Chapter 6
Empowering Cyber Resilience:
Effective Strategies for Combating Social Engineering Threats

Ajay Pratap
Amity University, Lucknow, India

Gauri Rastogi
Amity University, Lucknow, India

ABSTRACT

Social engineering remains an enduring and emerging threat in cybersecurity. This chapter delves into the fluid landscape of social engineering threats, examining the strategies employed by cyber criminals and providing valuable perspectives on the current defence mechanisms that organizations and individuals can utilize for the efficient reduction of these vulnerabilities. The development of social engineering threats is propelled by a profound grasp of human psychology, coupled with the growing dependence on digital communication and information-sharing channels. This paper underscores the importance of collaboration among individuals, organizations, and security experts in the continuous effort to combat social engineering. It highlights the significance of staying informed about emerging threats and continuously improving defensive strategies to confront the constantly evolving landscape of social engineering attacks. This article introduces a comprehensive framework designed to address these challenges and shape the future of cybersecurity.

DOI: 10.4018/979-8-3693-6665-3.ch006

Copyright © 2025, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

1. INTRODUCTION

In recent years, there has been a notable rise in the importance of capability and resilience across various business domains. This shift is driven by a growing recognition of environmental and social impacts, prompting businesses to integrate these principles into their operations to meet consumer expectations and ensure long-term sustainability. Consumer behavior reflects this trend, with research from Nielsen indicating that approximately 66% of consumers worldwide are willing to pay a premium for products and services that demonstrate commitment to environmental and societal concerns. This signifies a shift towards products that not only offer quality but also have positive impacts on the environment and society.

Similarly, perceptions of resilience have evolved, with the World Economic Forum identifying it as one of the top five risk trends for 2022. This highlights the importance for businesses to not only address daily challenges but also possess the capability to adapt and endure in the face of rapid and unforeseen changes within the global landscape. The emphasis on capability and resilience is not fleeting; rather, it has become a fundamental aspect of successful business strategies. Businesses that can effectively integrate these elements into their operations stand to gain favor with consumers, navigate complex challenges, and sustain long-term growth in an ever-changing world. In today's digital world, the cybersecurity landscape is constantly evolving, posing a complex and ever-changing challenge. Among the most concerning threats faced by individuals and organizations is social engineering. Social engineering exploits human psychology, manipulating individuals into divulging sensitive information. This paper aims to explore the evolving landscape of social engineering threats and examine the modern defenses developed to combat them. The digital era has opened up unprecedented opportunities for communication, cooperation, and information exchange.

As social engineering attacks persist in affecting individuals and organizations, there are frequently legal and regulatory consequences as shown in Figure 1. A comprehensive understanding of the evolving landscape is instrumental in enabling policymakers and legal authorities to formulate suitable frameworks for addressing and preventing social engineering attacks. This, in turn, contributes to fostering a more secure digital environment. To sum up, ongoing research on social engineering is indispensable for proactively addressing the dynamic nature of cyber threats. In summary, researching social engineering is crucial due to its dynamic nature, human involvement, the expanding digital landscape, and the potentially devastating consequences of successful attacks. Staying ahead of social engineering trends and developing innovative defenses enables better protection for individuals, organizations, and the broader digital ecosystem. Stages of social engineering attacks are shown in Figure 2.

8 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/empowering-cyber-resilience/366067

Related Content

Relational Work in Synchronous Text-Based CMC of Virtual Teams
Erika Darics (2010). *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction (pp. 830-851).*
www.irma-international.org/chapter/relational-work-synchronous-text-based/42821

Communication 2.0 at School: A Way to Connect Teachers and Students
Simona Lamonaca (2019). *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications (pp. 1754-1765).*
www.irma-international.org/chapter/communication-20-at-school/221029

An Analysis of Prospective Teachers' Digital Citizenship Behaviour Norms
Mehmet Sincar (2011). *International Journal of Cyber Ethics in Education (pp. 25-40).*
www.irma-international.org/article/analysis-prospective-teachers-digital-citizenship/54451

Transparent Classrooms: How the Mobile Phone is Changing Educational Settings
Carla Ganito (2011). *International Journal of Cyber Ethics in Education (pp. 59-69).*
www.irma-international.org/article/transparent-classrooms-mobile-phone-changing/56109

Encountering New Risks in Educating Children in the Contemporary Society: The Risk of Cyberbullying
Selin Atalay (2022). *Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 263-284).*
www.irma-international.org/chapter/encountering-new-risks-in-educating-children-in-the-contemporary-society/301639