Security awareness: which behaviors are worth training, and what actually changes them?

This quarter, pick a few behaviors per role, starting with reporting at once and confirming payment and reset requests by call-back, turn on one-click reporting in Outlook and Teams, and book management's NIS2 training if your organization is in scope. Judge every other awareness measure by whether more people report, and sooner, not by click rates.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for
Security, IT and HR leads in EU organizations of any size, many in Germany, who run or buy security awareness programs, including management training under NIS2

Latest version
sheets.einblick.dev/security-awareness/

If you only do five things

1. **Pick a few behaviors per role.**
   Report at once, confirm payment and credential requests through a second channel, check identity before resets, sign in with passkeys or the password manager and use only the approved AI tool. Microsoft advises role-based training on phishing, ClickFix prompts and unusual requests to run commands or share credentials[1].
2. **Make reporting one click and blameless.**
   Turn on reporting of messages and calls in Teams[2] and the Report button in Outlook, then thank each reporter and say what happened. Users who fear reprisals won't report mistakes promptly, if at all, the NCSC warns[3].
3. **Train the help desk to refuse resets on a call alone.**
   Financially motivated groups vish help desks while posing as employees, and Mandiant advises training help desk staff on unauthorized MFA reset requests[4]. Write down how callers are verified, using the recovery rules in the passkeys and MFA sheet.
4. **Count reports and time to report, not clicks.**
   The lure sets the click rate: at UC San Diego Health, bland lures fooled 1-2% of staff and one over 30%[5]. ETH Zurich estimates that if 100 staff get a phishing email, one likely reports it within 5 minutes[13].
5. **Train management on decisions, and keep the record.**
   Management of German NIS2 entities must attend training regularly[6]; the BSI's example first session takes 4 hours[7]. Record provider, participants and roles, date, duration and content[8].

Build the program in this order

1. **Which mistakes would hurt you most?**
   Go through recent incidents, help desk tickets and fraud attempts, then pick three to five behaviors per role.
2. **Is the secure way the easy way?**
   Roll out passkeys, a password manager, the report button and an approved AI tool first. The BSI says systems should make secure behavior easy[10].
3. **Does each rule fit in one sentence?**
   Put one page of rules per role into onboarding. The NCSC says to test every rule for usability and to separate rules from advice[11].
4. **When does each person hear it?**
   At onboarding, on moving into a security-relevant role[9] and when threats change. The BSI suggests onboarding plus a yearly update[10].
5. **Does it hold up against a real attempt?**
   Test the process, not the person: have someone call the help desk for a reset and time how fast a report reaches security. Mandiant advises measuring how fast you detect interactive social engineering[4].

What to train, by role

- **Everyone.** Report at once, including your own click. Never grant remote access you didn't ask for: vishing callers use it to take over the computer[1]. If the password manager won't fill, stop: it fills only on the real domain[5]. Use only the approved AI tool; 67% of AI users on work devices use non-corporate accounts[12].
- **Finance and HR.** Confirm bank detail changes by call-back, as the endpoints and email sheet says. Payroll diversion peaks on Mondays[1].
- **Help desk.** Verify before every reset: call back on the directory number or ask the manager, and for admin accounts check ID in person, not over video.
- **Admins and developers.** Cover secure configuration, known threats and what to do in a security event[9]. Warn developers about fake recruiting and git repositories to troubleshoot, which espionage actors use[12].

Voice phishing and the help desk

- **A common script.** Attackers flood a user with spam, then message them on Teams as the help desk and ask them to share their desktop[12]. Tell staff that IT never contacts them from outside accounts.
- **Email that asks you to call.** One in four impersonation emails pushes the victim to a phone call, outside email defenses[1].
- **Callers keep people talking.** 93% of attackers studied kept a target on a Teams call for 20 seconds or more at least once, and most now use names that look like employees[1].
- **Limit who can reach staff.** Teams allows all external domains by default[17]; choose **Allow only specific external domains**.
- **Don't trust the voice.** AI and deepfakes make any unauthenticated conversation an easy target[1], so base every reset on a check.

What the evidence says about phishing training

- **Recent annual training didn't predict who clicked** in 10 simulations sent to over 19,500 UC San Diego Health staff[5].
- **Training after a click barely helps.** It cut failure rates by 1.7 percentage points, and over half of sessions ended within 10 seconds[5]. In ETH Zurich's 2022 study, staff shown training clicked more[13].
- **Reminders do the work, not content.** Delayed training worked as well, rewards didn't help, and the problem was attention, not knowledge[14].
- **Most people click eventually.** 56% of UC San Diego Health staff clicked at least once in 8 months[5].

What you owe regulators

- **NIS2.** Management bodies must follow training, staff training is encouraged, and training is a required measure[15].
- **Germany.** BSIG § 38 binds management; § 30 covers staff training and awareness[6,10]. Keep records of both[10,8].
- **Digital providers.** Regulation 2024/2690 requires recurring awareness for staff and management, and role training assessed for effectiveness[9].
- **DORA.** Awareness and resilience training are compulsory for all staff and senior management, and management body members train regularly[16].
- **AI Act.** For AI literacy, see the AI Act sheet.

What changed in 2026

- **Mandiant said to train beyond the inbox.** It names live voice phishing, messaging app lures and unauthorized MFA reset requests[4].
- **Staff can report Teams calls as scams.** Since March 2026[18], with Defender for Office 365 Plan 1[2], in Microsoft 365 E3 since July[18].
- **The BSI issued an example management curriculum.** It fills 4 hours, or 3 with a pre-read, and suggests decisions within 2 to 6 weeks[7].
- **Pretexting is now a DBIR entry vector.** It started 6% of breaches; median clicks were 2% for simulated calls and texts, 1.4% for email[12].

What you can skip

- **Monthly email simulations and click-rate targets.** Click rates track the lure more than the staff[5]. Spend the time on call-back rules, as the endpoints and email sheet advises.
- **Tips for spotting typos.** AI makes phishing personalized and fluent[1].
- **Prizes for reporting.** A small prize didn't increase reporting[14]; feedback on each report did[13].
- **Exams for management.** Neither the BSIG nor the BSI requires one[8].

Mistakes that cost the most

- **Punishing clicks.** The NCSC says it starts to resemble entrapment, and that staff afraid for their jobs won't report mistakes[3].
- **Annual videos as the whole program.** Clicks didn't drop after them[5].
- **Training the help desk but not the process.** The DBIR says pretexting calls for business rules[12]. Give them a script and the right to refuse.
- **Sending only the IT lead to management training.** The BSI says it doesn't replace management's own[7].

What this looks like at your size

Small team, no security staff

- Turn on the Outlook Report button and answer each report the same day.
- Give every new hire one page with five rules.
- Under NIS2, book a half-day session for the managing directors and file the record.

Growing, with IT or security staff

- Turn on Teams call reporting; add short modules for finance, HR, help desk, admins and developers.
- Report the rate and speed of reports on real phishing monthly.
- Have an outsider call the help desk twice a year to test the reset script.
- In Germany, agree simulations and report data with the works council first[19].

Enterprise or regulated

- Map training to Regulation 2024/2690 or DORA and record effectiveness reviews.
- Hold a quarterly risk session with management, a format the BSI lists[8].

Version history

5 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which narrowed 14 statements, mostly from the field studies, to what the sources say.

Sources

1. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
2. User reported settings in Teams. Microsoft Learn, 5 Oct 2026. learn.microsoft.com
3. Phishing attacks: defending your organisation, version 2.0. NCSC (UK), reviewed 13 Feb 2024. ncsc.gov.uk
4. M-Trends 2026 Executive Edition. Google Cloud (Mandiant), Mar 2026. services.google.com
5. Understanding the Efficacy of Phishing Training in Practice (IEEE S&P 2025). UC San Diego, 2025. sysnet.ucsd.edu
6. BSI-Gesetz (BSIG), §§ 30 and 38. Federal Ministry of Justice (Germany), checked 5 Nov 2026. gesetze-im-internet.de
7. Curriculum für eine Geschäftsleitungsschulung nach NIS-2. BSI, 28 Oct 2026. bsi.bund.de
8. Schulung für Geschäftsleitungen (Handreichung), version 1.0. BSI, 17 Apr 2026. bsi.bund.de
9. Implementing Regulation (EU) 2024/2690, Article 1 and Annex point 8. EUR-Lex, 2024. eur-lex.europa.eu
10. Grundlegende Schulungen und Sensibilisierungsmaßnahmen (#nis2know). BSI, checked 5 Nov 2026. bsi.bund.de
11. Cyber security culture principles: Principle 6. NCSC (UK), 4 Jun 2025. ncsc.gov.uk
12. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
13. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study (IEEE S&P 2022). ETH Zurich, 14 Dec 2021. arxiv.org
14. Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training (ACM CCS 2024). ETH Zurich, 2 Sep 2024. arxiv.org
15. Directive (EU) 2022/2555 (NIS2), Articles 20 and 21. EUR-Lex, 2022. eur-lex.europa.eu
16. Regulation (EU) 2022/2554 (DORA), Articles 5 and 13. EUR-Lex, 2022. eur-lex.europa.eu
17. Manage external meetings and chat with people and organizations using Microsoft identities. Microsoft Learn, 19 Nov 2025. learn.microsoft.com
18. What's new in Microsoft Defender for Office 365. Microsoft Learn, 28 Oct 2026. learn.microsoft.com
19. Betriebsverfassungsgesetz (BetrVG), § 87. Federal Ministry of Justice (Germany), as amended 19 Jul 2024. gesetze-im-internet.de