CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

The attacker's perspective "Social Engineering"

www.cyber-smv.dk

The tool has been developed as part of the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), supported by the Danish Industry Foundation. Published on May 12, 2026.

The attacker's perspective

Purpose

→To increase understanding of social engineering.

→To understand how attackers think and work.

→To become better at detecting manipulation before damage occurs

Mental model

→*Cybersecurity is more about people than technology.*

Participants

→All employees (administration and production).

→Highly suitable for onboarding and teams with external contacts.

Input

→Publicly available information (e.g., LinkedIn profiles, email signatures).

→Examples of social engineering attacks.

Case

→You work in a Danish manufacturing company with approximately 80–100 employees.
  →The company has:
  →An ERP system.
  →Suppliers in Denmark and abroad.
  →Production facilities connected to IT systems.
  →Employees with email, phone, and access cards.
→The attacker wants:
  →Login credentials.
  →Access to systems.
  →Information about suppliers, orders, or production.

Approach

→Step 1 – Think Like the Attacker (10–15 min.)

Task: Imagine that you are an attacker trying to deceive yourselves or your colleagues. Discuss the following:

1. Who in the company is the easiest to attack, and why?
2. What information can be found publicly? (e.g., website, LinkedIn, emails, etc.)
3. Which situations create busyness, stress, or authority?

Approach

→Step 2 – Design the Attack (15 min.)

Task: You must now design a social engineering attack.

1. How does the attacker make contact (email, phone, SMS, physical presence, etc.)?
2. What role does the attacker pretend to have (supplier, IT support, manager, shipping company, etc.)?
3. What emotion is the attacker trying to exploit (urgency, fear, helpfulness, authority, etc.)?

Approach

→Step 3 – The Defensive Perspective (10 min.)

Task: You must now switch perspective and answer the following:

1. What warning signs are there in the attack?
2. What should the employee do in the situation?
3. Who should be contacted internally?

Possible discussions: Think like the attacker

1. **Who in the company is the easiest to attack, and why?**

→Typical easy targets are:

- →Purchasing and finance - work with suppliers, invoices, and changes.
- →Reception and administration - used to helping and providing information.
- →Production staff under time pressure - focused on operations rather than security.
- →New employees - do not yet know the procedures and norms.

👉**The attacker's logic:** I choose people with:

- →Busyness.
- →Many external contacts.
- →Low likelihood of asking critical questions.

Possible discussions: Think like the attacker

2. What information can be found publicly? (examples)

→Names, job titles, and email addresses on the website.
→LinkedIn profiles (responsibilities, relationships, previous jobs).
→Suppliers mentioned in news articles or job postings.
→Production equipment and processes mentioned in marketing materials.
👉 **The attacker's logic:** The more the company shares openly, the easier it is to sound credible.

3. What situations create busyness, stress, or authority? (examples)

→End-of-month periods/invoicing periods.
→Production shutdowns or urgent orders.
→Supplier changes or system updates.
→Messages pretending to come from management or IT.
👉 **The attacker's logic:** I attack when the employee does not have time to think things through.

Possible discussions: Design the attack

1. How does the attacker make contact?

→Typical choices:

→Email (most commonly used and cheapest).

→Phone calls (create pressure and authority).

→SMS (short, urgent messages).

→Physical presence (“I’m from the supplier/IT department”).

👉 **The attacker’s logic:** I choose the channel where it is hardest to verify things quickly.

Possible discussions: Design the attack

2. What role does the attacker pretend to have?

Examples of roles:

→Known supplier
→IT support / system provider
→Manager or executive office
→Shipping company or technician

👉 **The attacker's logic:** I choose a role that is normally not questioned.

Possible discussions: Design the attack

3. What emotion is the attacker trying to exploit?

→Urgency: “This needs to be done now”
→Fear: “Otherwise the system will stop”
→Helpfulness: “Can you just help me?”
→Authority: “Management has asked me to do this”

👉 **The attacker’s logic:** If I control the emotions, critical thinking stops.

Possible discussions: The defensive perspective

1. What warning signs are there in the attack?

→Typical red flags:

- →Unexpected inquiries or contact attempts.
- →Time pressure or threats.
- →Unusual language, spelling mistakes, or tone.
- →Requests for login credentials, codes, or changes.
- →“We normally don’t do it that way.”

2. What should the employee do?

→Stop and take a pause.

→Avoid clicking, replying, or sharing information.

→Verify through a known contact channel.

→Contact a manager, IT, or the security officer.

👉 **VImportant point:** It is professional to be skeptical.

Possible discussions: The defensive perspective

3. Who should be contacted internally?

→ It depends on the company, but typically:

- → The immediate manager.
- → The IT manager/service desk.
- → The security or compliance function.
- → A shared email address or phone number for security incidents.