Social Engineering Attacks: Analysis and study

By Miriam Ferreira

Contents

Overview

In this project I explored social engineering attacks, focusing on how attackers exploit human behaviour rather than technical vulnerabilities. The goal was to understand common attack patterns, recognize red flags, and analyse how realworld attacks succeed even with existing security controls.

Scope of the Project

The project covers

- Common social engineering techniques
- Typical attacker workflow
- Behavioural and technical indicators of attacks
- A realworld example studied where social engineering led to ransomware compromise

Attack Types

Phishing: deceptive emails designed to steal credentials or deliver malware
Vishing: voicebased scams impersonating trusted entities
Smishing: SMSbased phishing attacks
Pretexting: attackers crafting believable identities or scenarios
Malicious Links and attachments: delivery mechanisms for further compromise

How Social Engineering Attacks Work

From the analysis, most attacks follow a predictable pattern

- Collection of publicly available information about the target
- Creation of a believable story using urgency, authority, or trust
- Delivery through email, SMS, voice, or messaging
- Coercing the victim into an action (clicking, replying, transferring funds)
- Exploitation of the access gained to achieve the attacker's objective

Key indicators and red flags

- Urgent or threatening language demanding immediate action
- Requests for credentials or sensitive data
- Slightly altered email domains or sender identities
- Unexpected contact through unofficial channels
- Repeated follow-ups designed to pressure the victim

- Attachments or links using unusual file types or shortened URLs

Real world example

The project included an analysis of a ransomware incident that began as a social engineering attack:

- The attacker impersonated a legitimate employee of a gaming platform
- Publicly available user information was used to build credibility
- Communication occurred outside official support channels
- The attacker applied pressure and scripted responses to force compliance

This case highlighted how social engineering often acts as the entry point for more serious technical attacks.

What I Learned

Through this project, I learned why human trust is often the weakest link in security systems. How attackers' chain psychological manipulation to get what they want. How small inconsistencies in tone, behaviour, or delivery can easily reveal attacks and why user awareness and process controls matter as much as technical defences.

Limitations and future improvements

The project focuses on analysis rather than detection tooling. Future work could include simulated phishing campaigns or defensive automation but for one of my first projects in this section, this gave me a good insight on threat vectors.

Disclaimer

This project is for educational purposes only and focuses on defensive awareness and analysis.