REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL

unicuritiba

Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

CLASSIFICATION OF SOCIAL ENGINEERING METHODS AND TYPES OF SOCIAL ENGINEERING ATTACKS

CLASSIFICAÇÃO DOS MÉTODOS DE ENGENHARIA SOCIAL E TIPOS DE ATAQUES DE ENGENHARIA SOCIAL

DIANA BERSEI
North Caucasus Federal University – Russia
https://orcid.org/0000-0001-7423-5978
E-mail: di.bersej2012@yandex.ru

KIRILL DOLGOPOLOV
North Caucasus Federal University – Russia
https://orcid.org/0000-0002-1504-1089
E-mail: nadal06@mail.ru

OLGA AMVROSOVA
North Caucasus Federal University – Russia
https://orcid.org/0000-0001-5474-306X
E-mail: kilinkarov.77@mail.ru

TATYANA ZHUKOVA
North Caucasus Federal University – Russia
https://orcid.org/0000-0002-1011-8905
E-mail: tany_zhukova@mail.ru

LYUDMILA SHERBAKOVA
North Caucasus Federal University – Russia
https://orcid.org/0000-0002-2942-5630
E-mail: l.scherbakova@listl.ru

ABSTRACT

Background: Social engineering is an acute threat to modern enterprises. In large companies, dynamic information flows and changes in management processes increase the number of attack points for social engineers, which entails possible unwanted information outflows.

Objective: The study aims to analyze social engineering attacks, identify their complexity, and compare them with the types of attacks. The primary objective is to determine the key mechanisms to counter social engineering.

Methods: The paper analyzes the current body of scientific literature concerning the legal regulation of social engineering methods and the study of criminalized social engineering. The methodological foundation of the study is a combination of scientific research

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL

unicuritiba

Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

methods, including the abstract-logical approach, correlation analysis, and the comparative method.

Results: The existing research testifies to the dynamic spread and development of social engineering technologies, which necessitates the development of an effective system to counter social engineering attacks. The most promising approach appears to be the one based on the technical component and simultaneously involving the training of employees of enterprises and organizations in counteracting unauthorized access to information. This approach will reduce the risk of information leakage and strengthen the information security of modern companies.

Keywords: Social engineering; Social engineering methods; Social engineering attacks; Access; Protected objects.

RESUMO

Antecedentes: A engenharia social é uma ameaça aguda para as empresas modernas. Nas grandes empresas, os fluxos dinâmicos de informações e as mudanças nos processos de gestão aumentam o número de pontos de ataque para os engenheiros sociais, o que acarreta possíveis saídas indesejadas de informações.

Objetivo: O estudo visa analisar os ataques de engenharia social, identificar sua complexidade e compará-los com os tipos de ataques. O objetivo principal é determinar os principais mecanismos para combater a engenharia social.

Métodos: O artigo analisa o corpo atual da literatura científica sobre a regulamentação legal dos métodos de engenharia social e o estudo da engenharia social criminalizada. A fundamentação metodológica do estudo é uma combinação de métodos de pesquisa científica, incluindo a abordagem lógico-abstrata, a análise de correlação e o método comparativo.

Resultados: A pesquisa existente atesta a disseminação dinâmica e o desenvolvimento de tecnologias de engenharia social, o que exige o desenvolvimento de um sistema eficaz para combater ataques de engenharia social. A abordagem mais promissora parece ser aquela baseada na componente técnica e que envolve simultaneamente a formação dos colaboradores das empresas e organizações no combate ao acesso não autorizado à informação. Essa abordagem reduzirá o risco de vazamento de informações e fortalecerá a segurança da informação das empresas modernas.

Palavras-chave: Engenharia social; métodos de engenharia social; ataques de engenharia social; acesso; objetos protegidos.

1 INTRODUCTION

In any organization, the staff is its coordination center. Conducting information exchange both within and outside the company, employees can become a certain threat

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

to the company. The reason for this is that having access to various arrays of information, including confidential, personnel may become a target for attackers who seek to obtain such information. These data can be both internal company documents and customers' personal banking data.

Even though organizations typically use advanced technical security measures to minimize the possibility of unauthorized access to this information, they must consider the risk of their employees becoming victims of social engineering attacks. Human beings, due to their inherent emotional nature, frequently exhibit heightened susceptibility in comparison to machines.

The foremost peril pertaining to the disclosure of confidential information does not solely stem from technical security vulnerabilities, but rather from the individuals comprising the fundamental fabric of the organization. Adversaries have come to recognize that it is more expedient to achieve illegal penetration into an organization's information and communication technology infrastructure via an individual possessing the requisite data access, as opposed to employing an intermediary avenue.

2 METHODS

This study analyzes scientific literature concerning the legal regulation of social engineering methods, as well as publications concerning criminal social engineering. The methodological basis of the study is provided by a combination of scientific research methods, including the abstract-logical, correlation analysis, and comparative approach.

3 RESULTS AND DISCUSSION

There is a considerable body of research devoted to the main problems of social engineering.

One of the first mentions of social engineering dates back to 1987. J. Quann and P. Belford in their 1987 paper describe a technology that enables specialists “to exploit

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

the help desks and other related support services normally associated with computer systems" to access the necessary information (Quann & Belford, 1987, p. 155).

I.S. Winkler and B. Dealy (1995) suggest that the hacker community began to define social engineering as "the process of using social interactions to obtain information about a 'victim's' computer system" (p. 1).

K.D. Mitnick defines social engineering as using influence and persuasion to deceive people and take advantage of their misplaced trust to obtain insider information (Mitnick & Simon, 2002).

According to H. Kluepfel (1989), social engineering has at its core "trickery and deceit" (p. 15).

The following definitions of social engineering demonstrate that there is no universal widely accepted one. In different sources, the concept of social engineering is understood as:

– "a social/psychological process by which an individual can gain information from an individual about a targeted organization";

– "a type of attack against the human element during which the assailant induces the victim to release information or perform actions they should not";

– "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks";

– "the art of gaining access to secure objects by exploiting human psychology, rather than using hacking techniques";

- "an attack in which an attacker uses human interaction to obtain or compromise information about an organization or its computer system";

– "a process in which an attacker attempts to acquire information about your network and system by social means";

– "a deception technique utilized by hackers to derive information or data about a particular system or operation";

– "a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures";

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

– “a hacker’s manipulation of the human tendency to trust other people to obtain information that will allow unauthorized access to systems”;

– “the science of skilfully maneuvering human beings to take action in some aspect of their lives”

– “Social Engineering, in the context of information security, is understood to mean the art of manipulating people into performing actions or divulging confidential information”;

– “the act of manipulating a person or persons into performing some action” (Kluepfel, 1989, p. 18).

The subject area of social engineering is also defined differently by authors. In particular, it is described as:

– “using subversive tactics to elicit information from end users for ulterior motives” (Kluepfel, 1991, p. 182);

– “using influence and persuasion to deceive people and take advantage of their misplaced trust to obtain insider information” (Goldstein, 2009, p. 268);

– “the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks” (Voyager, 1994, p. 36).

These definitions outline the various ideas of what social engineering includes. Some of these definitions are intentionally focused on obtaining information from an organization. Some authors define social engineering as manipulating and convincing people to perform some action. Moreover, specific delineations are crafted concerning the acquisition of entry into computer systems and networks. The only element that unites all these definitions is the exploitation of a person to obtain some unauthorized information or to perform a series of actions for the aforementioned purposes.

Proceeding from the above, we can conclude that social engineering is a science of using social interaction as a means to convince an individual or organization that they need to fulfill a specific request on the part of an individual or organization.

Social engineers, same as computer hackers, use various tactics to foster the interlocutor’s trust in them. They often use a set of minor attacks that achieve their purpose

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

collectively. Social engineering relies on the use of the opponent's advantages. Information obtained from a phonebook can enable a phone call. The reception of information via a phone call can instigate subsequent phone calls. The social engineer collects and accumulates all possible information to subsequently organize a complex attack based on this information. The successful execution of an attack endeavor has the potential to yield substantial financial ramifications for the targeted company. A determined attacker demonstrates a willingness to obtain information by any means available.

The efficacy of social engineering can be attributed to the innate inclination of individuals to assist others and derive satisfaction from such interactions. Capitalizing on their expertise in social dynamics, social engineers adeptly cultivate trust, often assuming personas that resonate with their victims' established levels of trust.

Numerous motives underlie socially engineered attacks, as expounded in the hackers' manifesto, which elucidates the motivations driving hackers to infiltrate secure systems. Primary impetuses encompass the pursuit of knowledge, the quest for self-actualization, and a hunger for challenges.

Of heightened concern are social engineering attacks that strategically aim to compromise an organization's valuable assets. Examples include disgruntled former employees seeking retribution while pilfering corporate information.

The objectives pursued through social engineering attacks span from accessing personal information to intellectual property. Nonetheless, it is crucial to acknowledge that these ultimate goals necessitate the acquisition of numerous discrete fragments of information before their realization can be attained.

In the age of the mass spread of computer technology, more and more people can become potential victims of social engineers. The latter carry out targeting with skillfully crafted social engineering attacks.

To effectively counteract social engineering attacks, it is first necessary to know the basic methods of their implementation. Let us consider them in detail.

Phishing is a type of online fraud in which an intruder gains access to confidential user data – usernames and passwords. This scheme is quite popular. The goal of phishing is to illegally obtain confidential information. An example of this is an email sent to the

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

victim designed as a fake official letter – from a bank or a payment system – requiring them to verify certain information or perform certain actions.

Shoulder surfing involves physically looking at the victim's personal information over their shoulder. This technique is usually used in public places such as restaurants, airports, subways, etc.

Quid pro quo (“a favor for a favor”) is a type of attack involving an attacker contacting the company by corporate phone or email. Often the attacker introduces themselves as a technical support specialist who reports some technical problems at the employee's workplace and offers to help fix them.

A Trojan is a malicious software product that an attacker uses to collect, destroy, or modify information, disrupt the operation of a computer, or use a user's resources for personal benefit. Most often, the victim receives an email containing “interesting” content, an antivirus update, or other information that might attract them.

Reverse social engineering refers to a situation in which the victim unwittingly provides the attacker with the information they need. For example, customer service representatives often get user IDs, passwords, and other important personal information just because no one doubts their integrity.

Spam and pop-ups can generally be described as more annoying than unsafe by most end users, but they are extremely dangerous threats because they can prompt the user to click on various links, after which scammers gain access to their sensitive data.

F. Mohd Foozy et al. (2011) classify a social engineering attack as either human-based or technology-based. Human-based attacks use several techniques that are combined to make up an attack. In this way, attacks are most often carried out using several technical means, such as emails, software, and websites.

P. Tetri and J. Vuorinen (2013) pinpoint three basic social engineering tactics: persuasion, fabrication, and data mining.

Persuasion encompasses the act of compelling an individual to adhere to an unsuitable solicitation. Within the scholarly discourse, the authors delineate two salient attributes of persuasion: direct engagement and the active participation of the victim within the perpetrator's initiated course of action.

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Review*e-
ISSN: **2316-2880**

Fabrication entails employing various methods, including impersonation and the utilization of counterfeit identification documents, with the intention of misleading victims into perceiving the attacker as a different individual altogether.

Data mining denotes the systematic procedure of acquiring information from the designated target.

Below we provide a classification of social engineering attacks (Figure 1).

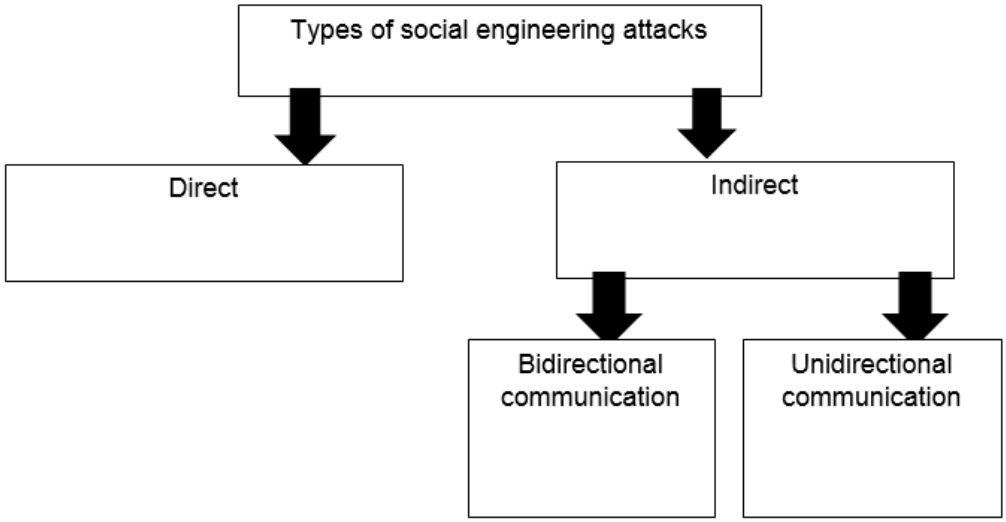

Figure 1. Types of social engineering attacks

A social engineering attack can be either direct or indirect. An indirect attack refers to an occurrence wherein communication with an intermediary medium serves as the means of perpetration. The third-party medium can be flash drives, brochures, or other media (e.g., web pages). This form of attack involves communication that takes place without direct engagement with the social engineer.

A direct attack entails an occurrence characterized by the involvement of two or more individuals engaged in distinct types of conversations. This conversation can be either unilateral or bilateral. Accordingly, there can be two modes of communication: unidirectional or bidirectional.

Bidirectional communication refers to two or more parties participating in a conversation. A popular example of this category of attack is a targeted attack, where a

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

social engineer influences a target to gain access to something that the target has access to.

Unidirectional communication denotes a form of conversation characterized by a singular flow, wherein the social engineer engages with the target without affording the target an avenue to provide feedback. Typically, this mode of communication is facilitated through various communication mediums, such as mass emails or SMS. An illustrative instance of an attack falling within this category is an email phishing attack, wherein an assailant directs a fraudulent email towards the target.

Now, let us consider the different types of communication carried out as part of a social engineering attack.

Bidirectional communication encompasses a mutually interactive discourse involving two individuals, wherein information flows in both directions. This form of communication accommodates the engagement of either an individual or a group of individuals as the social engineer. Similarly, the target of the attack may pertain to either an individual or an organization.

The common conduits employed for bidirectional communication encompass email exchanges, personal conversations, and phone discussions. The bidirectional communication medium presents an avenue where compliance principles, techniques, and objectives can synergistically converge.

An instance of a social engineering attack employing bidirectional communication arises when a social engineer endeavors to influence a call center agent into divulging confidential information pertaining to a specific customer. In this scenario, the attacker and the target exist as separate entities. The pretext technique is employed, as the social engineer assumes the guise of the customer whose information is being sought.

The compliance principle employed in this example is authoritative, as the individual masquerading as a social engineer assumes a persona suggesting authorized access to the information.

The objective of this attack is to illicitly obtain access to sensitive information belonging to the client.

Unidirectional communication bears resemblances to bidirectional communication, with the distinction lying in the unidirectional conversation flowing solely from the social

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

engineer to the target. Both the social engineer and the target can manifest as either individuals or entities. Unidirectional communication frequently leverages unidirectional media channels, such as one-way text messages, emails, or printed postal messages.

An example of a social engineering attack using unidirectional communication is emails. The technology used here is a phishing attack. For instance, the target places an online order at some online store and waits for the goods to be delivered. The phishing email is disguised as an email from the store's network and informs the target that there is a limited offer associated with the order. The target recognizes the connection between the email and their order and clicks on the malicious link. While the target is learning about the limited offer, the social engineer, by clicking on the compromised link, gains unauthorized access to the victim's computer.

Indirect communication, as a distinct form, encompasses the utilization of a third party as a medium of interaction. The social engineer and the target can encompass a diverse range, including individuals, groups of people, or entire organizations. In the realm of indirect communication, brochures, flash drives, and web pages frequently serve as conduits.

An exemplar of a social engineering attack employing indirect communication arises when a social engineer deliberately leaves an infected flash drive strategically positioned in a selected location, with the intention that it will be discovered and subsequently accessed by the target. After activating this device on the victim's computer, the social engineer also gains unauthorized access to the computer. The method employed in this attack is commonly referred to as "baiting" due to the deliberate placement of a physical object within the target's visual range. The efficacy of such an attack hinges upon the target's inherent curiosity. Additionally, the principle of social validation comes into play, as individuals are more inclined to comply when their actions align with perceived social norms. In the context of this attack, the target may feel a social obligation to locate the owner of the misplaced flash drive. Consequently, the target connects the flash drive to their computer, unknowingly activating a backdoor and inadvertently granting access to the social engineer.

Modern methods of countering social engineering attacks rely on security policies and training employees against social engineers.

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Review*e-
ISSN: **2316-2880**

Social engineering is a clear threat. M. Braverman (2006) reports that out of 384 respondents who confessed to being subjected to social engineering attacks, 15% of the cases were their own fault.

Security policy and staff training are the two primary approaches to preventing social engineering attacks. A security policy alone would not be able to prevent information breaches. However, if it differentiates data by sensitivity levels, it can become a rather efficient tool against social engineering attacks.

Personnel training is currently the most influential factor in countering engineering attacks. Training programs encompass a range of approaches, varying from annual multi-day seminars to ongoing reinforcement through posters and mailings. The underlying objective is to equip employees with knowledge regarding the tactics employed by social engineers to execute attacks and manipulate trust. This knowledge empowers employees to detect and respond to such attacks promptly. Furthermore, staff members receive guidance on refraining from disclosing certain sensitive information over the telephone, such as passwords and identification numbers. However, a significant challenge arises as even experienced social engineers possess the capability to establish trust with nearly every employee. Consequently, it becomes unrealistic to place sole reliance on employees as the primary line of defense against social engineering attacks (Boshmaf et al., 2013; Kvedar et al., 2010; McDowell, 2013; Robila & Ragucci, 2006; Uschold & Gruninger, 2004).

Social engineering relies on strategies such as influence and persuasion to exploit victims, compelling them to violate security protocols and disclose highly confidential information.

Empirical surveys conducted over the past five years have consistently demonstrated that office workers, who ideally should be well-versed in the significance of security, exhibit a willingness to share personal and security credentials when enticed with appropriate incentives or rewards (Braverman, 2006). Accordingly, if even professionals are that vulnerable to social engineering attacks, then ordinary users are virtually unprotected against this threat.

R. Van Rees (2003) asserts that today's level of awareness of the capabilities of social engineers among users and businesses is insufficient to fight this rising threat. A

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

study conducted by Greening (Nohlberg, 2008) at the University of Sydney sought to expose students to social engineering. The results indicate that out of 338 students targeted by a simplified email with a false address, 138 sent back their identification data, thus providing confidential information to social engineers.

Yet some researchers argue that user training is useless (Abraham & Chengalur-Smith, 2010). Asserting that security is always a second priority for end users, scientists suggest that the key to better security is actually in the hands of application developers and that data reveal that well-thought-out training in security can be effective (Erbschloe, 2004).

Indeed, web-based learning, context-based learning, and embedded learning all increase the ability of users to accurately identify an attack. A group study by S.A. Robila and J.W. Ragucci (2006) involved a user discussion on the phishing threats and attributes that need to be considered when dealing with such a threat. Following a review of the knowledge of the panelists, it was found that users' awareness of the application of social engineering techniques had increased significantly (Boshmaf et al., 2011).

Therefore, as part of the training of company personnel to counter social engineering attacks, the following areas of activity can be proposed:

– providing educational material on a wide range of social engineering techniques;

– providing links to supporting materials such as news reports on social engineering trends and techniques;

– organizing interactive meetings to allow staff to test their own ability to recognize and defend themselves against social engineering attacks.

Organizations typically use advanced technical security measures to minimize the risk of unauthorized access, yet every organization has employees that are potentially vulnerable to social engineering attacks. As computing devices become more and more widespread, the audience of people who have access to them is also growing. This is why social engineers are becoming increasingly interested in these people, especially if they have access to information that social engineers seek.

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Social engineering is the science of using social interaction as a means of persuading an individual or organization to fulfill a specific request from an intruder, where either social interaction, persuasion, or inquiry is based on computer technology.

Social engineers obtain information using social engineering attacks. A social engineering attack can utilize either direct or indirect communication. Direct attacks are distinguished into those using bidirectional or unidirectional communication. The class of indirect attacks is further defined as attacks that employ intermediary objects to create a communication platform.

4 CONCLUSION

Social engineering attacks have become so sophisticated that they can be compared in the degree of infiltration to technical types of attacks. However, in a social engineering attack, the weakest link is people, and with proper training, they can effectively resist social engineers.

The key mechanism for combating social engineering should be educating users to raise their awareness of deceptive techniques and ways to detect them, as well as improving the technical means of information security.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society 32(3), 183-196. http://dx.doi.org/10.1016/j.techsoc.2010.07.001

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). The socialbot network: When bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC 2011 (pp. 93-102). New York: ACM. http://dx.doi.org/10.1145/2076732.2076746

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2013). Design and analysis of a social botnet. Computer Networks, 57(2), 556-578. http://dx.doi.org/10.1016/j.comnet.2012.06.006

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Braverman, M. (2006). Behavioural modelling of social engineering-based malicious software. In Proceedings of the Virus Bulletin Conference, October 11-13, 2006, Montreal, Canada (pp. 15-22). Virus Bulletin Ltd.

Erbschloe, M. (2004). Trojans, worms, and spyware: A computer security professional's guide to malicious code. Amsterdam; Boston: Elsevier Butterworth Heinemann.

Goldstein, E. (2009). The best of 2600, collector's edition: A hacker odyssey. Indianapolis: Wiley Publishing, Inc.

Kluepfel, H. (1989). Foiling the wiley hacker: More than analysis and containment. In Proceedings of the 1989 International Carnahan Conference on Security Technology, October 3-5, 1989, Zurich, Switzerland (pp. 15-21). New York: IEEE. https://doi.org/10.1109/CCST.1989.751947

Kluepfel, H. (1991). In search of the cuckoo's nest [computer security]. In Proceedings of the 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, October 1-3, 1991, Taipei, Taiwan (pp. 181-191). New York: IEEE. https://doi.org/10.1109/CCST.1991.202213

Kvedar, D., Nettis, M., & Fulton, S.P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. Journal of Computing Sciences in Colleges, 26(2), 80-87.

McDowell, M. (2013). Cyber security tip st04-0141. Avoiding social engineering and phishing attacks. Technical report. United States Computer Emergency Readiness Team. Retrieved from http://gauss.ececs.uc.edu/Courses/c6056/pdf/social-engineering-Avoid-Phishing-Attacks-US-CERT.pdf

Mitnick, K.D., & Simon, W.L. (2002). The art of deception: Controlling the human element of security. Indianapolis: Wiley Publishing.

Mohd Foozy, F., Ahmad, R., Abdollah, M.F., Yusof, R., & Mas'ud, M. (2011). Generic taxonomy of social engineering attack. In Malaysian Technical Universities International Conference on Engineering & Technology (MUiCET 2011), November 13-15, 2011, UTHM, Batu Pahat, Johor, Malaysia (pp. 1-7). http://eprints.utem.edu.my/id/eprint/191

Nohlberg, M. (2008). Securing information assets: Understanding, measuring and protecting against social engineering attacks: PhD thesis, Stockholm University, Stockholm.

Quann, J., & Belford, P. (1987). The hack attack – Increasing computer system awareness of vulnerability threats. In 3rd Applying Technology to Systems: Aerospace Computer Security Conference, December 8-11, 1987, Orlando, FL, USA (pp. 155-157). American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.1987-3093

unicuritiba
Submetido em: 22/06/22
Aprovado em: 03/04/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Robila, S.A., & Ragucci, J.W. (2006). Don't be a phish: Steps in user education. In Proceedings of the 11th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education, ITiCSE 2006, June 26-28, 2006, Bologna, Italy (pp. 237-241) New York: Association for Computing Machinery. http://dx.doi.org/10.1145/1140124.1140187

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. Behaviour & Information Technology 32(10), 1014-1023. http://dx.doi.org/10.1080/0144929X.2013.763860

Uschold, M., & Gruninger, M. (2004). Ontologies and semantics for seamless connectivity. ACM SIGMOD Record, 33(4), 58-64. http://dx.doi.org/10.1145/1041410.1041420

Van Rees, R. (2003). Clarity in the usage of the terms ontology, taxonomy and classification. CIB Report, 284(432), 1-8.

Voyager. (1994). Janitor privileges. 2600: The Hacker Quarterly, 11(4), 36-36.

Winkler, I.S., & Dealy, B. (1995). Information security technology? Don't rely on it: A case study in social engineering. In Proceedings of the 5th Conference on USENIX UNIX Security Symposium, June 5-7, 1995, Salt Lake City, Utah, USA (Vol. 5, pp. 1-5). Berkeley: USENIX Association.