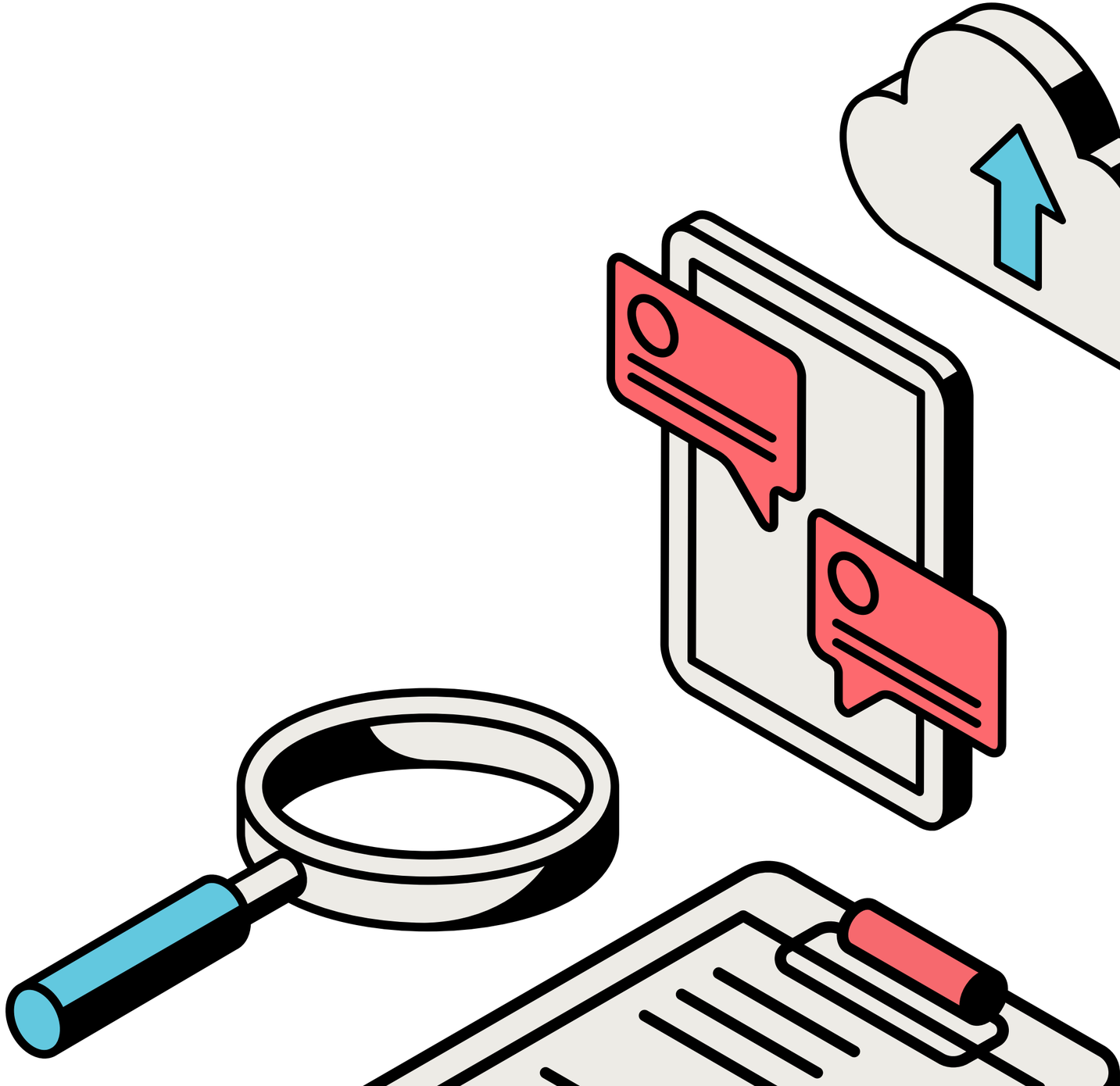
cyber673

Social Engineering



Date: January 23 2025

Prepared by: Fauzan Salleh

Content:

1. Introduction
2. Types of Social Engineering Attacks
3. Psychological Principles Behind Social Engineering
4. Common Targets and Vulnerabilities
5. Prevention and Mitigation Strategies
6. Real Life Example
7. Demo

cyber673

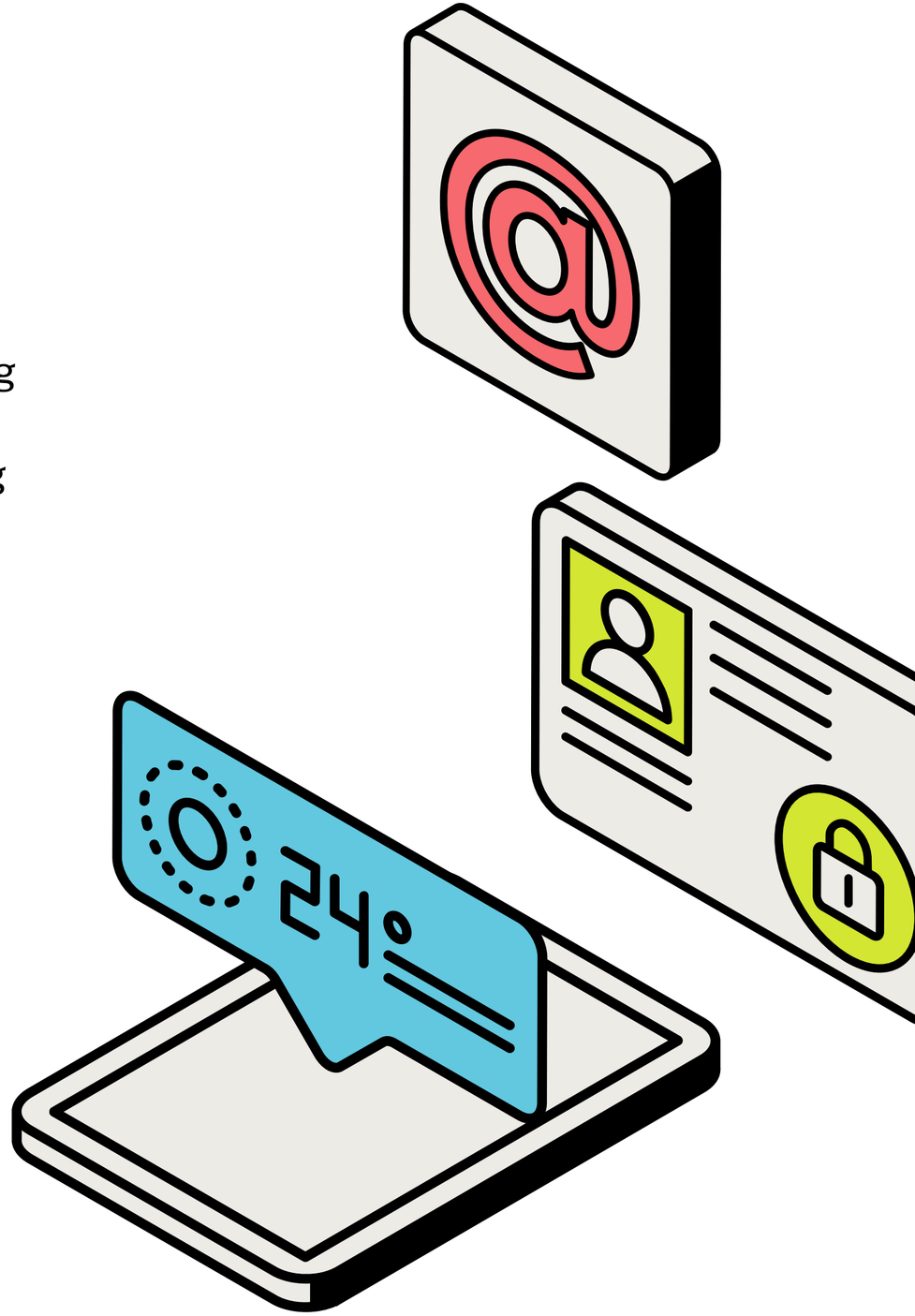
Introduction

- Definition:
  - Social engineering is the art of manipulating people into performing actions or divulging confidential information. Unlike traditional hacking, which exploits technical vulnerabilities, social engineering exploits human psychology

- Famous hacker Kevin Mitnick helped popularize the term ‘social engineering’ in the ’90s, although the idea and many of the techniques have been around as long as there have been scam artists.

- Social engineering attacks increased 45% in 2023, coincident with the launch of ChatGPT (source: SlashNext)
- On average, companies face more than **700** social engineering attacks annually, or about **2.7** attacks every day. (Firewall Times)

cyber673



Types of Social Engineering Attack

A

Phishing

involves sending fraudulent communications, usually emails, that appear to come from a reputable source. The goal is to steal sensitive data like login credentials or financial information.

B

Baiting

involves offering something enticing to the target, such as free software or a music download, to trick them into providing personal information or downloading malware.

C

Pretexting

involves creating a fabricated scenario (pretext) to obtain information from the target. The attacker often pretends to need the information to confirm the target's identity.

cyber673

Types of Social Engineering Attack

D

Business Email Compromise (BEC)

involves an attacker impersonating a high-level executive or trusted business partner to trick employees into transferring money or sensitive information.

E

Quid Pro Quo

involves an attacker offering a service or benefit in exchange for information or access.

F

Tailgating

also known as piggybacking, involves an unauthorized person following an authorized person into a restricted area.

cyber673

Psychological Principles Behind Social Engineering

AUTHORITY

SOCIAL PROOF

SCARCITY & URGENCY

FAMILIARITY & LIKING

RECIPROCITY

cyber673

Common Target and Vulnerabilities

Individuals

- **Lack of Awareness**: Many people are not familiar with social engineering techniques and may not recognize suspicious behavior
- **Weak Passwords**: Using simple or reused passwords makes it easier for attackers to gain access to accounts
- **Over-Sharing Information**: Sharing too much personal information on social media can provide attackers with the data they need to craft convincing attacks

cyber673

Common Target and Vulnerabilities

Organizations

- **Insufficient Training:** Employees may not receive adequate training on recognizing and responding to social engineering attacks
- **Poor Security Policies:** Lack of robust security policies and procedures can leave organizations vulnerable
- **Third-Party Risks:** Vendors and partners with weaker security practices can be exploited to gain access to the organization

cyber673

Prevention and Mitigation Strategies

1	Awareness and Training
2	Implementing Security Policies
3	Using Multi-Factor Authentication (MFA)
4	Regular Security Audits
5	Technology Solutions
6	Encouraging a Security-Conscious Culture

cyber673

Real Life Example:

Pepco Social Engineering Attack (2024)

cyber673

Pepco Group

- **Incident**: In February 2024, Pepco Group, a major European retailer, suffered a devastating social engineering attack.
- **Impact**: The attack resulted in a loss of approximately €15.5 million.
- **Method**: The attackers likely used a sophisticated phishing technique, spoofing legitimate employee emails to deceive the finance staff into transferring funds
- **Significance**: This case highlights the growing sophistication of social engineering attacks and the significant financial impact they can have on organizations.

cyber673

Real Life Example:

Bunny Loader Malware

cyber673

Bunny Loader Malware

- **Overview:** Bunny Loader is a new malware loader observed by Rapid7, designed to deliver and execute additional malware on compromised systems.
- **Techniques:** It uses advanced evasion techniques such as Process Doppelgänging, DLL Search Order Hijacking, and Heaven's Gate to avoid detection
- **Payloads:** Bunny Loader has been used to deliver various infostealers, including Stealc, Lumma, and Amadey
- **Distribution:** The loader is often disguised as legitimate software, such as a 7-zip installer, to trick users into executing it
- **Impact:** Once executed, the loader can steal sensitive information from the victim's system and send it to the attacker's command and control servers

cyber673

Thank you.

cyber673