Chapter 16
Assortment of Social Engineering Attacks in the New Digital Era

Geetha Manoharan
https://orcid.org/0000-0002-8644-8871
SR University, India

Chetan Dudhagara
https://orcid.org/0000-0003-1220-5719
Anand Agricultural University, India

ABSTRACT

Social engineering involves stealing secrets. Assaults seek different information each person. Deception is used to gain passwords, financial data, and viruses. This spyware may steal passwords, financial data, and computer control. Attackers utilize social engineering because victim confidence is easier to influence than program weaknesses. Phishing for a password is easier than cracking it. Fast technical change has increased social engineering assaults, which target psychology rather than technology. Hackers utilize many methods to deceive people into disclosing sensitive information or taking digital security risks. We discuss numerous digital social engineering attacks in this chapter. Discussing phishing, pretexting, baiting, quid pro quo, and whaling. We also explore attackers' psychological manipulation and their massive damage to people and organizations. We emphasize awareness, education, and training to prevent social engineering assaults and protect crucial data in the digital era.

DOI: 10.4018/979-8-3693-6665-3.ch016

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

INTRODUCTION TO SOCIAL ENGINEERING

Social engineering refers to malicious actions that take place through human connections. It uses psychological manipulation to trick users into disclosing sensitive information or making security mistakes. Social engineering attacks happen in one or more stages. The attacker investigates the target first to gather background information needed to carry out the assault, such as potential avenues of entry and faulty security measures. Subsequently, the attacker attempts to gain the target's confidence by providing triggers for behaviors that breach security standards, such as exposing private data or granting access to critical resources.

Utilizing human weaknesses is the core of social engineering. We are naturally curious, fearful, trustworthy, and want to be of service to others. Psychological manipulation is how attackers trick victims into divulging private information (Singh, D., et al., 2024), allowing unwanted access, or carrying out destructive actions. Observation, thorough study, and the capacity to adopt many personas and circumstances are typically necessary for social engineering to be successful. An individual or group can use social engineering as a tactic to trick and coerce people into revealing private information, carrying out certain tasks, or allowing unwanted access. It frequently uses deceptive and psychologically manipulative methods to take advantage of human psychology and the propensity to trust others. Social engineering plays on people's innate desire to be helpful, inquisitive, or trustworthy, as opposed to traditional hacking techniques, which focus on taking advantage of technological flaws. By using human flaws, social engineering aims to obtain illegal access or obtain private information for malevolent intentions. Users of businesses' protected information systems are the target of more social engineering assaults than ever before, and their ability to withstand these attacks is declining. Machine learning technologies are taken into consideration as a potential solution to this problem, and the requirement of creating tools to safeguard businesses (Manoharan, G., et al., 2024) from social engineering assaults is documented. Here are the findings from the creation of a software program called a resilience scanner, which assesses an organization's workforce to see how resilient they are against social engineering assaults. As demonstrated by Astakhova, L., & Medvedev, I.A. (2021), it has multiple uses, including identifying user vulnerability, involving users more in the process of identifying social engineering attacks and fostering an information security culture within an organization. It also has potential for future development.

22 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/assortment-of-social-engineering-attacks-in-the-new-digital-era/366077

Related Content

A Study of Cyber Threats on Physical and Mental Health With Special Reference to Pandemic Times
Sanju Choudhary, Vishva Chaudharyand Vijendra Singh Meel (2023). *Cyberfeminism and Gender Violence in Social Media (pp. 288-295).*
www.irma-international.org/chapter/a-study-of-cyber-threats-on-physical-and-mental-health-with-special-reference-to-pandemic-times/331912

The Emergence of Crypto Travel: Revolutionizing Global Tourism With Blockchain and Digital Currencies
Ashish Raina (2025). *Exploring the World With Blockchain Through Cryptotravel (pp. 33-42).*
www.irma-international.org/chapter/the-emergence-of-crypto-travel/364074

Constructing a Diaspora Anglophone Cameroonian Identity Online
Eric A. Anchimbe (2010). *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction (pp. 130-144).*
www.irma-international.org/chapter/constructing-diaspora-anglophone-cameroonian-identity/42776

Online Decision-Making in Receiving Spam Emails Among College Students
Zheng Yanand Hamide Y. Gozu (2012). *International Journal of Cyber Behavior, Psychology and Learning (pp. 1-12).*
www.irma-international.org/article/online-decision-making-receiving-spam/64347

Effect of Screen Media Technologies on Physical and Psychological Well Being in Middle Aged Adults
Priya Singh, Prabhas Bhardwaj, Sushil Kumar Sharmaand Anil Kumar Agrawal (2023). *International Journal of Cyber Behavior, Psychology and Learning (pp. 1-17).*
www.irma-international.org/article/effect-of-screen-media-technologies-on-physical-and-psychological-well-being-in-middle-aged-adults/330132