Effective Strategies for Combatting Social Engineering in Cybersecurity

Rajeev Kumar (/affiliate/rajeev-kumar/437279/), Saurabh Srivastava (/affiliate/saurabh-srivastava/464340/), Ahmed A. Elngar (/affiliate/ahmed-a-elngar/428616/)

Pages: 340

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

ISBN13: 9798369366653
ISBN13 Softcover: 9798369366660
EISBN13: 9798369366677

Description & Coverage

Description:

In the digital age, the convergence of advanced technologies and human behavior presents a complex cybersecurity challenge, particularly through the lens of social engineering. Social engineering attacks exploit psychological manipulation rather than relying solely on technical vulnerabilities. By leveraging human trust and deception, these attacks become particularly difficult to defend against, evolving alongside advancements in artificial intelligence, machine learning, and other technologies. This dynamic environment heightens the risk of cyber threats, underscoring the need for comprehensive and innovative strategies to address these emerging vulnerabilities.

Effective Strategies for Combatting Social Engineering in Cybersecurity offers a thorough exploration of these challenges, providing a well-rounded approach to understanding and countering social engineering threats. It delves into the theoretical aspects of social engineering, including the psychological principles that drive these attacks, while also offering practical solutions through real-world case studies and applications. By bridging the gap between theory and practice, the book equips academics, practitioners, and policymakers with actionable strategies to enhance their defenses.

Coverage:

The many academic areas covered in this publication include, but are not limited to:

- Attack Techniques
- Blockchain Technology
- Consequences and Prevention Measures
- Cyber Resilience Strategies
- Cyber Security
- Deep Fakes
- Digital Era of Stealth
- Effective Defense Strategies
- Machine Learning
- Online Interactions
- Organizational Resilience
- Phishing Detection
- Social Engineering Attacks
- Wireshark Effective Strategies

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.

Chapter 7

Securing the weakest link - compressive approaches to social engineering attacks prevention: Strategies for Enhancing Organizational Resilience Against Social Engineering Threats

Farooq Ahmad, Bably Dolly, Zohaib Khan

In today's world, where digital interactions and online transactions are crucial for both personal and professional activities, social engineering attacks have become more common and sophisticated, threatening data security and organizational integrity. These attacks exploit a lack of awareness to gain illegal access to systems. While research includes various studies and methods for preventing these attacks, a thorough analysis of effective strategies is lacking. Current methods involve health campaigns, frameworks with human security sensors, user-focused approaches, and vulnerability models. This chapter thoroughly examines different types of social engineering attacks, such as phishing, vishing, and pretexting, highlighting the human element as the weakest link in cybersecurity. It then delves into prevention methods, stressing the need for awareness training and behavioral changes among users as a key defense. This chapter seeks to equip readers with practical insights and tools to protect against social engineering attacks by integrating current research and best practices.

Chapter 8

Protecting against social engineering using Wireshark Effective Strategies with real-world Examples

Manvi Mishra, Md Shadab Hussain, Sudheer Singh

In the domain of cybersecurity, defending against social engineering attacks remains a critical challenge. This abstract explores effective strategies and real-world examples of using Wireshark—a powerful network protocol analyzer—to mitigate the risks posed by social engineering tactics. Social engineering attacks exploit human psychology rather than technical vulnerabilities, making them difficult to detect through conventional security measures alone. This chapter delves into various strategies for leveraging Wireshark in defense against social engineering. Key aspects include configuring Wireshark for optimal security monitoring, setting up filters and profiles to capture relevant traffic, and decrypting SSL/TLS communications to uncover malicious intent hidden within encrypted data. Detection techniques encompass monitoring DNS and HTTP traffic for signs of phishing attempts, identifying malware communications, and conducting behavioral analysis to spot anomalies in network behavior

Chapter 9

Emerging Trends and Future Directions in Social Engineering Defense

Gopalji Varshneya, Priyanka Tyagi, Rachit Kumar, Nishant Dublish

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 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.

Chapter 10

Exploring the Future Landscape Emerging Trends in Social Engineering Defense: Exploring the Future Landscape: Emerging Trends in Social Engineering Defense

Shweta Dwivedi

Social engineering attacks, characterized by their manipulation of human behavior to breach security protocols, have emerged as a significant threat in the cyber security landscape. As technology evolves, so do the tactics employed by malicious actors. This paper explores the future landscape of social engineering defense by examining emerging trends and innovative strategies designed to mitigate these sophisticated threats. In the beginning, an analysis of the current state of social engineering attacks highlights recent high-profile incidents to illustrate the evolving nature of these threats. The analysis includes a review of common attack vectors such as phishing, pretexting, baiting, and tailgating, emphasizing the psychological manipulation techniques used to exploit human vulnerabilities. One key trend is the integration of advanced artificial intelligence (AI) and machine learning (ML) technologies to detect and respond to social engineering attempts in real time.

Chapter 11

A Comprehensive Guide to Blockchain Technology and its Role in Enhancing Cyber Security and Combating Social Engineering

Praveen Tripathi, Shambhu Bharadwaj

This book chapter will provide an in-depth exploration of blockchain technology, covering its history, fundamental principles and practical applications. The chapter begins with an introduction to the decentralized nature of blockchain, explaining how it works to provide security, immutability and transparency in a trustless environment. It also examines various types of blockchain including public, private and permissioned and explores the advantages and limitations of each. This chapter looks at the future of blockchain technology discussing emerging trends and potential developments in the field. It highlights ongoing research and development efforts aimed at improving the functionality and security of blockchain, as well as exploring new use cases and business models. Overall, this book chapter will provide a comprehensive introduction to blockchain technology, offering insights into its workings, practical applications and potential impact on various industries.

Chapter 12

Social Engineering in Social Media and Online Interactions

Tarun Vashishth, Vikas Sharma, Kewal Sharma, Sachin Chaudhary, Sachin Kaushik, Vinod Bagar

Social engineering in social media and online interactions has emerged as a critical concern in the digital age, driven by the increasing interconnectivity and sharing of personal information online. This study is motivated by the growing prevalence of cyberattacks that exploit human psychology rather than technical vulnerabilities, targeting individuals through platforms where they share personal details. By examining various social engineering techniques such as phishing, pretexting, and