various services - email, online contacts with financial institutions and public bodies, chat services, downloads, among others - companies are vulnerable to various types of attack - malware, spying, phishing, interesting software, hoaxing, pop-ups, etc [25].

For example, when using email services, institutions are vulnerable to attacks, especially malware. A virus infection can result in the installation of backdoors in order to guarantee to malicious third parties' access and control of the infected machines, with potential disclosure of information and also the execution of attacks on other systems from the former. On another note, it is universally recognized that companies, in order to reduce costs with the storage of information, are turning to storage services and file sharing in the cloud. In their use, institutions hand over the management of their information to third parties, losing control over the processes that are running or where data is stored. Before subscribing to these services, customers, in order to reduce the risks associated with their use, should certify that the supplier guarantees the integrity, availability, confidentiality, authenticity and non-repudiation of the information [17].

According to the study developed by ISACA, which included more than 1500 companies from more than 50 countries in Europe, Middle East and Africa, one in five companies that are cloud computing clients do not value the risks of using the technology. Nearly two-thirds were willing to assume a certain level of risk, (12%) of IT managers said they were willing to take the risk to maximize business return.

In the analysis of the services that are used over the phone, it appears that this is the preferred means of contact with partners (98%), with this channel being associated with the possibility of various types of attacks - impersonation/pretexting, smishing, vishing, among others. By including the use of smartphones in the analysis, one should add the attacks associated with the use of the internet, since this type of equipment allows access to the service [25]. The graph in Figure *4* shows us which sectors have the most business attacks.

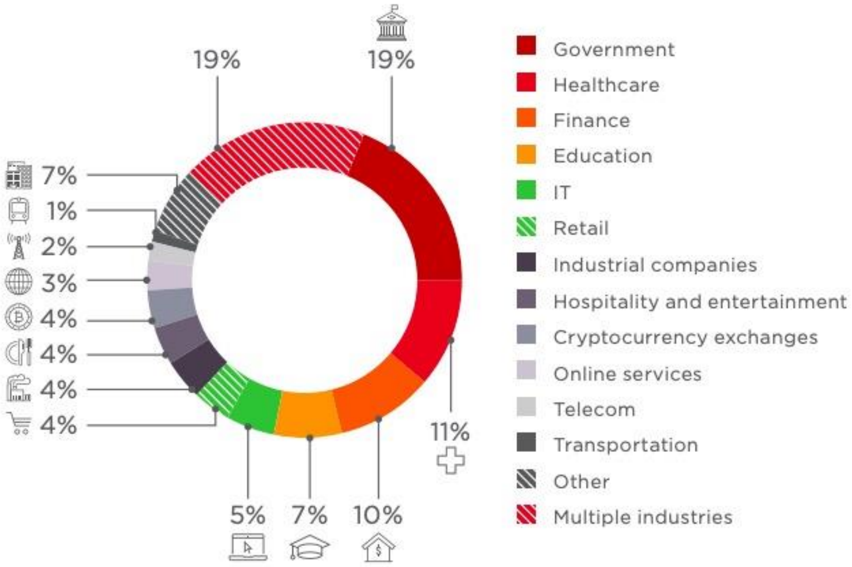


Figure 4 – Organization victims' category

4 State of Future Attacks in enterprises

According to Kevin Haley, Security Response Specialist at Symantec, the attack risks will tend toward: cyber conflicts; emergence of Ransomware [26]; emergence of malware for mobile devices - madware [27]; scams linked to social networks and attacks on mobile platforms and cloud services.

Regarding cyber-attacks, Kevin states that conflicts between nations, organizations and individuals will tend to be developed in the virtual world. The application of espionage technique, in the virtual world, may be successful.

New malware [28] will emerge, including Ramsomware and Madware. Ramsomware is a type of attack consisting of malicious software that locks the computer and demands a ransom fee to unlock it.

Mobile devices are increasingly used both inside and outside corporate networks, containing sensitive data and information increase the information security risks and arouse interest in the development of attacks. Madware is a type of malware developed for mobile devices, which aims to collect information. This type of threat installs itself on devices through app downloads. This type of attack has increased significantly in the last months. A significant part of these attacks is carried out by social engineering [29].

5 Conclusions

In this paper, we described common attack scenarios for modern social engineering attacks on victims. Policies and distributed collaboration as well as communication over third-party channels offers a variety of new attack vectors for advanced social engineering attacks. We believe that a detailed understanding of the attack vectors is required to develop efficient countermeasures and protect knowledge workers from social engineering attacks. Situations were presented that happen on a daily basis, regarding advanced attacks used in organizations, in communications on online platforms and social networks. Social engineering attacks are attacks that exploit individuals' social and psychological vulnerabilities, attacking weaknesses such as vanity, loneliness, self-centeredness, and others, taking advantage of these weaknesses to target companies through their weakest link, which is the human being. It is extremely important that companies invest in the training and dissemination of this type of attack so that employees can be more alert. We hope this article can contribute to alert organizations and employees to the importance of these attacks, which are increasingly frequent and cost companies millions.

References

1. R. Ballagas, M. Rohs, J. G. Sheridan and J. Borchers, "BYOD: Bring your own device," in *Proceedings of the Workshop on Ubiquitous Display Environments,*, 2004.
2. K. Krombholz, H. Hobel, M. Huber and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and applications*, no. 22, pp. 113-122, 2015.
3. P. F. Drucker, Landmarks of tomorrow: a report on the new ”post-modern” world. 1st edition, New York: Harper, 1959.
4. RSA, "Anatomia de um ataque," RSA, 17 Julho 2013. [Online]. Available: http://blogs.rsa.com/anatomy-of-an-attack/.
5. M. J. Schwartz, "Microsoft Hacked: Joins Apple, Facebook, Twitter," InformationWeek, 25 02 2013. [Online]. Available: https://www.darkreading.com/attacks-and-breaches/microsoft-hacked-joins-apple-facebook-twitter/d/d-id/1108800?. [Accessed 26 02 2021].
6. N. Perlroth, "Hackers in China Attacked The Times for Last 4 Months," New York Times, 30 01 2013. [Online]. Available: https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html. [Accessed 2021 02 26].
7. M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek and E. Weippl., "Social snapshots: digital forensics for online social networks," in *27th Annual Computer Security Applications Conference*, 2011.
8. R. Maurya, Social engineering: Manipulating the human (Vol. 1), Scorpio Net Security Services, 2013.

9. A. Kamis, "Behavior Decision Theory," istheory.byu.edu, 2011. [Online]. Available: http://istheory.byu.edu/wiki/Behavioral_. [Accessed 1 09 2017].
10. S. Jackson, Research Methods and Statistics: A Critical Thinking Approach, Belmont, CA: Wadsworth, Cengage Learning, 2008.
11. T. Qin and J. K. Burgoon, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering," *Intelligence and Security Informatics*, pp. 152-159, 2007.
12. T. Peltier, "Social Engineering: Concepts and Solutions," *Information System Security*, vol. 5, no. 15, p. 13–21, 2006.
13. S. Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus, 2001.
14. C. F. M. Foozy, R. Ahmad, M. F. Abdollah, R. Yusof and M. Z. Mas'ud, "Generic taxonomy of social engineering attack and defence mechanism for handheld computer study," in *alaysian Technical Universities International Conference on Engineering & Technology*, Batu Pahat, Johor, 2011.
15. S. Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus, 2001.
16. S. Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus, 2001.
17. A. Wagner, Social Engineering Attacks, Techniques & Prevention, UK: Lightning Source, 2019.
18. K. Parsons, A. McCormac, M. Pattinson, M. Butavicius and C. Jerram, Phishing for the truth: A scenario-based experiment of users' behavioural response to emails, FIP Advances in Information and Communication Technology, 2013.
19. L. Tam, M. Glassman and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," *Behav. Inf. Technol,* pp. 233-244, 2010.
20. S. Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus, 2001.
21. M. Workman, A teste of interventions for security threats from social engineering, Emerald Group Publishing Limited, 2008.
22. K. D. Mitnick and W. L. Simon, The art of intrusion: The real stories behind the exploits of hackers, intruders, & deceivers, Indianapolis: Wiley, 2006.
23. M. Huber, S. Kowalski, M. Nohlberg and S. Tjoa, "Towards automating social engineering using social networking site," *CSE'09. International Conference on, volume 3,* p. 117–124, 2009.
24. M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek and E. Weippl, "Social snapshots: digital forensics for online social networks," *In Proceedings of the 27th Annual Computer Security Applications Conference*, 2011.
25. F. Silva, "Classificação Taxonómica dos Ataques de Engenharia Social," 2013.
26. A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks.," *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 3-24, July 2015.
27. A. Feizollah, N. B. Anuar, R. Salleh and A. W. A. Wahab, "A review on feature selection in mobile malware detection," *Digital investigation,* vol. 13, pp. 22-37, 2015.

28. J. Sahs and L. Khan, "A machine learning approach to android malware detection," *2012* European *Intelligence and Security Informatics Conference,* pp. 141-147, August 2012.

29. K. Haley, "Symantec's Cloud Security Threat Report Shines a Light on the Cloud's Real Risks," 24 06 2019. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantecs-cloud-security-threat-report-shines-light-clouds-real-risks. [Accessed 9 03 2021].