DOI: 10.2507/35th.daaam.proceedings.xxx

SOCIAL ENGINEERING AS A PROBLEM IN SMALL ORGANIZATIONS

Miroslav Tomšů, Veronika Rosíková & Matúš Madleňák

This Publication has to be referred as: Tomšů, M[iroslav]; Rosíková, V[eronika] & Madleňák, M[atúš] (2024). Social engineering as a problem in small organizations, Proceedings of the 35th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/35th.daaam.proceedings.xxx

Abstract

Digital information technology surrounds us at every step, and it is part of our everyday lives. This increased reliance on digital technology brings both convenience and risks. This paper explores the issue of social engineering in the context of its impact and consequences. In the context of small organizations, the risk of these attacks increases due to limited resources for cybersecurity and inadequate employee training. This paper discusses solutions to the issue of social engineering and suggests measures that small organizations can implement to reduce the risk of these attacks.

Keywords: social engineering, cyber security, cyber-crime, organization.

1. Introduction

The increasing interest in digital technology in organizations has heightened the need for security, especially in case of social engineering, which is considered one of the biggest threats. Many authors address the issue of social engineering from the perspective of its techniques and general prevention [1, 2], of social networks [3], of the cognitive aspect [4], of machine learning techniques [5,6], or of the COVID-19 pandemic when work in organizations shifted to home offices [7], but few authors discuss its implementation into organizational policies [8, 9]. This issue is addressed by a study that focuses solely on the banking sector [10] or healthcare organization [11].

This area should be more concerned with implementing [12] the security management system enshrined in European Union law [13]. The issue, however, is binding only for specific organizations to which the law applies [14]. However, more attention is paid to this issue, which leads to organizations needing to prepare for the threat of social engineering.

This paper proposes specific security measures, methods, and tools that are not only against social engineering in small organizations.

2. Characteristics of social engineering

Social engineering is a form of attack that targets the weakest link in any security chain - a person. Moreover, people's actions are greatly influenced by their emotions, and this attack attempts to arouse the victims' positive or negative feelings. Most often, it is compassion, curiosity, shame or fear. When such emotions surge, the attackers rely on a judgment error that forces their victims to perform a task they would not normally do.

In short, social engineering can, therefore, be defined as a fraud based on psychological manipulation, the primary purpose of which is to lure the user into sensitive personal or payment information. It is much easier to fool the user and obtain data access than to circumvent the computer's security.

In practice, the deceived person trusts the false information given to him via email, call or SMS. For this reason, he begins to act according to the intended instructions the attacker gave during this contact. These instructions most commonly include clicking a link, downloading an attachment or software to a computer, or transferring a specific amount of money [15].

2.1. The most common social engineering techniques

Phishing - phishing is a form of social engineering. The attacker poses as a trustworthy entity and requests sensitive information from the victim under a seemingly legitimate pretext.

Spear Phishing - is a targeted form aimed at a specific individual, organization, or company. Typical phishing campaigns do not target victims individually – they are not sent to hundreds or thousands of recipients. The attackers' tactic is to exploit acquired internal information or publicly available information, such as the names of executives, and then manipulate email addresses to resemble official ones.

Vishing - a method similar to phishing emails, but instead of emails, it involves fraudulent phone calls. A cybercriminal disguises themselves, for example, as a bank or insurance company representative. Attackers benefit from making calls at night because their victims are less focused.

Smishing - an attempt to obtain trustworthy information through SMS messages. Smishing's goal is often to redirect users to a website that collects sensitive data. Some messages may prompt users to send sensitive information even in direct replies to SMS.

Scareware - malicious code that uses various techniques to induce anxiety and fear, indirectly forcing users to install additional malicious code on their devices. In the past, we have encountered fake antivirus products that warn about critical malware on the device. These programs are usually harmful themselves – they often display ads or collect data about the device or user.

Impersonation (Spoofing) - the impersonation technique is the same in the physical world. Cybercriminals contact company employees, posing as, for example, the CEO, and attempt to manipulate the victim into taking specific actions, such as approving fraudulent transactions. [16]
Use common technical terms. Do not try to create new English words.

2.2. Features of social engineering

Social engineering relies on weaknesses in the human psyche rather than gaps in technological solutions. It exploits people's trust, fear or inattention.

An overly urgent message that tries to force the recipient to act without thinking or a non-standard request for sensitive data should raise suspicions of an attack. Reputable companies never ask for passwords or personal information via email or phone. The most common signs of social engineering include:

Time pressure: All social engineering attacks are more successful if the victim believes it is necessary to make a quick decision.

Fear of missing out: The fear of missing out phenomenon is behind the success of social networking. However, it also becomes an effective manipulation tactic if we believe the victim's inaction (refusal to disclose personal information) will lead to personal loss.

The fallacy: Not all social engineering techniques are purely psychological. An attacker can use vulnerabilities in a website to redirect the victim to an unsafe site in the hope that they will enter personal or financial information.

Fake reviews: This does not apply to companies that pay for store app reviews to make their product more appealing. Fake reviews can also make a website or service more credible and encourage the victim to enter personal information.

Fake identity: This is an essential element of all phishing scams. Attackers present themselves as a trustworthy organization or individual to make the victim feel safe and provide sensitive information.

Incomplete information: To be more convincing, hackers often use public or readily available information to encourage the victim to divulge even more. For example, scammers with an address, phone number, and the last four digits of a credit card can pose as an online merchant. [17]

3. Consequences of social engineering

The main risk is that the human factor always plays a significant role in social engineering techniques. While organizations may invest much money in security, it will only ever be as strong as its weakest link – the employees. Indeed, their mistakes are much more difficult to predict and prevent.

For organisations, social engineering poses serious risks. Attackers can cause financial losses by convincing employees to transfer money into fake accounts, or they can obtain sensitive business information and data. It can cause not only the aforementioned financial losses but also a loss of credibility with clients and partners. Data breaches can result in serious legal consequences and penalties.

If they do occur, other serious risks follow depending on the objectives of the specific attacker. The most common consequences of social engineering:

- Unauthorised access to the internal infrastructure of the company,
- installation of malware on a company computer (how to identify and fix a compromised computer),
- unauthorised entry into the workplace by an attacker after being let in by a deceived employee,
- extortion of sensitive access, personal or payment information,
- gathering sensitive information to launch the subsequent phases of the attack,
- direct transfer of funds by the defrauded person.

From this, we can easily deduce that the consequences for individuals and organisations can be devastating. Examples include loss of control of corporate systems, infected computers, empty bank accounts, encryption of critical corporate data or its complete loss. [18]

3.1. Features of social engineering

Social engineering is an integral part of cybercrime, and according to the IC3 and Verizon's 2023 report, social engineering is a growing problem. Verizon's 2023 report indicates that 74 % of data leaks were due to human error, and up to 50 % of social engineering attacks are based on pretexting. FBI, in turn submits that for the year 2023, there were:

- 12,5 billion USD stolen in U.S. cyberspace
- 521 652 victims were attacked in the U.S. (an additional 315 880 victims were uncovered across the 20 other countries examined).
- The most significant financial losses of up to 3,4 billion USD occurred among seniors over 60 years. To put this in perspective, the under-30 years population only lost about 401 million USD, nearly seven times the amount lost by the senior population. [12]

The 2022 State of the Nation's Cybersecurity Report from the National Cyber Security Council shows that social engineering is a pervasive and growing threat. The most common types of cyberattacks in 2022 included phishing, spear phishing, vishing, and phishing emails, all different social engineering techniques. The report also shows that attackers most often targeted the public, healthcare and private sectors.

The National Cyber Security Index, which measures the preparedness of different countries to prevent cyber threats and their ability to manage cyber incidents that have already occurred, is very positive for the Czech Republic, as we are currently the safest of all countries, measured a score of 98,33. We must still be vigilant and prepared for the real threat of social engineering. [19]

4. Social engineering as a problem in the organization

In today's digital age, where both the private and public spheres increasingly rely on information systems and technology, cybersecurity is becoming a vital issue for organisations of all sizes and in all lines of business.

In 2016, the European Union created a comprehensive document, NIS (Network Information Security), which aims to ensure a consistent and high level of security at the network and information systems level in EU member state organisations. Until now, national cybersecurity measures have varied considerably not only in form but also in practice. Only a few countries have had a legislative framework in this area, and not all have established top-level security groups such as CSIRTs/CERTs. The purpose of the Directive is to set out the basic requirements that all EU Member States must meet. [20]

Many articles [21, 22] can be read about the term information security management system, but all describe organisations directly affected by the Directive and the law. Thus, they only apply to address some smaller organisations that are not required to implement cybersecurity laws and information security management systems.

Figures have to be made in high quality, which is suitable for reproduction and print. Check photos and colour prints on the quality of black white reproduction. Text and explanations on the figures must be readable. The figures have to be placed as close as possible to the first reference to them in the paper.

5. Proposal of new measures

This paper proposes a methodology for managing a small organization in the private sector that will specify the basic principles of information security focused on social engineering. To do this, it is necessary to determine the importance organizations place on information security and whether they are adequately secured against attacks.

5.1. Research

Ten organisations with up to 50 employees, mainly in the private sector, were contacted. Semi-structured interviews were conducted with employees and employers. The interview lasted between an hour and an hour and a half, depending on the fluency of the interview and asking follow-up questions.

The questions covered the following topics:

For employers:

- Is there cyber security training? If yes, how?
- Are employees allowed to use a private phone during work hours?
- Does each employee have unique PC login credentials? If so, are there specific password requirements? If yes, what are they?
- Do employees use work email for personal purposes as well?
- Are there company guidelines that specify rules of conduct for employees regarding social engineering threats and prevention of attacks?
- What types of documents do you attach to employee contracts?
- Do employees take company PCs home? If so, are there set rules for use outside of work? If so, what are they?

For employees:

- Have you been trained in social engineering (cybersecurity, information security)? If yes, how?
- Do you use a mobile phone during working hours?
- Do you have a unique password on your company PC, and have you never revealed the password to another person?
- Have you established company guidelines, for example, by collective bargaining agreement, which define your rules of conduct in information security?
- Do you take your company PC home? If so, do you have particular security rules, for example, in case of loss?
- Do you visit private email, social networking sites, etc., during working hours on a private phone?

The questions were asked individually or with follow-up questions as the conversation developed. The use of dynamic questions was minimal. Questions related to the main topic - social engineering - were asked first. The interviews concluded with a comparison of the state of the companies with the ideal state. The perfect state is defined as a state where the company has done everything possible to protect itself against social engineering attacks and sociotechnical manipulation techniques.

5.2. Evaluation

Organisations are very similar in terms of their approach to the issue. The data collected was very consistent; therefore, it was not difficult to isolate and describe the general characteristics of the group.

Small companies have measures related to phishing emails; they take these as the biggest threat. Therefore, they mainly train employees to use PCs and apply basic restrictions on selected websites. Each employee has PC login credentials, but this is now the minimum-security standard. Some employees also own a company phone, but these devices do not have passwords or anti-virus systems. In general, small businesses do not have company guidelines that specify rules of conduct for employees regarding social engineering threats. Nor are such regulations used to regulate attack prevention. If an attack does occur, measures are created after the fact, i.e., when the attack happens.

If the problem doesn't occur, it doesn't solve it, and they do not focus on prevention. They perceive the threats associated with social engineering as not very real. They have an advantage regarding the number of employees; their numbers are low, reducing the chances of personally carrying out a possible attack.

6. Information security methodology

This chapter aims to establish a basic guideline to consider during employee training. Another goal should be to create awareness among employees that they are the critical element of the organization's defence mechanism.

6.1. Information security guidelines for employees

The aim is to define precise rules and guidelines for employees to follow. The definitions must be accurate, and the organisation's people must understand their importance and respect them so that they become their business.

In particular, the guidelines should cover the following areas: computer use, information handling, access data and passwords, internet and data storage, use of email clients, social networking, rules on telephone and mobile phone use, and document disposal.

6.2. Training and education

Every employee should receive basic security training. Initial training for new employees should be mandatory and access to computer technology should only be allowed after completion of this course. The training should be short so that it captures employees' attention, and they remember the important points. We should refrain from training sessions lasting several hours to a full day, where people are demotivated, and their attention span is zero. The emphasis should be on situations and cases that can harm the company, understanding their principle and providing specific instructions on corporate information security. The training programme should include the following points:

- the use of socio-techniques
- recognition of sociotechnical issues,
- procedures in case of suspicious requests for information,
- highlighting the need to authenticate persons requesting information,
- trusting others without adequate verification,
- handling sensitive information.

6.3. Audit

The employer should conduct regular checks to ensure employees adhere to the contractual security rules. Audits should be performed regularly and processed by an independent external provider.

6.4. Penetration testing

The penetration test mimics a hacker attack on network infrastructure or servers from an external or internal network. Penetration can also be conducted using the social engineering method, where the hacker uses non-technical tools such as exploiting people's trust and weaknesses. Attacks can help to obtain sensitive information or cause unavailability of services and unauthorised access to data.

7. Discussion

This paper has examined previous efforts to address the problem of social engineering, but none of them addresses the environment of small organisations in the private sector. While previous works have examined social engineering in terms of its techniques and prevention in general, social networks, cognitive and machine learning techniques, or the implementation of an information security management system in directly covered organisations, they have not addressed the problem of the impact of social engineering on small organisations.

The findings of the brief research indicate that employees in organisations have only minimal security measures in place, perceive threats associated with social engineering as not very real, and have almost no corporate cybersecurity policy and rules of conduct regarding social engineering threats. Such rules are not even used to regulate the prevention of these attacks.

The main objective of this section is to critically evaluate the results of our work in a broader context.

The employer must always provide a suitable environment for the employee by ensuring that all programs are up-to-date and that all devices have secure antivirus software. Many times, companies are attacked simply because of outdated software versions. These obsolete systems have vulnerabilities that even not-so-experienced hackers can find and get into the employee's PC.

The advantage of having an in-house security solution provider is funding. For example, the task is assigned to an employee or performed by a department with expertise. Efficiency thus varies from case to case. Company connections often influence employees, and so the results can be manipulated.

An external security investigator provides an independent view of the issue. The resolvers have a practical methodology and more experience with these types of audits. Therefore, they have no ties to the environment and staff and are not biased in their assessment. The disadvantages are the cost of acquiring an external firm, the disclosure of sensitive information, and the need to select an external firm.

Employee training methods are workable but need to be sufficiently updated and to reflect the dynamic environment in which most organisations find themselves today. Employees are not trained against all hazards. This can be done, for example, by creating an awareness campaign in which more emails are sent out to employees, explaining how to recognise a possible attack and what to do if an attack is suspected.

The issue of cyber security, in general, can be complicated for senior management in organisations to grasp due to traditional role divisions, with management focusing only on strategic management, difficult-to-explain (business) benefits, lack of understanding of cyber threats, vulnerabilities and measures, and failure to recognise the long-term benefits in protecting data and maintaining the company's reputation.

The contribution of the proposed solution in this article is mainly the complexity and the level of measures leading to a secure cyber environment in organisations that do not address this issue. The benefit is not only to increase employee (user) awareness of potential threats in cyberspace, but it is also primarily focused on social engineering, but also, to protect the entire organisation and mitigate the impact of threats on organisations.

Further research should focus on improving efficiency and reducing costs associated with security measures. It may also include artificial intelligence and machine learning tools to facilitate specific processes. Long-term studies should also be conducted to evaluate the lasting impact of training on user security behaviour. Future research should include developing incident response plans that can be easily adapted to different types of organisations and threats.

8. Conclusion

This article looked at the impact of social engineering on small organizations. In comparison with the available literature, it was found that the issue still needs to be addressed at this level. The aim was to propose specific security measures, methods, and tools to counter social engineering in the particular environment of small organizations and enhance their cyber security. The research revealed that most of the employees of organizations are entirely under-protected.

In the second part, specific security measures were proposed for managing small organizations, focusing on enhancing cybersecurity with a focus on social engineering. The discussion summarized the benefits of these solutions and the possible limitations they may pose and provide possible suggestions for future research.

9. Acknowledgments

This article was supported by grant project IGA/FAI/2023/002, „Protection of the population, soft targets and the information environment” solved in 2023-2024.

10. References

[1] Birthriya, S. K., Ahlawat, P. & Jain, A. K. (2024) ‘A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies’, Journal of Applied Security Research, pp. 1–49. doi: https://doi.org/10.1080/19361610.2024.2372986.

[2] Samad, A. (2024). Social Engineering in Cybersecurity: Prevention and Mitigation Strategies.

[3] Huseynov, F. & Ozdenizci Kose, B. (2022). Using machine learning algorithms to predict individuals’ tendency to be victim of social engineering attacks. Information Development, pp. 298-318. doi: https://doi.org/10.1177/02666669221116336.

[4] Burda, P., Luca Allodi & Zannone, N. (2023). Cognition in Social Engineering Empirical Research: a Systematic Literature Review. ACM Transactions on Computer-Human Interaction. doi: https://doi.org/10.1145/3635149.

[5] Ramakrishnan, S., Malini Mittal Bishnoi, Shanmugan Joghee, S Jijitha and Kumar, A. (2024). Social Engineering:Role of Teachers in Cohabitation of AI with Education. pp. 1-6. doi: https://doi.org/10.1109/iccr61006.2024.10532897.

[6] D. V. Grbic & I. Dujlovic (2023). Social engineering with ChatGPT, 2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina. pp. 1-5, doi: https://doi.org/10.1109/INFOTEH57020.2023.10094141.

[7] Sharma, V., Renu Saharan, Wilson, K., Sharma, D., Suresh Beniwal & Chander Parkash Dora (2022). Privacy and Security Challenges in the Era of the COVID-19 Pandemic. Advances in medical technologies and clinical practice book series, pp.287–308. doi: https://doi.org/10.4018/978-1-6684-5741-2.ch017.

[8] Salama, R. & Fadi Al-Turjman (2023). Cyber-Security Countermeasures and Vulnerabilities to Prevent Social-Engineering Attacks. CRC Press eBooks, pp.133–144. doi: https://doi.org/10.1201/9781003322887-7.

[9] Steinmetz, K.F. and Holt, T.J. (2022). Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations. Social Science Computer Review. doi: https://doi.org/10.1177/08944393221117501.

[10] Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution.

[11] Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing. ISSN 1123-1132.

[12] Farid, G., Warraich, N.F. & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science. doi: https://doi.org/10.1177/01655515231160026.

[13] Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review. doi: https://doi.org/10.1016/j.clsr.2023.105890.

[14] Božić, V. (2023) Enhancing Hospital Cybersecurity: Implementing the NIS2 Directive for Resilience and Compliance. Journal of Health Care Management. pp. 220-235.

[15] Chetioui, K., Bah, B., Alami, A.O. & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, [online] 198(1877-0509), pp.656–661. doi: https://doi.org/10.1016/j.procs.2021.12.302.

[16] Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. International Journal of Computer Applications, pp. 1-11. ISSN: 0975-8887

[17] Syafitri, W., Shukur, Z., Mokhtar, U.A., Sulaiman, R. & Ibrahim, M.A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. IEEE Access, pp. 39325-39343. doi: https://doi.org/10.1109/ACCESS.2022.3162594.

[18] Wang, Z., Zhu, H. and Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access, pp.11895–11910. doi: https://doi.org/10.1109/access.2021.3051633.

[19] Report on the state of cyber security of the Czech Republic for 2022, , Available: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

[20] Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A. & Janicke, H. (2020). A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. IEEE Xplore. doi: https://doi.org/10.1109/COMPSAC48688.2020.00-20.

[21] Onyshchenko, S., Yanko, A., Hlushko, A., & Sivitska, S. (2020). Increasing information protection in the information security management system of the enterprise. In International Conference Building Innovations. pp. 725-738. Cham: Springer International Publishing.

[22] Alzahrani, L. & Seth, K.P. (2021). The Impact of Organizational Practices on the Information Security Management Performance. Information, 12(10), p. 398. doi: https://doi.org/10.3390/info12100398.