Chapter 3
Social Engineering in the Digital Age:
A Critical Examination of Attack Techniques, Consequences, and Preventative Measures

Vinay Kumar Pant
Moradabad Institute of Technology, India

Janmejay Pant
Graphic Era Hill University, India

Rohit Kumar Singh
https://orcid.org/0009-0001-3104-0350
Moradabad Institute of Technology, India

Saurabh Srivastava
Moradabad Institute of Technology, India

ABSTRACT

Social engineering is one of the biggest dangers in the digital world today. Attacks using social engineering are extremely dangerous to individuals and organizations by exploiting human psychology to compromise security controls to steal sensitive information. This study explores the different forms of social engineering attacks, analyzes real-world cases, and investigates the strategies attackers employ. It aims to assess the potential consequences for individuals and organizations targeted by these attacks. The study also assesses the effectiveness of current prevention methods, proposing enhanced strategies and best practices to implement measures to reduce the vulnerability with social engineering. By understanding the intricate tactics of

DOI: 10.4018/979-8-3693-6665-3.ch003

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

attackers and the vulnerabilities they exploit, this research aims to provide a robust framework for improving security awareness and defense mechanisms against social engineering threats.

1. INTRODUCTION

The twenty-first century has witnessed a swift transition of various domains like social engagement, Streaming services, education (E-learning platforms) and business (Online marketplaces) to Internet platforms. Consequently, there has been an exponential rise in both quantity and implication of info circulating within the digital world (Abass, I., 2018). The fundamental principle behind social engineering is the exploitation of human behavior and cognitive biases. Attackers craft scenarios that elicit specific responses from their targets, using tactics that can range from impersonation and pretexting to sophisticated phishing campaigns. These attacks can be highly targeted, such as spear phishing aimed at specific individuals or organizations, or broadly cast, like mass email phishing campaigns that target a large number of people indiscriminately. Social engineering assaults have more potential now that they are available online. Attackers can use the large volumes of personal data provided by social media sites, email, and messaging apps. Furthermore, social engineers have more opportunity to take advantage of human error as a weak link as a result of the complexity of digital systems growing.

1.1. Emerging Trends of Social Engineering

- **Deepfakes and Artificial Intelligence:** AI advancements are making it simpler to produce realistic deepfake audio and video, which can be used to pass for real people in convincing ways.
- **Social Media Exploitation:** Assaulters are using social media sites more frequently to obtain personal data for focused assaults (Abroshan, H et al., 2021).
- **Use of Mobile Devices Is Growing:** Social engineering attacks are also moving to mobile platforms, tricking consumers with SMS or app notifications.

1.2. Frequent Targets

Although anybody can become a victim, some groups are more vulnerable than others:

- **Workers:** Frequently singled out for access credentials or corporate data.

14 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/social-engineering-in-the-digital-age/366064

Related Content

Adolescent Perceptions of the Risks and Benefits of Social Networking Site Use

Beatrice Hayes, Alana James, Ravinder Barnand Dawn Watling (2022). *International Journal of Cyber Behavior, Psychology and Learning (pp. 1-22).*
www.irma-international.org/article/adolescent-perceptions-of-the-risks-and-benefits-of-social-networking-site-use/306646

Development and Validation of Teachers Mobile Learning Acceptance Scale for Higher Education Teachers

Niti Mittal, Monica Chaudharyand Shirin Alavi (2017). *International Journal of Cyber Behavior, Psychology and Learning (pp. 76-98).*
www.irma-international.org/article/development-and-validation-of-teachers-mobile-learning-acceptance-scale-for-higher-education-teachers/179596

The Tension Between Human and Cyborg Ethics

Anne Gerdes (2011). *International Journal of Cyber Ethics in Education (pp. 25-35).*
www.irma-international.org/article/tension-between-human-cyborg-ethics/52098

Threats to the Critical Information Infrastructure Protection (CIIP) Posed by Modern Terrorism

Metodi Hadji-Janev (2014). *Cyber Behavior: Concepts, Methodologies, Tools, and Applications (pp. 2077-2097).*
www.irma-international.org/chapter/threats-to-the-critical-information-infrastructure-protection-ciip-posed-by-modern-terrorism/107833

Getting on the "E" List: Email List Use in a Community of Service Provider Organizations for People Experiencing Homelessness

Craig R. Scott, Laurie K. Lewisand Scott C. D'Urso (2010). *Cases on Online Discussion and Interaction: Experiences and Outcomes (pp. 334-350).*
www.irma-international.org/chapter/getting-list-email-list-use/43673