

Social Engineering

Faculty of Engineering & Technology

Subject: Computer Security (Comp 432)

Instructor: Mohammad Khanafseh

A dark blue diagonal gradient bar that starts from the bottom left corner and extends towards the top right corner, covering the lower half of the slide.

Members



Hassan A Melhim
1203289



Rasheed S AlQobbaj
1202474



Mohammed I Shabaneh
1201297

What is social engineering?

Key aspects:

- Scouting for information, targets, and vulnerabilities.
- Social skills to manipulate, lie, detect social cues.
- Technical skills to use Hacking technique.

Common technologies involved

OSINT:

- Gathering information from public resources to research the potential target.
- Key Concepts:
 - Data Sources
 - Information gathering
 - Exploitation

Spear-Phishing:

- Targeted attempt to steal information through impersonation
- Key Concepts
 - Personalization
 - Deceptive Tactics
 - Payloads

Case Study:

Evaldas Rimasauskas

Scamming \$100 Million from Facebook and Google

Case Study: Evaldas Rimasauskas Scamming \$100 Million from Facebook and Google



The scam exploited several vulnerabilities:

- **Lack of Verification Protocols:**
Employees failed to verify the authenticity of the emails and the associated requests through independent channels.
- **Over-Reliance on Email Communication:**
The companies' reliance on email for processing financial transactions without additional layers of verification or security checks made it easier for the scam to succeed.

To what degree does social engineering threatens cybersecurity?

The **motivation** for this research stems from the increasing sophistication and frequency of social engineering attacks, which pose significant threats to individuals and organizations. These attacks exploit the fact that **humans are often the weakest link in the security chain**, as it is often easier for attackers to manipulate individuals than to breach well-defended systems.

Additionally, the intriguing role of human psychology and behavior in these attacks highlights the need for understanding and mitigating these vulnerabilities. The interest in social engineering also arises from its significant implications in **criminal investigations**, where understanding these tactics can aid in solving and preventing crimes.

Threats, Countermeasures, and Future Trends

Threats and Risks

Main risks

- Financial Loss
- Data Breach
- Reputation Damage
- Operation Disruption

Threat Actors

- Cybercriminals
- Nation-State Actors
- Insider Threats

Countermeasures and Detection

Detection methods

- Email Filtering
- Raising Awareness
- Employee Education

Countermeasures

- Technical Level
 - Multi-Factor Authentication
- Managerial Level
 - Regular training programs
- Individual Level
 - Beware of suspicious links

Future Trends and Challenges

- Evolving tactics
 - Use of AI to advance the attackers disguises
- Increased accuracy in targeting
 - Targeting remote workers more due to less secure networks

References

- Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media Yeboah-Ofori, Abel. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. International Journal of Cyber-Security and Digital Forensics. 7. 87-98. 10.17781/P002378.
- Evaldas Rimasauskas Scamming \$100 Million from Facebook and Google Jr., Tom Huddleston. "How This Scammer Used Phishing Emails to Steal over \$100 Million from Google and Facebook." CNBC, CNBC, 27 Mar. 2019.
- Impact of Social Engineering Attacks: A Literature Review Fuertes, Walter & Arévalo, Diana & Castro, Joyce & Ron, Mario & Estrada, Carlos & Andrade, Roberto & Peña, Felix & Benavides, Eduardo. (2022). Impact of Social Engineering Attacks: A Literature Review. 10.1007/978-981-16-4884-7_3.
- Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks Halevi, Tzipora & Memon, Nasir & Nov, Oded. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. 10.2139/ssrn.2544742.