Analysis and classification of chosen social engineering methods in cybersecurity[1]

Monika Olchowik

Institute of Teleinformatics and Cybersecurity, Faculty of Cybernetics, MUT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warsaw, Poland
monika.olchowik.pl@gmail.com

ABSTRACT: Cyberthreat landscape is everchanging and dynamically evolving. Tools, techniques and software are getting more and more intricate. In contrast social engineering methods have been used in various attacks long before computers have been created, yet they are as useful as before, even in cyberspace. Social engineering attacks are quite often successfully used by conmen and hackers, and as such are a constant part of cyberthreat landscape. In order to detect and prevent the usage of aforementioned techniques greater understanding and systematisation of the process is need. In this paper a classification of chosen social engineering methods has been proposed. The classification is based on Kevin Mitnick's Social Engineering Cycle. This classification allows for creation of attack patterns and could be used as a basis for a social engineering attack matrix. Moreover, the paper presents a collection of different methods used in each of the stages of the cycle, describes them and provides examples of their usage.

KEYWORDS: Social Engineering, Social Engineering Cycle, Social Engineering Methods, Social Engineering Methods Classification

1. Introduction

Digital revolution is happening even faster with each passing year. It influences not only how business is conducted, but it also changes all aspects of life. From communication to transportation, technology is ever-present and everchanging. As such the cybersecurity threat landscape is constantly evolving. With each passing year new vulnerabilities, methods and vectors of attacks are discovered and used. In response organizations develop new procedures, patch and upgrade their software. Finally, they constantly invest in even more

[1] Artykuł poświęcam pamięci mojego promotora dr. inż. Zbigniewa Suskiego

sophisticated systems for better detection and defence.

Yet no matter the technology used, there is one unchanging component – the technology is made for and used by people. This allows to exploit the oldest vulnerability, that is the human nature. Such attacks might be performed by social engineering. This process can be defined as "manipulating people, by deception, into giving out information, or performing an action [1]".

Even up to 34% of organizations consider careless/unaware employees as the biggest vulnerability [2]. Employee weakness is considered to be responsible for 20% of confirmed breaches by 2020 [3]. In order to minimise this risk, it is important to understand social engineering and its methods.

2. The Social Engineering Models

One of the most well-known social engineering models is Mitnick's Social Engineering Cycle. It consists of four stages: Research, Developing Rapport and Trust, Exploiting Trust, and Utilizing Information [4]. The cycle is shown on Figure 1.

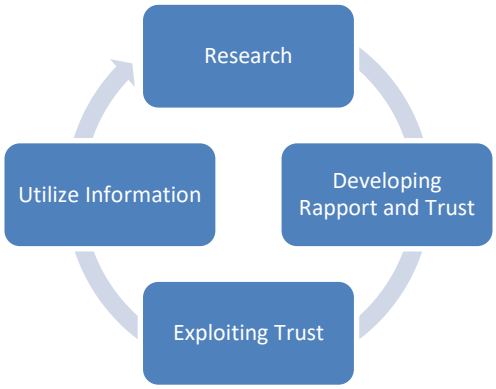

Figure 1. The Social Engineering Cycle

During the initial part called Research attacker tries to gather as much information as possible about a target. In this phase it is important to acquire data about the people, the company, but also about the targeted social group.

In the second phase the attacker uses the information gathered to develop the trust between himself and the victim. There are many approaches to this phase, all of them deeply rooted in psychology. [4] The attacker could assume position of authority over the victim or try to be friendly and approachable. It is also possible for this phase to take longer. The attacker can slowly introduce themselves into the surroundings of the victim. If performed successfully the

victim will recognize the attacker as the part of the chosen community, or the company. This phase creates the base of the success of a social engineering attack. The victim is more likely to be vulnerable to an attack if they believe the attacker.

The third step is the key of the social engineering attack. Its goal is to convince the victim to perform an action or to give out information. The attacker could simply ask the victim about the needed data or ask for help. However, in a process called the reverse sting the victim might be manipulated to request help from the attacker and by following the instructions of the attacker realising his current goal [4].

The fourth phase called Utilise Information is dependent on the attacker acquiring all the necessary information. In this case the goal of the attacker is achieved, and no more actions are necessary. Otherwise the attacker continues and performs the phase one again.

It is worth noting that there are other social engineering models. An example of this is the Social Engineering Attack Framework. It has been inspired by the Social Engineering Cycle [5].

The Social Engineering Attack Framework is divided into six phases: Attack Formation, Information Gathering, Preparation, Relationship Development, Relationship Exploit, and Debrief. Each of the phases consists of individual steps [5]. Individual steps of this model are shown on Figure 2. It is of note that "Goal Satisfaction" does not belong to any of the phases.

Individual steps of The Social Engineering Attack Framework (Figure 2) are coloured according to their phase: brown (Attack Formation), orange (Information Gathering), violet (Preparation), dark blue (Relationship Development), light blue (Relationship Exploit), green (Debrief), teal (not belonging to any phase).

It is possible to notice correlation between phases of those two models. The Research phase has been split into Attack Formation, Information Gathering and Preparation. Developing Rapport and Trust is a direct equivalent of Relationship Development. Exploiting Trust is covered by Relationship Exploit. Utilizing Information corresponds to two actions: Transition and Goal Satisfaction.

The difference in the two aforementioned models is the maintenance, which is not explicitly shown in the Social Engineering Cycle. However, it is possible that such actions are a part of the Exploiting Trust phase. In this action the attacker is trying to calm the victim and appease their emotional state. The goal of this step is to ensure that the victim does not feel as if they have been attacked [5] and thus do not perform any actions such as changing passwords or reporting the incident.

Due to the similarities between the models in this article methods will be classified by their role in accordance with the Social Engineering Cycle, as it is the most often used model to describe social engineering attacks.

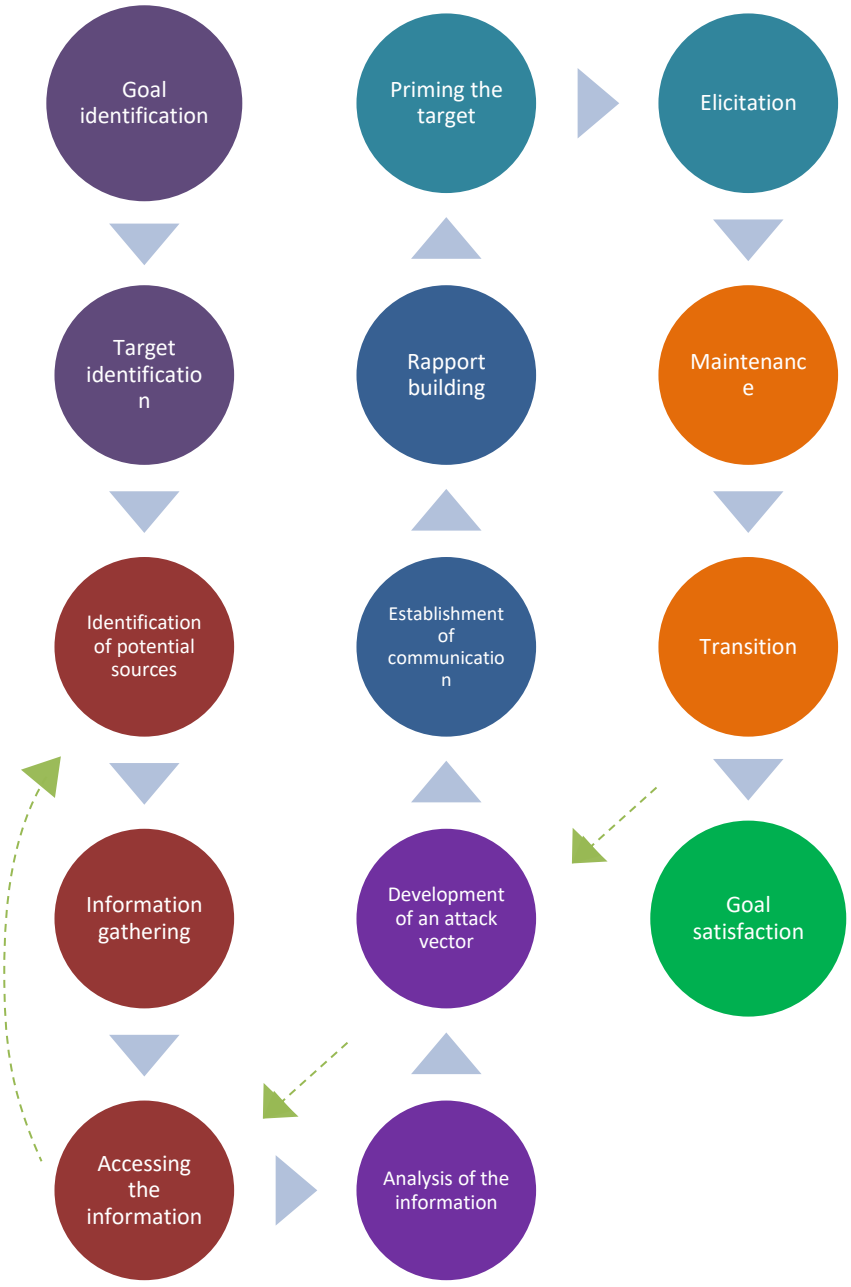

Figure 2. The Social Engineering Framework

3. Classification of methods based on the Social Engineering Cycle

3.1. Basis of the classification

Methods analysed in this paper have been chosen based on the prevalence of their usage and their applicability to various scenarios [1, 4, 8]. Thus, it is possible to attempt to classify these general-purpose methods based on the stage of the social engineering attack, in which they would be used. Each of the phases has a common goal and thus the basis of the proposed classification is the result achieved by the usage of a given method. However, the last phase of the cycle – Utilising Information is a notable exception as its goals are highly case specific and thus this phase has not been included as a part of the categorization.

The proposed classification of different sociotechnical methods introduces following categories:

- Research,
  - Passive information gathering,
  - Active information gathering,
- Developing Rapport,
- Trust and Exploiting trust.

Moreover, the methods used in the Research phase have been split in two categories in order to differentiate between the Passive and Active Information Gathering.

3.2. Research

During the research phase the goal of an attacker is to find as much information about his target as possible. The methods used in this phase can be categorized in analogous way as the scanning methods. The distinction between the methods is whether the target can learn or suspect that the information is being gathered.

3.2.1. Passive information gathering

Passive information gathering is centred on the idea of acquiring data without the victim being aware about it. As such open-source intelligence (OSINT) tools are used at this stage. The OSINT Framework [6] offers a collection of websites and tools used in such processes. Among the important

sources used during a reconnaissance are:

- search engines,
- company website,
- unsecured cloud storage,
- people databases,
- social networks and dating sites,
- tools for analysis of social networks,
- databases of leaks from online communicators,
- online registries and records,
- forums and blogs,
- files and their metadata.

Social media is a source especially rich in personal data. It is an ideal source of data for social engineers who would like to commit identity theft. Sources like Facebook, Instagram, Twitter or LinkedIn allow the attacker to learn about the mannerisms of a victim, important events from their life and other personal information [7]. All of this is willingly shared by the target. For example, knowing that an important executive in a company is on vacation on the other side of the world, a social engineer might safely assume the identity of a person representing the executive, e.g. a new assistant.

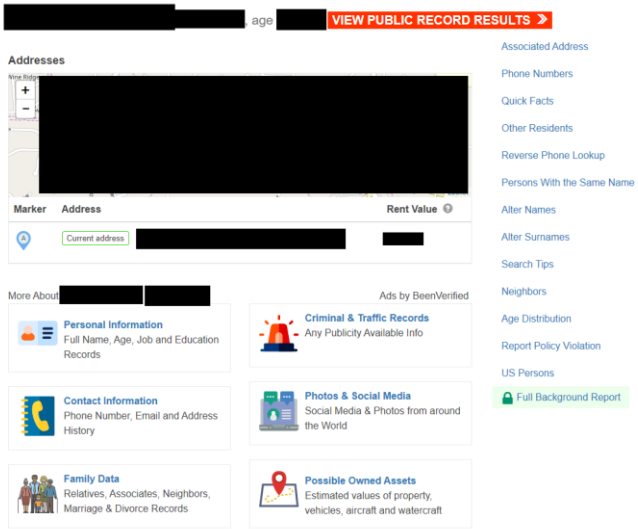

Figure 3. An example people database [9]

It is worth noting that people databases contain collections of personal information about many people. The knowledge of the person's name and surname is required and usually sufficient to use them. Additionally, some of them offer paid services. An example is shown on Figure 3. The attacker can also use highly specific tools such as Maltego. This tool helps with the information gathering, automating some of the actions required, and as such makes the process easier for the attacker [8].

3.2.2. Active information gathering

Active information gathering requires a degree of sophistication. An attacker risks that a victim will realize that they are being targeted and in turn will be on high alert. It is also possible that the attacker is exposing himself to a greater danger. Most notable example of active information gathering is people watching. If done incorrectly the attacker can be spotted and engaged by the victim. If done correctly however, one might be able to learn the occupation, personal details, habits and interests of the victim. A cybersecurity researcher by the name of Johnny Long was able to spot and determine the identity of a government agent at the airport [10]. During people watching it is possible to find a pattern in corporate attire and analyse badges. A good replica of a badge that supposedly stopped working might be enough for a security team to let a person inside of a building [10].

If a person watched by a social engineer uses a computer or a phone, the attacker might try shoulder surfing. This action is a simple act of watching the victim's device over their shoulder in order to gather important information that is being shown on the screen [10] or typed [11]. In some cases, it might be used to obtain the unsuspecting victim's password [4]. If two co-workers are chatting, eavesdropping might be an additional source of relevant information. The social engineer can learn through this e.g. their nicknames [12], or the projects the employee is participating in.

A similarly useful, simple and widely applicable technique is dumpster diving. An attacker might need to enter a property to engage in this activity. However, it can yield surprisingly useful results. It is possible to find personal information, corporate classified data, and financial information this way [10]. Vehicle watching is a different, supplementary action. It is based on looking at documents and receipts left unattended by a victim in their car.

A social engineer requires good observational skills. He not only needs to analyse badges and various documents, but also has to understand the inner workings of the company's building. The attacker should be aware of the layout of the building, its entries and exits, guards and other security staff, requirements for entry, and location of keypads. This information might be needed as shown in

the example of "Big Blue Pest Control" [8]. In this case social engineers were rejected by the security guards in the lobby. However, they remembered their names. Then they spotted the entry used by smokers, with lower security than the main entry. By pretending to be inspecting the building they successfully followed others into the building and then inside of it into an elevator. Later they claimed that they were referred by the security guard whose name they remembered. This was enough for them to enter the mailroom.

A different approach to active information gathering is the usage of all sorts of personality quizzes [11]. In this case the attacker disguises his true goal. Quite often a victim is enticed by the potential reward – a funny and memorable result. If the quiz is memorable enough the victim can share it with their friends. One of the most straightforward examples spotted in the wild was a questionnaire called "What does your password say about you?" [11]. It was created as a Facebook app, and contained questions about length of the password, and its complexity. However other quizzes e.g. testing compatibility between people or determining the job that would suit the user, can be used to determine the personality profile of the victim or provide enough information to impersonate a person. A live survey about Easter candy eating habits conducted by InfoSecurity Europe in 2006 shown that in 81% the researchers gathered enough of information to attempt an identity theft [12].

3.3. Developing Rapport and Trust

In this phase the Social Engineer engages the victim. If the communication is initiated in person, non-verbal communication is of high importance. As such, the verbal statements have to be corresponding with the message sent by micro and macroexpressions, voice, body language and gestures [13]. These elements are necessary for a successful elicitation to occur, that is to learn useful details about the target in the course of a seemingly normal and friendly conversation [13].

However, what is more surprising is that non-verbal communication might be applied even in a phishing attack. Emoticons might be used to convey openness and friendliness when trying to befriend the victim on social media platforms and dating sites. A different technique of non-verbal communication is called framing [13], that is using pictures, fonts, formatting etc. so that the victim thinks that the malicious content is part of a legitimate site or communication.

In general, common behaviours of social engineers in this phase include:

- assumption of authority,
- showing confidence,
- impersonation and pretexting:

    - name dropping,
    - insider knowledge including usage of the lingo,
    - usage of leaked data,
    - excuses;
- befriending the target:
    - flattery and validation,
    - flirting,
    - asking open ended questions,
    - quid pro quo;
- using sympathetic / guilt-inducing themes;
- elicitation;
- setting time constrains or creating artificial scarcity of items / information.

All the aforementioned behaviours might be spotted in both personal interactions, as well as communication over the Internet. The example of the latter are extortion campaigns. In the first five months of 2019, 300 million of such emails have been stopped by Symantec [14]. One of the most popular type is sextortion. The attacker informs the victim that he knows what their current password is. To establish trust attacker uses leaked data hoping that the target hasn't changed their password since then. Then the social engineer impersonates a hacker claiming that he hacked a website and infected the victim's computer, essentially gaining access to the victim's camera. Through that, he collected videos of illicit nature. As such the attacker assumes the position of authority and threatens the target that the video will be made public if they won't comply with the request. Campaigns following this simple scheme have been popular in 2019 [14][15] and 2020 [16]. Even though these attacks focus on intimidating the target, trust is still required. Otherwise, the victim would not believe in the possible negative consequences.

Sympathy might be dangerous as well. Assuming an identity of a desperate jobseeker that unfortunately spilled coffee over his resume is enough to elicit sympathetic feelings. Even more, it might be just enough to convince a receptionist to plug a USB stick with malicious files in and open them [17].

Curiosity and the need to reciprocate a favour might be also used against the target. Quid pro quo is a method in which the attacker offers something of perceived similar value. It can be as simple as providing feedback in a conversation e.g. information about the created persona [13] , or as complicated as offering free services in exchange for access to information [18].

A different way of establishing trust is elicitation, especially if combined with impersonation. A hacker group UG-NAZI has extracted credit card data thanks to tech support performing a password reset on database admin account.

The tech support tried to verify if the attacker on the phone is really the database admin, by asking different questions that the attacker knew the answers to. As such by sharing information, he gained trust of the victim [13].

3.4. Exploiting trust

Social engineer in this phase tries to convince the target to provide information or perform an action that will satisfy the current goal of the attacker. In this phase following methods are used:

- questions
- baits
- threats and negative consequences for not fulfilling requests
- reciprocation
- reverse sting
- distraction

Exploiting trust might be as simple as nicely asking the victim to perform an action, as it was shown in the example of a desperate jobseeker and a helpful receptionist. However, it isn't always enough. In extortions attacker bases his message on threats e.g. of publishing videos, or even infecting the victim's family with SARS-COV-2 [18].

On the other hand, a phishing campaign "2011 Recruitment Plan" targeting RSA shows the importance of baiting. The attack targeted a small group of employees. However, it was crafted well enough to look like a legitimate message. The email had a malicious Excel spreadsheet attached. For one of the targets the information about a possible recruitment plan was interesting enough for them to open it [7].

Similar effect has the usage of authority and giving orders or by reciprocation. Helping a person makes them more likely to comply with requests. Especially impressive effects can be created if it is used with a reverse sting approach. That is an attack in which the attacker manipulates the victim into turning to the attacker for help. One of the examples of this is a final stage of an attack on a new employee in a company. The attacker is aware of the name, surname and phone number of the target. Social engineer introduces himself as a member of information security team and offers to help the victim with all the intricacies of cybersecurity policies. After walking through some of them he asks about the complexity of the current password. As the new employee did not have a complex password the attacker proposed a change to a new password that they have created together [4]. The victim was grateful for help and provided each answer to the fullest capacity. However, they have unknowingly endangered the

company. Another example of this is a story of an unnamed social engineer mentioned by Kevin Mitnick. First, the attacker called a publicly known phone number for a sheriff's station. He introduced himself as a police officer and claimed that he tried calling a different number and implied that he must have made a mistake. In turn, the local police officer provided him with the correct phone number for internal use. Thus, the attacker has received the information he wanted even without asking for it [4].

A different approach is used if the goal is to make sure that a person does not perform an action. Then a distraction might be just enough. The Whurley's exploit shows that a story about a work colleague not returning the money and thus the attacker lacking money to take a date out might be distracting enough not only to bypass the security check, but also being given dating advice and money for lunch [19].

4. Summary

The social engineering cycle is an important tool that can be used to understand and describe social engineering attacks. Even a seemingly simple attack such as phishing might be described using a single cycle. Usually attacker has to perform research, impersonate a person or an organization in order to establish trust and legitimacy, and in the end ask, threaten or convey in any other way that the victim should open a malware-ridden attachment or a malicious link.

The simplicity of this model makes remembering and understanding it easy. Thus, it allows for an assignment of social engineering methods and techniques to the phases of the cycle. The end result of such classification could be used for creation of a social engineering attack matrix. A formalized attack matrix could allow for faster detection or easier analysis of the attack.

References

[1] MANN I., *Hacking the Human: Social Engineering Techniques and Security Countermeasures.* Aldershot: Gower, 2008.

[2] *Is cybersecurity about more than protection?* EY Global Information Security Survey 2018-19. EYGM Limited, 2018.

[3] *How does security evolve from bolted on to built-in? Bridging the relationship gap to build a business aligned security program.* EY Global Information Security Survey 2020. EYGM Limited, 2020.

[4] MITNICK K.D., SIMON W.L., The Art of Deception: Controlling the Human Elements of Security. Wiley Publishing, Indianapolis, 2002.

[5] MOUTON F., MALAN M.M., LEENEN L., VENTER H.S., *Social Engineering Attack Framework.* In: Information Security for South Africa, Conference Paper, South Africa, Johannesburg, 2014.

[6] *OSINT Framework*, 5.2.2020. [Online]. Available: https://osintframework.com/. [Accessed 16.4.2020].

[7] ALEXANDER M., *Methods for Understanding and Reducing Social Engineering Attacks.* The Sans Institute, 2016.

[8] HADNAGY C., *Social Engineering. The Science of Human Hacking*. Wiley, Indianopolis, 2018.

[9] *Public Records Encyclopedia*, ClusterMaps.com, [Online]. Available: https://clustrmaps.com/. [Accessed 16.4.2020].

[10] LONG J., *No Tech Hacking. A Guide to Social Engineering., Dumpster Diving and Shoulder Surfing*. Elsevier, Burlington, 2008.

[11] BROWER J., *Which Disney© Princess are YOU? (Web 2.0) Social Engineering on Social Networks*. The SANS Institute, 2010.

[12] MANJAK M., *Social Engineering Your Employees to Information Security*. SANS Institute, 2006.

[13] HADNAGY C., EKMAN P., *Unmasking the Social Engineer: The human element of security*. Wiley, Indianapolis, 2014.

[14] *Symantec Enterprise Blog*, Symantec, 30 July 2019. [Online]. Available: https://symantec-blogs.broadcom.com/blogs/threat-intelligence/email-extortion-scams. [Accessed 16.04.2020].

[15] *Naked Security, Sophos*. 17.12.2019. [Online]. Available: https://nakedsecurity.sophos.com/2019/12/17/dont-fall-for-this-porn-scam-even-if-your-passwords-in-the-subject/. [Accessed 17.4.2020].

[16] ABRAMS L., *Bleeping Computer, Bleeping Computer*, 9.4.2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/large-email-extortion-campaign-underway-dont-panic/. [Accessed 17.4.2020].

[17] HADNAGY C., *Social Engineering: The Art of Human Hacking*, Wiley, Indianapolis, 2011.

[18] *Naked Security, Sophos*. 19.3.2020. [Online]. Available: https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/. [Accessed 17.4.2020].

[19] SIMON W.L., MITNICK K.D., *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Wiley, Indianapolis, 2005.

Analiza i klasyfikacja wybranych metod socjotechnicznych stosowanych w cyberbezpieczeństwie

STRESZCZENIE: Cyberbezpieczeństwo jest dziedziną dynamicznie się zmieniającą. Narzędzia, techniki, oprogramowanie są ciągle rozwijane i stają się coraz bardziej złożone. W przeciwieństwie do nich metody socjotechniczne używane były od wielu lat i nadal nie straciły na swojej aktualności, nawet gdy wykorzystywane są w cyberprzestrzeni. Ataki socjotechniczne są często przeprowadzane z suckcesem przez oszustów oraz hackerów. Niezmiennie pozostają one zagrożeniem. W celu wykrycia i przeciwdziałania takim technikom konieczne jest zrozumienie i usystematyzowanie procesu ich wykorzystania. Niniejszy artykuł proponuje klasyfikację wybranych metod socjotechnicznych opartą o Cykl Socjologiczny Kevina Mitnicka. Klasyfikacja pozwala na tworzenie wzorców ataku oraz może zostać użyta w celu stworzenia matrycy ataków socjotechnicznych. Niniejszy artykuł przedstawia również zbiór różnych metod socjotechnicznych używanych w każdym z etapów cyklu, opisuje je oraz przykłady ich zastosowania.

SŁOWA KLUCZOWE: Socjotechnika, Cykl Socjotechniczny, Metody Socjotechniczne, Klasyfikacja metod socjotechnicznych

Received by the editorial staff on: 1.06.2021

Artykuł poświęcam pamięci mojego promotora dr inż. Zbigniewa Suskiego