THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Social engineering — manipulation as method

Social engineering is the foundation of nearly every other threat in this library. We explain the six classic levers (authority, scarcity, reciprocity, consistency, liking, consensus) and how they operate in the workplace.

min read: 7 min **Updated:** 14 March 2026 **Risk:** High risk
Source: awareness-as-a-service.com/en/resources/threats/social-engineering

What is social engineering?

Social engineering describes the systematic use of psychological manipulation to induce people to take actions they would otherwise not take — revealing credentials, opening a door, authorising a payment, installing software.

The term is deliberately broad: social engineering is not a single attack type, but the foundation of almost every other threat in this library. Phishing manipulates via email. CEO fraud exploits hierarchy. Vishing works over the phone. What all of them share is reliance on human predictability — on six principles that social psychologist Robert Cialdini described in the 1980s and which have since been systematically deployed by attackers.

In a corporate context, social engineering plays a particularly important role in initial access: the first step into a well-secured network almost always passes through a person rather than a technical gap.

At a glance

01

Technology cannot stop it alone

No firewall ruleset protects against an employee who gives a convincing-sounding caller a password. Social engineering bypasses technology by targeting people.

02

Predictable patterns

Authority, scarcity, reciprocity, consistency, liking, consensus — anyone who knows these six levers can spot them before they take effect.

03

Physical attacks are real

Tailgating, impersonation, and dumpster diving are physical social engineering techniques that occur regularly in corporate environments.

How to recognise social engineering

Unnatural friendliness
Attackers deliberately build rapport before making a demand. Conspicuously friendly strangers who take a keen interest in your work deserve closer attention.

Unnecessary urgency ("immediately", "right now")
Time pressure disables reflective thinking. Anyone pressing you to act immediately without time for questions is exploiting the scarcity principle.

Appeal to authority
"The CEO personally instructed this", "I am from the IT security team" — invoking authority raises willingness to break rules.

"Could you just do this for me?"
Small favours asking someone to share credentials or unlock systems — often preceded by a favour the attacker did first (reciprocity).

Tailgating
Someone follows you through a secured door without their own access card. Politeness (holding the door) is used as an entry point into secured areas.

Suspiciously accurate internal knowledge
If someone knows project names, colleague names, or internal procedures that are not public, they may have researched them via LinkedIn, OSINT, or a compromised account.

How to protect yourself

For employees

- **Slow down every unusual request:** When uncertain, "let me check and get back to you" is always acceptable. No pressure to decide on the spot.
- **Verify identity via a known channel:** For calls or emails requesting access or actions, call back on a number you already have.
- **Do not hold doors for strangers** who cannot show their own access credential. This is a protective measure, not rudeness.
- **Do not share internal details unnecessarily:** Org charts, project names, and colleague names are valuable reconnaissance material for attackers.

For administrators

- **Regular tabletop exercises and social engineering simulations** (physical and digital).
- **Communicate clear escalation paths:** What do I do when I receive a suspicious request? Who do I call?
- **Privileged Access Management (PAM):** High-privilege credentials scoped to specific tasks and automatically time-limited — minimises the blast radius of a social engineering compromise.
- **Visitor management system:** Physical visitors always registered, escorted, and accompanied. No free access for "IT technicians" without a helpdesk ticket.
- **Awareness campaigns** on Cialdini's six principles: when employees recognise the patterns, they can catch them in real time.

Real cases

CASE 01 · UNIVERSITY · DE · Q2/2025

An attacker called the IT department posing as a lecturer, claiming to be abroad with an expired laptop password. He knew the IT manager's name and a current project. The helpdesk employee reset the password without identity verification. The attacker subsequently accessed exam data.

Damage: exam content exfiltrated, data protection incident · **Detection:** the real lecturer reported password issues a week later · **Lesson:** Password resets must only occur after secure identity verification (video call or in person).

CASE 02 · PHARMACEUTICAL COMPANY · CH · Q3/2025

An attacker posed as an external maintenance engineer and entered the building using a convincing-looking (forged) security badge. In an unsupervised server room, he installed a hardware keylogger on an administrator's PC. The device went undetected for six weeks.

Damage: admin credentials exfiltrated, forensic investigation required · **Detection:** spotted during a routine internal IT check · **Lesson:** Physical access to IT infrastructure must be linked to a helpdesk ticket — unannounced technicians are not admitted.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Interrupt the action** if possible — stop a transaction, revoke credentials, close the door again.
2. **Document everything:** who called, what was said exactly, what information was shared?
3. **Inform IT Security or the information security officer** — even for incidents where "probably nothing happened". Attempts are signals.
4. **Change credentials** if they may have been shared or viewed.
5. **Request elevated monitoring** on affected systems to detect follow-on attacker actions.
6. **Alert colleagues:** If an attacker has targeted a specific role, project, or building area, other employees may be contacted next.

Frequently asked questions

Can social engineering occur with no technical component?

Yes. Tailgating, impersonation at government offices, collecting discarded documents (dumpster diving), and screen-watching (shoulder surfing) are entirely physical social engineering techniques.

Why are even experienced employees vulnerable?

Because Cialdini's principles target evolutionary behavioural patterns — not gaps in knowledge. Under time pressure, authority pressure, or social pressure, people respond differently than in calm analysis.

What is OSINT and how do attackers use it?

OSINT (Open Source Intelligence) means gathering information from public sources: LinkedIn, Xing, company websites, company registries, press releases, GitHub. Attackers use it to appear convincingly well-informed.

Do security awareness trainings actually help?

Yes — when they are conducted regularly, practically, and with simulations. Annual one-off training has little lasting effect. Short, frequent learning units and simulated attacks with debriefings demonstrably work better.

Related topics

Social engineering is the foundation for phishing, CEO fraud, and many insider threat scenarios. Employees who understand manipulation techniques have a significantly higher detection rate across all other threat types.