Social Engineering - Discover how attackers exploit human psychology to manipulate individuals into revealing confidential information or performing actions that compromise security.

Email Attachments - Understand the dangers hidden in email attachments and links, and learn how to protect your devices from malicious software like botnets and rootkits.

Dumpster Diving - Learn about the risks of dumpster diving, where attackers sift through trash for sensitive information, and find out how to dispose of data securely.

Pop-Up Ads - Implement strategies to keep your browsing safe. Identify and avoid hoaxes using pop-up ads that can deceive you into downloading harmful software.

Shoulder Surfing - Find out how attackers can steal your information just by watching over your shoulder and discover practical steps to prevent this invasive tactic.

Tailgating - Understand the threat of tailgating, where unauthorized individuals follow legitimate personnel into secure areas, and learn how to guard against it.

Martin Grobisen

E-mail: grobisen@gmail.com

Cyber Training

Keeping our company safe!

STAY CYBER SAFE: PROTECT YOURSELF FROM SOCIAL ENGINEERING ATTACKS

Welcome to our cyber training course, designed to arm you with the knowledge you need to recognize and thwart social engineering attacks. In today's digital landscape, being informed is your best defense.

- Social Engineering
- Email Attachments
- Dumpster Diving
- Pop-Up Ads
- Shoulder Surfing
- Tailgating

What is Social Engineering?

Social engineering is the art of manipulating people into divulging confidential information or performing actions that compromise security. It exploits human psychology rather than technical vulnerabilities.

Common Social Engineering Attacks

Authority: Attackers pose as authority figures to trick staff into sharing sensitive information.

Scarcity: Creating a sense of urgency to prompt quick, unsafe actions.

Urgency: Pressuring targets to act quickly without proper verification.

Familiarity: Pretending to be someone familiar to gain trust.

Trust: Exploiting established trust to bypass security measures.

Further Reading:

What is Social Engineering? - IBM

10 Types of Social Engineering Attacks - CrowdStrike

Email Attachments and Links

Email attachments and links can be used to infect computers with malware, such as botnets and rootkits. Botnets are networks of infected computers controlled remotely, while rootkits hide malicious software.

Analyzing Web Links

To evaluate the veracity of web links, check the URL for misspellings, unusual domain names, and verify the site's security (look for "https" and a padlock icon).

Further Reading:

What is Social Engineering? - IBM
Website Link Analyzer - cmlabs

Dumpster Diving

Dumpster diving involves searching through trash for sensitive information. To counter it, shred all documents, erase storage media, and educate staff about the risks.

Further Reading:

What is Dumpster Diving? - TechTarget

Hoaxes with Pop-Up Ads

Hoaxes often use pop-up ads to trick users into downloading malware. Always close pop-ups without clicking and use ad blockers.

Further Reading:

What is a dumpster diving attack? Tips to keep your data safe - Comparitech

Shoulder Surfing

Shoulder surfing is when attackers watch over someone's shoulder to steal information. Use privacy screens and be aware of your surroundings.

Further Reading:

What Is Shoulder Surfing? How It Happens & How to Avoid It - Aura

Tailgating

Tailgating is when unauthorized individuals follow authorized personnel into secure areas. Always ensure doors close behind you and report suspicious behavior.

Further Reading:

Social Engineering: 9 Attack Techniques and 6 Defensive Measures