Information security threat assessment using social engineering in the organizational context – literature review

António Lopes[1][0000-0001-8996-6394], Leonilde Reis[2][0000-0002-4398-8384], Henrique São Mamede[3][0000-0002-5383-9884] and Arnaldo Santos[4][0000-0001-5139-6728]

[1] ESCE IPS Polytechnic Institute of Setúbal, Setúbal, Portugal
[2] ESCE CICE IPS Polytechnic Institute of Setúbal, Portugal
[3] UAb - INESC TEC, Universidade Aberta, Lisbon, Portugal
[4] UAb - Universidade Aberta, Lisbon, Portugal

[1] antonio.jorge.lopes@esce.ips.pt
[2] leonilde.reis@esce.ips.pt
[3] hsmamede@gmail.com
[4] arnaldo.santos@uab.pt

lncs@springer.com

Abstract. Due to the value and diversity of data that organizations use and produce in their activity, it is extremely important to protect this asset. Security flaws can arise due to several factors and whenever it is difficult to access the desired information because of technological barriers. In this case, attacks are redirected to the exploitation of human beings vulnerabilities through various techniques. The objective of this work focuses on literature review, studying the underlying theme of Social Engineering, as it uses human trust, convincing someone of something fake, using various interactions and different vectors to gain access to private information. Design Science Research will support the research work due to the possibility of construction, evaluation, and subsequent validation of the artefact. The contribution of a framework proposal for preventing social engineering attacks in organizations and providing the best recommendations, guiding, and supporting the stakeholders in the selection and definition of controls that guarantee the security of organizational information and avoid possible attacks by Social Engineering. It is expected that the practical effects of the future work will result in a reduction in the number of attacks using Social Engineering, greater individual and collective preparation to deal with this problem and, over time, the incentive to the continued expansion of the adoption of these artefacts at the organizational level.

Keywords: Social Engineering, Information Security, Information Systems, Information and Communication Technologies.

1 Introduction

In modern society, data plays an important role in virtually every context and has enormous value. In the organizational context, since they start their activity, a set of different types of data is gathered, making the proper protection of this asset very relevant. After its processing, data can generate information to support organizational decision making. Information has become an essential resource for the management of modern organizations [1]. The attributes that must be guaranteed are classified by [28]: confidentiality, integrity, availability, authenticity, and accountability.

Thus, since information is one of the main resources used in organizational activity, Information Security should be a constant concern of organizations since it increasingly presents greater dependence on Information Systems (IS) and information and Communication Technologies (ICT). Information Security attacks aim to steal confidential data, which leads organizations to invest more in Information Security. The training of soft skills and good practices has a relevant role in raising users awareness of organizations' Information Security, which, if applied, could have avoided or mitigated these attacks [10].

Social Engineering (SE) consists of attacks involving psychological manipulation of humans, carried out by attackers to influence people to take actions, either against themselves, without acknowledging this fact, or against third parties, namely organizations [13]. SE is the acquisition of information about computer systems through non-technical methods and meanings. While the technical security of most critical systems is high, the systems remain vulnerable to attacks by social engineers [4]. Traditional approaches to security are often focused on the vulnerabilities of a system or computer network. Few approaches consider the vulnerabilities of humans through SE, and none of them analyzes the personal behaviours of employees [4].

Although the number of SE attacks and the damage they cause has been increasing, awareness and consideration of these types of attacks when defining security requirements remains negligible. Thus, in an increasingly global society, in which the interaction between people and IS is carried out through ICT, [6] considers that people are more exposed than ever. The most practised and effective penetration attacks are social rather than technical.

1.1 Contribution

The paper presents the research in progress for the development of an SE prevention framework. In this sense, we understand that Systematic Literature Review (SLR) and future research are pertinent work due to the relevance of strengthening, within organizations, the recognition by organizational managers and those responsible for IS to issues related to Information Security. More specifically, in this context, addressing issues related to the prevention of potential SE attacks through the adoption of best practices, information, and knowledge about the techniques most used in attacks to Information Security. In this sense, the framework that will be developed intends to fill a gap in this area, support organizations in the detection of SE attacks, enhance the

identification and mitigation of attacks, and minimize the risk. In practice, the aim is to find a solution to a problem that proves to be original, relevant, and verifiable.

The Design Science Research (DSR) methodology will be adopted as a theoretical basis to support the scientific validity for the preparation of this work [24]. It is an indicated research methodology for research projects in technologies and IS systems architectures [11]. It is complemented that this is also a methodology inherent to the activity of artefact design, ensuring, in this way, discipline, rigour and transparency [23], cited by [16]. The DSR methodology is a research method that suits the IS area with connection to issues that they originate in organizations, contributing to the resolution of specific and complex problems [5] & [14], cited by [26]. DSR methodology is a problem-solving paradigm that aims to improve human knowledge by creating innovative artefacts that solve problems and improve the environment in which they are instantiated [7]. The DSR methodology will be used according to the specificity of the ongoing research work.

1.2 Motivation

In this line of reasoning, we are motivated and intend to investigate whether organizations are aware of potential SE attacks. The future development of a framework proposal (conceptual framework) to prevent SE attacks based on international standards will aim to promote and disseminate knowledge in this area.

There are several open questions, which were identified in the preliminary literature review and which we present below: (1) There is still a need to explore a set of different SE techniques [30], which can provide an insight into which methods are most effective, leading to the creation of a standard approach for SE. This pattern can later be integrated with future security reviews in organizations. (2) Another unresolved issue is identified and translates into developing new detection and prevention techniques against SE attacks [27] and programs to train organizations' employees.

The work intends to address those issues when developing the proposed framework for the prevention of SE attacks, which allows organizations to understand their level of maturity regarding the prevention of this problem. Currently, it is a good opportunity to carry out the study. It is inserted in the most sensitive and transversal area of organizations.

It is intended to provide guidance and best practices regarding the responsiveness of organizations in the context of detecting potential SE attacks. Through research, it is intended to develop an innovative work, which allows providing organizations and their employees with an artefact that allows them, during their activity, a greater concern, attention, awareness and new knowledge in the context of SE. The base will consist of several techniques that can be used by attackers, called social engineers, to exploit their vulnerabilities, to obtain confidential information, whether personal or organizational. More specifically, the steps that are intended to be achieved during the investigation will be: (1) Identification of the SE techniques used by attackers, establishing a relationship with international standards, best practices and models referenced by the scientific community, so that the proposed framework to be developed can cover different contexts and allow a global perspective, according to each of the references indicated

initially. (2) Development of the framework proposal (conceptual framework) to prevent SE attacks, allowing organizations to identify potential SE attacks. (3) Verification of the scope of the developed framework proposal, using the various SE attack techniques, models and best practices identified in the literature review.
The research work intends to present a proposal for an adaptable framework to support organizations in preventing threats to Information Security. Lines of action will be proposed for a timely response to SE attacks.
It is important to disseminate the SE concept and the awareness of organizations and their employees about this threat, referring to how it manifests itself in a hidden way, which techniques are most used by attackers and the respective forms of defence and detection available. Reinforcing the importance of security and information integrity will allow greater ability to identify attacks, increasing Information Security. In practice, models/frameworks should be created that allows employees to know about security policies and procedures for dealing with confidential information while evaluating their exposure to ES. It is intended that it is possible to maintain the business processes supported by the organizational IS without disturbance [19].

2 Related Work

Most companies are based or even totally dependent on information such as financial data for banks to remain in the market and be competitive [9].

For organizations, information is the organizational resource with the greatest value after human resources [18], allowing managers to make the right decisions, defining the business strategy, performance and competitiveness, to the existing competition in the market(s) where they operate. Information Security should be an obvious concern for organizations, given the current context of business dependence on IS and ICT [18]. SE reveals itself as an increasingly present threat today [18], although it is quite neglected. In this sense, it becomes increasingly pertinent that managers and those responsible for IS recognize the importance of Information Security. In this specific context, it becomes increasingly pertinent to know which attack techniques are used and the best practices regarding its protection.

The growing number of Information Security incidents caused by employees of organizations requires the development of methods to assess the Information Security system through improvements in the safety of its human resources [2]. Many authors are investigating the Information Security culture from the human perspective as a critical resource for the successful protection of information resources [31]. A person can become an object or target of SE through psychological influence or manipulation by attackers.

2.1 Information Security

This area is a discipline that is growing fast. Information protection is of vital importance to organizations and governments, and the development and adoption of measures against illegal access to information is an area that is receiving increasing attention [20]. It does not matter how secure the organization is, how advanced the

technology is, or the level of an application update. There is still a vulnerability in all sectors – the "Human" factor. Human beings are also considered vulnerable, as people present in different sectors of activity can also be used to obtain confidential information. In this context, the concept of SE arises, referring to the manipulation of individuals to induce them to perform specific tasks or provide information that may be useful to an attacker. SE does not necessarily require a great deal of knowledge about many techniques to be successful. Instead, SE enhances the use of common psychological aspects of human beings, such as curiosity, courtesy, credulity, empathy, and greed. SE has increased a lot in recent years. SE was used in 95% of attacks in recent years [17].

2.2 Social Engineering

Over the years, there have been a series of attempts to define the concept of SE, namely in the literature, in which each author has been presenting their views [8]. According to [28], the term was described as "Human Hacking" [8], the art of tricking people into revealing their credentials and then using them to gain access to networks or accounts. On the other hand, [22] advocates that SE attacks have been around for some time. SE attacks use psychological manipulation to trick users into providing confidential information so that attackers gain unauthorized access to a computer system. The term can also include activities such as exploiting human vulnerabilities. The term is defined as a violation of organizational security through interaction with people to induce them to break normal security procedures [12], cited by [29].

Also, [29] advocate that the lack of a structured definition of the concept led to elaborating works that focused exclusively on an attempt to define the term. In this sense, [32] present a subdivision of SE, in cybersecurity, as a type of attack in which the attacker(s) exploit human vulnerabilities through social interaction to violate cybersecurity, with or without the use of technical means or technical vulnerabilities.

The art of obtaining confidential information from a human being is known as SE [17]. ICT use has increased exponentially over the last few years, but the SE threat is still an issue. SE attacks can happen in organizations due to lack of awareness and knowledge about this issue. SE is a very common practice to obtain confidential information and data using phone calls, emails, SMS or direct approach to potential victim(s). SE can be very useful to the attacker if proper technique is used. SE uses human behaviour to the detriment of technical ways to explore systems, data, or anything useful and profitable [3]. It is a technique based on human behaviour to hack and persuade people so that it is possible to access someone's system.

SE turns out to be of particular interest in allowing the optimization of Information Security practices given the specificity of the business [18]. Thus, it is considered that SE has emerged as a serious threat in virtual communities and is an effective means to attack IS. The services used by employees enhance the preparation of spaces for sophisticated SE attacks.

Thus, at this stage of elaboration of the work plan, it is intended to present that SE aims to carry out attacks through human interaction and exploitation of the respective vulnerabilities, usually initiated by people called social engineers, who through a set of

techniques available and social skills try to obtain confidential information, compromising organizational information. The relevance of this theme is highlighted, given its importance in an organizational context.

3 Social Engineering - Framework

Through the previous section, it was possible to verify that there are several types of attacks that social engineers can use in the context of SE. Advances in ICT have made communication between humans more accessible and instantaneous. SE is one of the biggest challenges for organizational Information Security because it taps into the natural human tendency of trust [27]. SE attacks are increasing, and security mechanisms are becoming less and less secure. These types of attacks aim to psychologically manipulate people to disclose valuable information and confidential data of interest to cyber criminals [15], cited by [27]. SE is challenging the security of networks and IS, regardless of the robustness of its firewalls, encryption methods, intrusion detection systems and antivirus software. Humans are more likely to trust other humans compared to computers or technologies. Therefore, from this perspective, humans are the weakest link in the security chain [25], cited by [27].

Although SE attacks may differ, they have a common pattern [21], cited by [27]. The common pattern is described through four phases: (1) obtaining information about the target; (2) developing a relationship with the target; (3) exploiting available information and executing the attack; and (4) leaving without a trace.

It was possible to verify that it is possible to obtain confidential information through the exploitation of human vulnerabilities. In organizations, to prevent employees from becoming victims of SE attacks, adopting methodologies for controlling access to information is pertinent. So far, being a relatively recent concept, there are some models (see Fig. 1) where the attack can be divided into more than a phase, each being treated as a new attack, according to the model [21].

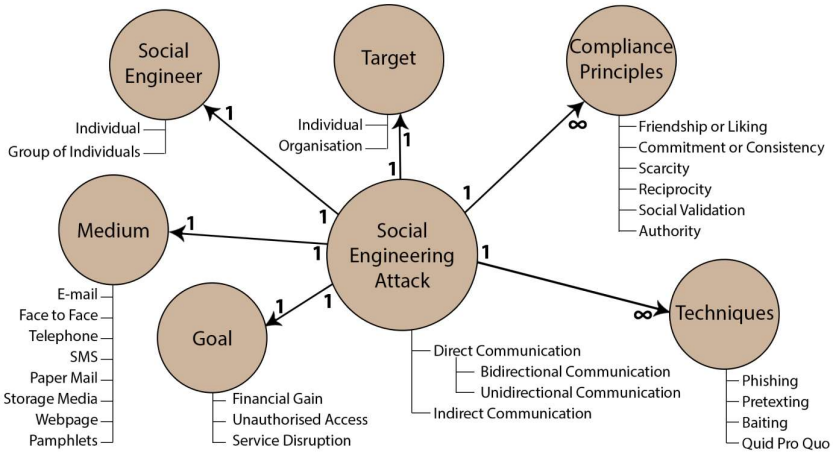

Fig. 1. An ontological model of a Social Engineering attack (adapted from [21]).

In terms of the attack framework, [21] also present a proposal (see Fig. 2), which illustrates the planning and flow of an attack in generic terms, involving six main phases, namely the planning of the attack, gathering information about the victim, preparing, developing the relationship, exploring and finishing without a trace, achieving the objective - obtaining confidential information.

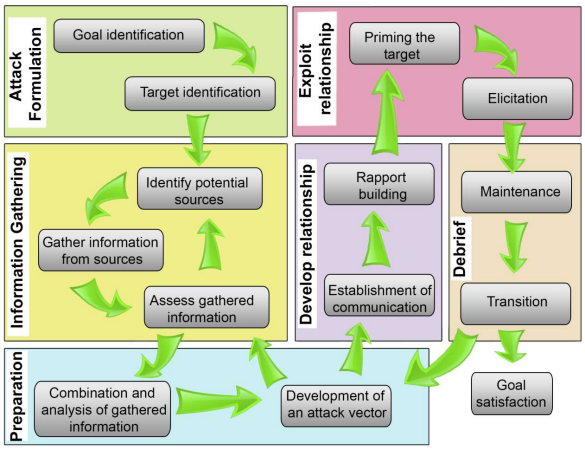

Fig. 2. Social Engineering attack framework (adapted [21]).

In this follow-up, current studies intend to demonstrate the usefulness of SE attack frameworks in preventing SE attacks. One of these studies published by [21] states that when a question is asked to the potential victim of an attack, it is very important that they understand, without any doubt, what kind of information is being requested, that is, whether it is confidential. We intend to present a new artefact in this domain, not in the SE attack perspective, but in the domain of prevention of SE attacks, using the best practices described in international standards and norms.

4 Future work

Currently, an SLR is underway, following the Barbara Kitchenham protocol guidelines. Through a preliminary review of the literature, attacks using SE techniques are harmful to any organization. Many organizations have been victims of this type of attack in recent years, having obtained confidential data from the organizations and their employees.

Based on the studies analyzed, it can be concluded that most incidents with Information Security are related to processes and human behaviour itself, to the detriment of more technical issues. This issue, increasingly present in organizations, intends to show that information is a constant target regarding the violation of its basic properties, namely its integrity, confidentiality, and availability, through exploiting human vulnerabilities.

Thus, organizations and their employees should be aware of the issues underlying SE. It is considered that the review of the state of art allowed fostering motivation for research towards the development of a model that could effectively allow us to understand if the attacker is trying to exploit a person's vulnerabilities to obtain confidential information.

After the SLR, using current and comprehensive literature, including key articles relevant in the context of the area under investigation and regarding the next steps of the work in progress, it is intended to aiming to define the constituent elements of the Framework to be developed, so that it is adaptable to different organizational contexts. In practice, the aim is to find a solution to a problem that proves to be original, relevant and verifiable.The Framework consists of a proposal that will be developed analyzing international norms and standards of security good practices, realizing how these standards can contribute to the development of an Information Security Framework in the context of Social Engineering. This artefact will be validated using focus group technique, in order to be able to assess whether it is complete, whether it solves the problem that was initially identified, whether there are any aspects that need improvement and whether it covers all areas related to SE. After the validation mentioned above, it is intended to carry out a case of application of the Framework, so that it is possible to draw conclusions about its applicability and usefulness. The Framework should be adaptable and extensible over time, according to new ES attack techniques that emerge.

It will have as its main objective the promotion and systematization of organizational knowledge in this area to prevent, reduce the number of attacks and encourage the continued adoption of this type of artefacts in an organizational context. SE is a current problem in society in general and in organizations, and it is also a novelty in some contexts.

References

1. Ada, Ş., Ghaffarzadeh, M.: Decision Making Based On Management Information System and Decision Support System. European Researcher. 93. 260-269 (2015).
2. Astakhova, L.: Evaluation Assurance Levels for Human Resource Security of an Information System. Procedia Engineering. 129. 635-639 (2015).
3. Bansla, N., Kunwar, S., Jain, K.: Social Engineering: A Technique for Managing Human Behavior (2019).
4. Beckers, K., Pape, S.: A Serious Game for Eliciting Social Engineering Security Requirements (2016).
5. Bianchi, I., Dinis, R.: Governança de TI em universidades públicas: Proposta de um modelo. Instituto Universitário de Lisboa (ISCTE-IUL). Homepage, http://repositorium.sdum.uminho.pt/handle/1822/39467, last accessed 2021/11/01.
6. Breda, F., Barbosa, H., Morais, T.: Social Engineering and Cyber Security (2017).
7. Brocke, J., Hevner, A., Maedche, A.: Introduction to Design Science Research (2020).
8. Conteh, N., Schmick, P.: Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research (2016).
9. Diesch, R., Pfaff, M., Krcmar, H.: A Comprehensive Model of Information Security Factors for Decision-Makers. Computers & Security (2020).
10. Farinha, P., Sousa, G.: O Impacto da Consciencialização dos Colaboradores na Segurança da Informação das Organizações. Revista CyberLaw. Edição N.º XI. Março 2021. CIJIC (2021).
11. Ferreira, I., Ferreira, S., Silva, C., Carvalho, J.: Dilemas iniciais na investigação em TSI design science e design research, uma clarificação de conceitos. Proceedings of Conferência Ibérica de Sistemas y Tecnologias de Informação (2012).
12. Ghafir, I., Prenosil, V., Alhejailan, A., Hammoudeh, M.: Social engineering attack strategies and defence approaches. pp 145–149 (2016).
13. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. Baker, T.: Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74 (2018).
14. Hevner, A., March , S., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly, 1(28), 75–105 (2004).
15. Kalniņš, R., Puriņš, J., Alksnis, G.: Security Evaluation of Wireless Network Access Points. Applied Computer Systems (2017).
16. Lacerda, P., Dresch, A., Proença, A., Antunes, A.: Design Science Research: 89 método de pesquisa para a engenharia de produção. Gestão & Produção, 20(4), pp. 741–761. Homepage, https://doi.org/10.1590/S0104-530X2013005000014, last accessed 2021/11/01.
17. Lohani, S.: Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1. Homepage, https://ssrn.com/abstract=3329391, last accessed 2021/11/01.

18. Lopes, A., Reis, L.: Framework para Avaliação de Ameaças à Segurança de Informação com Recurso a Engenharia Social no contexto Organizacional. IFM Conference – Internacional Fórum on Managment (2021).

19. Lopes, A., Reis, L.: Engenharia Social: Uma ameaça oculta para a Segurança da Informação Organizacional. In Reis L., Cagica Carvalho L., Mata C., Simões D., Xara-Brasil D., Cordeiro J., Nabais J., Dias R., Galvão S., Barbosa V. (eds), Temas Emergentes em Ciências Empresariais - Novas abordagens nas áreas científicas da Contabilidade, Finanças, Sistemas de Informação, Metodologias e Práticas Pedagógicas. Edições Sílabo (2022).

20. Merwe, J., Mouton, F.: Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle (2017).

21. Mouton, F., Leenen, L., Venter, H.: Social engineering attack examples, templates and scenarios. Comput. Secur. 2016, 59, 186–209 (2016).

22. Pandey, A.: Phishing and Social Engineering Techniques (2019).

23. Pedro, S.: Modelação de Processos para as principais áreas de Recursos Humanos. Nova Information Management School (2015).

24. Peffers, K., Tuunanen, T., Rothenberger, M., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems (2007).

25. Pokrovskaia, N.: Social engineering and digital technologies for the security of the social capital development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19 (2017).

26. Roquete, M.: Modelo de maturidade para apoio à implementação de uma filosofia de gestão orientada a processos numa organização. Nova Information Management School, Lisboa (2018).

27. Salahdine, F., Kaabouch, N.: Social Engineering Attacks: A Survey. Future Internet. 11 (2019).

28. Stallings, W.: Cryptography and network security: Principles and practice, seventh edition. Harlow: Pearson Education (2017).

29. Venkatesha, S., Reddy, R., Chandavarkar, R.: Social Engineering Attacks During the COVID-19 Pandemic. SN COMPUT. SCI. 2, 78. Homepage, https://doi.org/10.1007/s42979-020-00443-1, last accessed 2021/11/01.

30. Van, D., Sjouw, A., Smakman, M., Smit, K.: Social Engineering as Approach for Probing Organizations to Improve IT Security: A Case Study at a Large International Firm in the Transport Industry. 119-126 (2019).

31. Veiga, A., Astakhova, L., Botha, A., Herselman, M.: Defining organizational information security culture – Perspectives from academia and industry. Computers & Security. 92 (2020).

32. Wang, Z., Sun, L., Zhu, H.: Defining social engineering in cybersecurity. IEEE Access. Vol. 8. pp. 85094. Homepage, https://doi.org/10.1109/ACCESS.2020.2992807, last accessed 2021/11/01.