Chapter 4
Psychological Dimensions of Social Engineering in Cybercrime

Sonu Sharma
https://orcid.org/0009-0004-3836-590X
Poornima University, Jaipur, India

Bright Keswani
https://orcid.org/0000-0003-1464-0431
Poornima University, Jaipur, India

Ashish Avasthi
https://orcid.org/0000-0003-3069-1984
Poornima University, Jaipur, India

Sangita Gupta
https://orcid.org/0009-0009-3751-8317
Poornima University, Jaipur, India

Sumit Kumar Kapoor
https://orcid.org/0009-0005-6291-3176
Poornima University, Jaipur, India

Nikhil Kumar Goyal
https://orcid.org/0009-0007-4532-8033
Poornima University, Jaipur, India

ABSTRACT

This chapter reflects on social engineering as an important aspect of cybercrime, based on the psychology principles that make it possible to manipulate and deceive the individual in digital realities. It explains cognitive and emotional loopholes that attackers use, i.e. trust, fear, authority and curiosity, and discusses some commonly-used attack vectors, i.e. phishing, pretexting and impersonation. The discussion points out both the personal and corporate other results, that vary between financial loss and psychological trauma and loss of reputation. The idea is that there is a synergy between human psychology and technological systems that cybercriminals are able to adjust their tactics to the changing systems. The chapter also discusses defense measures, involving awareness training, psychological resilience and technical measures, as well as legal and ethical issues.

DOI: 10.4018/979-8-3373-4898-8.ch004

1. INTRODUCTION

1.1 Cybercrime in the Modern Era

Cybercrime has elevated the single and incidence-based computer misuse to an international systematized and very lucrative business. In the previous decades, individuals hackers driven by curiosity or fame were the main perpetrators of attacks. Cybercrime today is fuelled by monetary gain or political interest and even attempts by states to do the same. Attackers use the enormous digital landscape that is the internet, a connected network of billions of devices, cloud-based work, and communication infrastructure, to target individuals and organisations in large volumes. Cybercrime is no longer focused just on technical skills; the approach figured in social, cultural and psychological measures in order to overcome security protocols (Abroshan, Devos, Poels, & Laermans, 2021).

The emergence of digital banking, e-commerce, and telework has increased the targets of the criminals. Due to poor authentication mechanisms, human carelessness, and cognitive failures, malicious parties will always take advantage to access the system even though it is solid technologically. Indeed, some of the worst attacks in recent years have not been caused by sophisticated malware or zero-day attacks but instead by tricked employees clicking on malicious links or improperly sharing confidential information. Therefore, cybercrime indicates the paradox of the fact that technology continuously evolves on the one hand and, on the other hand, the human aspect always stays under threat of attack.

In addition, cybercrime is not confined to one country; therefore, a comprehensive way of controlling it or prosecuting it is impossible. Criminals in one region of the world can assault the victims located thousands of kilometers with little chance of being detected. This has led to the formation of dark web marketplaces where stolen data and phishing kits together with hacking services get sold off as commodities. The impact of this process of professionalization of cybercrime is that even those with very little technical knowledge can actually deliver effective attacks using purchased social engineering tools. This dynamic rides more strongly in view of the fact that cybercrime needs to be looked beyond a technological issue and more as a human dilemma (Wang, Zhu, & Sun, 2021).

1.2 Role of Human Psychology in Cybersecurity

Core to social engineering is human psychology. Cybercriminals also know that firewalls, intrusion detection systems, and encryption can inhibit the access of a digital system but that people could frequently be cajoled or coerced to give access. Human psychology is rife with predictable tendencies- to be inclined toward

Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*

www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186