KAFE Project

Social Engineering Attack

By Miriam Ferreira & Inès Brakta

Contents

Overview

This group project explored how attackers combine publicly available information (OSINT) with social engineering techniques to prepare realistic phishing attacks. The goal was to understand attacker methodology in order to highlight risks, identify warning signs, and emphasize the importance of security awareness.

All activities were conducted in a controlled lab environment using fictional data.

Project Type

- Educational security lab
- Threat modeling & awareness
- Attack simulation for defensive understanding

Tools Used

- Maltego - OSINT and relationship mapping
- Social Engineering Toolkit (SET) - Phishing simulation framework
- Kali Linux - Isolated lab environment

Methodology

The project followed a realistic attacker workflow.

Information Gathering (OSINT)

- Mapping public company infrastructure
- Identifying email patterns and employee roles
- Linking employees to roles and access levels

Target Selection

- Identifying roles commonly targeted in phishing campaigns (e.g. HR, IT, executives)
- Prioritizing targets based on authority and access

Attack Preparation

We simulated phishing pages using SET , then demonstrated impersonation techniques (trusted sender abuse) showing how minimal public data can be weaponized.

Victim Perspective

We demonstrated how realistic phishing emails appear to end users highlighting why these attacks succeed.

Personas and Threat Modeling

The project included several personas to model organizational hierarchy:

- Executive (high authority)
- HR employee (common phishing target)
- IT staff (trusted sender impersonation)
- Frontdesk staff (low security awareness)

This helped illustrate how attackers adapt techniques based on role and access.

Key Takeaways

- No systems were hacked - all information used was publicly accessible
- OSINT significantly lowers the barrier for social engineering attacks
- Trust, urgency, and authority are consistently exploited
- High authority and administrative roles are prime targets
- User awareness is as critical as technical defenses

Ethical Considerations

- No real users or organizations were targeted
- No credentials were harvested from real systems
- The project focused on understanding attack preparation, not exploitation

What I Learned

- How attackers chain OSINT with social engineering
- Why role-based targeting is more effective than random phishing
- How easy it is to abuse trust relationships
- The importance of security awareness training and internal procedures

Collaboration

This was a group project completed with Inès Brakta.

Disclaimer

This project is for educational and defensive awareness purposes only.