KORUR

SECURITY WORKSHOPS · MATERIALS

Security Workshop Materials

The reference guide that accompanies Korur's hands-on security awareness workshops for your whole team.

The threat landscape changed. Your team's habits haven't. We come to you and turn your staff into your strongest line of defense, through doing, not slideware.

Why Your Team Needs Training Now

The threat landscape changed. Your team's habits haven't, yet.

74%

Human Error Drives Breaches

Three-quarters of all breaches involve a human element, phishing clicks, misconfigured tools, or stolen credentials.

€85K

Average SME Incident Cost

The average cybersecurity incident costs a Dutch SME €85,000, most of that from downtime, recovery, and reputational damage.

NIS2

NIS2 Requires Training Records

The EU NIS2 directive, now in force, requires organizations to document employee security training. Penalties reach €10M.

12 h

Phishing Is Faster Than Ever

Without trained staff, phishing breaches go undetected for an average of 12 hours, enough for attackers to move laterally and deploy ransomware.

What Your Team Walks Away With

Concrete skills and materials your team applies from day one.

- Ability to identify phishing, vishing, and pretexting attempts in real-world scenarios
- Safe device, password, and public network habits that reduce your attack surface
- A clear personal action plan for responding to a suspected incident
- NIS2-compliant training records for every participant
- A practical role-specific incident response reference card
- Access to a follow-up Q&A session with a Korur engineer

Workshop Format

A structured half-day or full-day format built around doing, not listening.

1. **Threat Landscape Briefing**
   We open with a 30-minute brief on the actual threats your industry faces right now, real examples, real attacker techniques.
2. **Hands-On Lab Exercises**
   Participants work through guided attack-and-defense scenarios using live tools. No slide decks, actual keyboards.
3. **Role-Specific Breakouts**
   Teams split by role (management, developers, operations, general staff) to work through scenarios relevant to their daily work.
4. **Incident Response Simulation**
   A tabletop exercise where participants practice what to do, who to call, what to preserve, what not to do, when an incident is suspected.
5. **Debrief and Action Plan**
   We close with a structured debrief, distribute reference materials, and set 30-day follow-up actions for each participant.

> This document is a companion to Korur's Security Workshop Materials. It summarizes the framework covered during the live training. The hands-on labs, role-specific breakouts, and Q&A take place during the session itself.

Ready to run this with your team?
Korur delivers this training on-site, tailored to your industry and stack. Book a session at **korur.nl/contact**.