


Chapter 9

Emerging Trends and Future Directions in Social Engineering Defense

Gopalji Varshneya

 <https://orcid.org/0009-0008-9511-3716>

Sharda University, India

Priyanka Tyagi

Sharda University, India

Rachit Kumar

Sharda University, India

Nishant Dublish

IMS Unison University, India

ABSTRACT

In today's quickly changing digital society makes social engineering attacks a much bigger concern, it will create significant challenges to organizations as well as individuals. The chapter explores social engineering threats and strategies for mitigation. Beginning with an introduction to social engineering attacks, it highlights its critical aspects of organizations and individuals from manipulation. Historical viewpoints give insight into the evolution of social engineering attacks, providing us clues to understand current threats. The chapter explains the different tactics used by cybercriminals today and predicts future trends in social engineering. It also discusses technological advancements and tools for detection and prevention of

DOI: 10.4018/979-8-3693-6665-3.ch009

these types of attacks, supported by real-world case studies. Ethical and legal view also critically analyzed to maintain integrity in defense efforts. Lastly, the chapter concluded with the need for proactive defense strategies to effectively address emerging threats in social engineering.

INTRODUCTION:

Human unawareness to technological advancement and their loopholes is often considered the weakest link in cybersecurity, yet educational efforts tend to prioritize technical aspects over addressing human vulnerabilities (Kaushalya et al., 2018). Social engineering exploits this vulnerability, cybercriminals are using persuasion and manipulation to extract private information from targets. Effective defense against such attacks necessitates prioritizing information security awareness and offering comprehensive training programs to address human vulnerabilities (Ghafir et al., 2016). Additionally, developers should design user interfaces in a manner that makes small changes readily noticeable to users. These programs should educate employees about social engineering threats and tactics, equipping them with strategies to defend against such attacks. By implementing a multi-layered defense approach, organizations can mitigate security risks and protect their systems and data (Mughal et al., 2018). This chapter focuses on social engineering defense, covering awareness-raising, training, and the deployment of security measures to combat this pervasive threat in the digital age (Wang et al., 2020).

Hackers and malicious actors have leveraged various techniques, such as phishing emails, pretexting, baiting, tailgating etc. to manipulate targets and gain unauthorized access to sensitive information or systems (Okoli et al., 2024). The growing reliance on social media and online networking has provided evil-doers with vast resources for gathering personal details and crafting convincing narratives to carry out successful social engineering attacks (Burda et al., 2024).

One of the key aspects of social engineering within the context of information security is its reliance on psychological manipulation to bypass technical understanding of human psychology and social interactions, malicious actors can create compelling scenarios that trick the individual. Cybercriminals often exploit cognitive biases, emotional triggers, and social norms to influence target behavior and extract valuable data (Papatsaroucha et al. 2021). To combat the threat of social engineering effectively, organizations must adopt a multifaceted approach that combines technical controls with comprehensive training and awareness programs. Employee education plays a critical role in mitigating the risks associated with social engineering by empowering individuals to recognize potential threats (Aldawood & Skinner, 2018), verify the authenticity of requests, and respond appropriately

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/emerging-trends-and-future-directions-in-social-engineering-defense/366070

Related Content

Exploring the Relationships Among Gratifications-Sought, Social Media Usage, and Social Support Among Chinese Temporary Migrants: A Uses and Gratifications 2.0 Perspective

Yuan Wang (2021). *International Journal of Cyber Behavior, Psychology and Learning* (pp. 15-27).

www.irma-international.org/article/exploring-the-relationships-among-gratifications-sought-social-media-usage-and-social-support-among-chinese-temporary-migrants/283105

MobileSens: A Ubiquitous Psychological Laboratory based on Mobile Device

Ang Li, He Li, Rui Guo and Tingshao Zhu (2013). *International Journal of Cyber Behavior, Psychology and Learning* (pp. 47-55).

www.irma-international.org/article/mobilesens-ubiquitous-psychological-laboratory-based/78281

Perceived Usefulness of Emoticons, Emojis, and Stickers in Text Messaging: Effect of gender and Text-Messaging Dependency

Shogo Kato, Yuuki Kato and Yasuyuki Ozawa (2018). *International Journal of Cyber Behavior, Psychology and Learning* (pp. 9-23).

www.irma-international.org/article/perceived-usefulness-of-emoticons-emojis-and-stickers-in-text-messaging/222775

Evaluation of South African Universities' Web Portal Interfaces using a Triangulation of Ubiquitous Computing Evaluation Areas and Technology Acceptance Model

Vathiswa M. Booie and George E.M. Ditsa (2014). *User Behavior in Ubiquitous Online Environments* (pp. 150-172).

www.irma-international.org/chapter/evaluation-of-south-african-universities-web-portal-interfaces-using-a-triangulation-of-ubiquitous-computing-evaluation-areas-and-technology-acceptance-model/81173

Gratification, Loneliness, Leisure Boredom, and Self-Esteem as Predictors of SNS-Game Addiction and Usage Pattern Among Chinese College Students

Selina Xingyuan Zhou and Louis Leung (2012). *International Journal of Cyber Behavior, Psychology and Learning* (pp. 34-48).

www.irma-international.org/article/gratification-loneliness-leisure-boredom-self/75170