DecisionTech Review
Vol. 2, 2022, 1-6. DOI: 10.47909/dtr.03

REVIEW ARTICLE

Pro-Metrics

Methods for the prevention of computer crimes in organizations: A review

Junior Villa-Soto

Faculty of Systems Engineering and Informatics,
National University of San Martín – Tarapoto, Peru.

ABSTRACT
In the digital era, cybercrimes such as virus attacks, online fraud, and unauthorized use of personal data have become prevalent, significantly impacting individuals and organizations worldwide. The paper delves into various cybercriminal techniques, highlighting the role of human manipulation and the importance of educating potential victims. Through a systematic review of the literature, the study assesses the effectiveness of existing prevention strategies, including educational programs, health campaigns, and technological solutions. It categorizes research findings into several methods and models for mitigating computer crimes, offering insights into the challenges and effectiveness of these approaches. The review concludes by identifying key areas for further research and recommending multi-faceted approaches for combating cyber threats. This comprehensive analysis aims to guide information security professionals and policymakers in developing more robust defenses against the ever-evolving landscape of cybercrime.

Keywords: computer crimes; systematic review; computer security.

1. INTRODUCTION

According to Brands & van Doorn (2022), computer crimes occur in a digital environment where unauthorized access to private information is involved in illegally using the stolen information. The most common forms of cybercrime are virus attacks, online fraud, phishing, social engineering, and unauthorized use of personal data, and they usually target different strata of society (Milani *et al.,* 2022); This is also mentioned (Suryan & Sreeya, 2019) that, from their perspective, cybercrime involves a computer and a community.

Cybercriminals' most commonly used attack methods include phishing, social engineering attacks on online communities or social networks, automated social engineering, and semantic attacks. These attacks take place through phone calls, emails, and face-to-face interactions. For example, (Syed, 2019), in their human manipulation study, found that criminals used social engineering and phishing attacks to manipulate or psychologically trick employees into making security errors and handing over sensitive information.

It should be noted that successful cybercrime attacks mainly depend on the degree of manipulation or deception of the target

Received: 14-12-2021. **Accepted:** 02-03-2022. **Published:** 10-03-2022

How to cite: Villa-Soto, J. (2022). Methods for the prevention of computer crimes in organizations: A review. *DecisionTech Review, 2,* 1-6. https://doi.org/10.47909/dtr.03

into revealing personal information. For this reason (Junger *et al.,* 2017) point out that vulnerability to cybercrime attacks, mostly phishing and social engineering, is because victims tend to trust and quickly reveal personal and sensitive information. Thus, in their review, Lallie *et al.,* (2021) describe cybercrime using the crime triangle, where they specify that for cybercrime to occur, three elements must be present: a victim, a motive, and an opportunity. In that same perspective, the severity and increase in these crimes are mainly due to the COVID-19 pandemic (Naidoo, 2020), which created new opportunities for cybercriminals. Furthermore (Rameem Zahra *et al.,* 2021) mention that the pandemic has caused mass migration to digital platforms, a radical change that leaves people vulnerable to cybercrime.

On the other hand, research on human behavior in the face of these computer crimes proposed a framework focused solely on the user (Albladi & Weir, 2018), in which the socio-psychological, perceptual, and socio-emotional perspectives are considered, which are the factors higher risk that affect user vulnerabilities. In this approach, the same authors (Albladi & Weir, 2020a) propose the prediction of an individual's vulnerability based on three angles: people's behavior, perception, and emotions.

The present review, then, has the purpose of analyzing the importance of computer crime prevention methods in society through a systematic bibliographic review, in which valuable information and relevant results are collected, at the same time recommending ways to prevent cybercrime attacks from being applied at the organizational level and the individual level.

2. MATERIAL AND METHOD

Hatfield (2018) states that educating and training potential victims is the best way to prevent cybercrime. Therefore, victims must have sufficient knowledge to protect themselves from cybercrime attacks. From here, the importance of knowing prevention methods and even predicting future computer crimes, both social engineering and phishing, arises. We ask ourselves: What are the most effective methods for preventing computer crimes?

Search criteria, article selection, and article evaluation define the literature review process. This systematic literature review searched for articles using three digital databases, used search strings to collect multiple articles, and selected relevant articles based on year, article type, and title, focusing on articles related to social engineering and phishing. The databases used for this research are Scopus, IEEE, and ScienceDirect.

3. RESULTS AND DISCUSSION

Computer crimes, mostly social engineering and phishing, have become very common in recent years. However, few researchers have reviewed the prevention of these computer crimes. At the same time, the lack of interest in prevention causes great economic losses in institutions and at the individual level.

On the other hand, Yasin *et al.,* (2019) consider social engineering in two categories: the type of attack and the persuasion technique used. Likewise, they also combine several theories to explain how social engineering attack activities are carried out. However, it did not provide information on how users should carry out prevention techniques against the types of attacks and persuasion techniques used by social engineering attacks.

Likewise, social engineering attacks have evolved into phone calls, emails, and face-to-face interactions. Social engineering attack methods include spoofing, social engineering attacks on an online community or social networks, automated social engineering, and semantic attacks. Various types of social engineering are developing along with the spread of information technology. Previous research on human manipulation has found that perpetrators psychologically manipulated or deceived employees, for example, using social engineering and phishing attacks, to commit security errors or hand over confidential information (Fatima *et al.,* 2019).

Cybercriminals send messages modified to make users believe that the messages received are legitimate and require users to follow the instructions or suggestions in the message. The most commonly used examples of phishing are email and website phishing. Some phishing uses malware, bots, and Trojans to gain more user access (Naidoo, 2020).

4. STUDY AND DESCRIPTION OF METHODS FOR THE PREVENTION OF COMPUTER CRIME

Social engineering and phishing can bypass all hardware or software to prevent general attacks. Social engineering is complex and challenging to stop, whether based on hardware or software technology. This is caused by social engineering attacks that target users using both hardware and software technology. Therefore, the device user must be involved to prevent social engineering and phishing attacks. The attacks are very diverse and often change depending on the use of the technique (see table 1).

Research	Method	Model	Evaluation	Computer crime
(Abe & Soltys, 2019)	Health campaigns	—	—	Social engineering
(Sánchez *et al.*, 2018)	Simulation	Formal	—	Social engineering
(Albladi & Weir, 2020b)	Questionnaire	User vulnerability	—	Social engineering
(Yasin *et al.*, 2019)	Interview	Social engineering Attack based game Analysis	Empirical	Social engineering
(Abe *et al.*, 2018)	Finite state machine	Mitigation and social prevention Facebook-based Phishing Engineering	Validation based on a realistic scenario	Phishing Social engineering
(Rastogi *et al.*, 2021)	Machine learning	Machine learning-based phishing website detection	Performing	Phishing
(Andryukhin, 2019)	Combine technical and social prevention techniques	—	—	Social engineering
(Kumar N *et al.*, 2019)	Machine Learning and recommendation	—	—	Phishing
(Singh C & Smt. Meenu, 2020)	Machine learning	Phishing attack detection	Performing	Phishing
(Algarni *et al.*, 2017)	Interview and questionnaire	Susceptibility to social engineering on social networking sites	—	Social engineering
(Athulya A A & Praveen K, 2020)	Blacklist method or whitelist method or search engine-based technique	Phishing strategies and helps the user practice phishing prevention	Precision and time	Phishing Social engineering
(Bhargava & Yablonovitch, 2015)	Controlled experiment	End-use awareness campaign to educate and train employees	—	Phishing Social engineering
(Albladi & Weir, 2018)	User-centered	User vulnerability	Expert reviews, reliability, one sample t-test	Phishing Social engineering
(Java S *et al.*, 2019)	Online tamper detection	—	—	Phishing Social engineering

Table 1. Social engineering prevention approach. Source: Syafitri *et al.*, (2022).

The research by Java *et al.,* (2019) presents the concept of social engineering and phishing attacks. It establishes that educating and training potential victims is the best way to prevent them. Consequently, victims must have sufficient knowledge to defend themselves against attacks. Deploying a health campaign is one of the strategies to prevent social engineering attacks. Identifying a social engineering attack as a semantic attack is challenging due to behavioral deception that technical defenses cannot detect (Abe & Soltys, 2019).

5. CONCLUSIONS

Previous research has established methods and frameworks for preventing social engineering and phishing attacks. Furthermore, cybercrime attacks remain unpredictable for unsuspected victims. Different cases and actors, especially for social media cases, can modify social engineering and phishing attack techniques.

Based on this systematic review of the literature, one investigation was found on the prevention protocol to configure the exchange of information in a social network, three investigations on user studies, three investigations on concepts of prevention of social engineering attacks, three research on engineering attack prevention model, one research on social engineering attack prevention method, four research on other methods.

There are three main areas of research in the approach to preventing cybercrime attacks: health campaigns to resist social engineering attacks, user vulnerability of social engineering victims, and protocols to protect information disclosure on social networks. The best forms of health campaigns depend on the audience reach and content of those campaigns. The campaign for both adults and teens also had different tactics. The campaign's good content also reduced the risk of social engineering attacks. The user vulnerability model for victims of social engineering could take some recommendations from knowledge of social engineering in the social network. This model was also used to test the user's vulnerability based on the risk assessment of the user's response. Testing this model was used to revoke privacy limits or to share confidential and private information on the social network.

According to this review, several works can support the prevention of cybercrime attacks. The reviews found can be used by information security professionals and experts to overcome social engineering and phishing attacks. They can carry out development based on a collaboration of various approaches such as protocols, methods, frameworks, models, and assessments to prevent cybercrime attacks.

Conflict of interest

The author declares that there is no conflict of interest.

Statement of data consent

The data generated during the development of this study has been included in the manuscript. ■

REFERENCES

Abe, N., Institute of Electrical and Electronics Engineers, & IEEE Computer Society. (2018). MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. *IEEE International Conference on Big Data,* 5040-5048.

Abe, N., & Soltys, M. (2019). Deploying health campaign strategies to defend against social engineering threats. *Procedia Computer Science, 159,* 824-831. https://doi.org/10.1016/j.procs.2019.09.241

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences, 8*(1). https://doi.org/10.1186/s13673-018-0128-7

Albladi, S. M., & Weir, G. R. S. (2020a). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity, 3*(1). https://doi.org/10.1186/s42400-020-00047-5

Albladi, S. M., & Weir, G. R. S. (2020b). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity, 3*(1). https://doi.org/10.1186/s42400-020-00047-5

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems, 26*(6), 661-687. https://doi.org/10.1057/s41303-017-0057-y

Andryukhin, A. A. (2019). Phishing Attacks and Preventions in Blockchain Based Projects. *Proceedings – 2019 International Conference on Engineering Technologies and Computer Science: Innovation and Application, EnT 2019,* 15-19. https://doi.org/10.1109/EnT.2019.00008

Athulya A A, & Praveen K. (2020). Towards the Detection of Phishing Attacks. *Proceedings of the Fourth International Conference on Trends in Electronics and Informatics.*

Bhargava, S., & Yablonovitch, E. (2015). Lowering HAMR near-field transducer temperature via inverse electromagnetic design. *IEEE Transactions on Magnetics, 51*(4). https://doi.org/10.1109/TMAG.2014.2355215

Brands, J., & van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior, 127.* https://doi.org/10.1016/j.chb.2021.107082

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security, 27*(6), 581-612. https://doi.org/10.3233/JCS-181253

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security, 73,* 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Java S, Linsha B F, Riaz S, Jeet K M, & Mushtaq A. (2019). Detection of Online Manipulation to Prevent Users Victimization. *Amity International Conference on Artificial Intelligence (AICAI).*

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66,* 75-87. https://doi.org/10.1016/j.chb.2016.09.012

Kumar N, Dabas P, & Komal. (2019). Detection and Prevention of Profile Cloning in Online Social Networks. *IEEE International Conference on Signal Processing.*

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security, 105.* https://doi.org/10.1016/j.cose.2021.102248

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to Cyber Victimization: Results from a Swiss Survey. *Deviant Behavior, 43*(2), 228-240. https://doi.org/10.1080/01639625.2020.1806453

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems, 29*(3), 306-321. https://doi.org/10.1080/0960085X.2020.1771222

Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A., & Wu, F. (2021). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal.* https://doi.org/10.1016/j.eij.2021.12.003

Rastogi, M., Chhetri, A., Singh, D. K., & Rajan V, G. (2021). Survey on Detection and Prevention of Phishing Websites using Machine Learning. *2021 International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021,* 78-82. https://doi.org/10.1109/ICACITE51222.2021.9404714

Sánchez, D., Domingo-Ferrer, J., & Martínez, S. (2018). Co-utile disclosure of private data in social networks. *Information Sciences, 441,* 50-65. https://doi.org/10.1016/j.ins.2018.02.010

Singh C, & Smt.Meenu. (2020). Phishing Website Detection Based on Machine Learning: A Survey. *International Conference on Advanced Computing and Communication Systems (ICACCS).*

Suryan, V. S. K., & Sreeya, B. (2019). Public opinion on cyber crime. *International Journal of Innovative Technology and Exploring Engineering, 8*(11), 3198-3200. https://doi.org/10.35940/ijitee.K2517.0981119

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access, 10,* 39325-39343. https://doi.org/10.1109/access.2022.3162594

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *Journal of Strategic Information Systems, 28*(3), 257-274. https://doi.org/10.1016/j.jsis.2018.12.001

Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy, 2*(4). https://doi.org/10.1002/spy2.73