



This is a translation for your convenience. Only the German version is legally binding. [Go to the German version](#)

Phishing training for the firm: decision paper

For the partners' meeting · As of 09.10.2026 · one page

Background

Our firm holds client data that have a market value for criminals: case files, payroll data with bank details, annual financial statements, access to professional portals. Almost every known incident at a law or tax firm began with an e-mail that someone took to be genuine. We are personally liable for confidentiality (§ 203 StGB (German Criminal Code), professional rules); in the event of a loss, the data protection supervisory authority, the professional indemnity insurer and the cyber insurer will ask what we did organisationally. Documented training of all employees is the answer to that question.

Proposal

All professionals and employees complete an online training course (around 45 minutes per person, in stages) followed by a phishing test in their own inbox. Provider: secureIT (Patrick Ihle, Ballrechten-Dottingen). No access to our systems, no installation, our IT service provider does not need to set anything up. Result: proof of training with a time stamp for the firm's records, a verifiable certificate per person, a data processing agreement (DPA).

Costs (one-off, net, no subscription)

FIRM SIZE	PRICE	INCLUDED
12 persons	€588	Training, phishing test, six months of monthly refreshers, proof of training and certificates. Repetition in the following year €22 per person.
25 persons	€1,225	
40 persons	€1,960	

Effort

- **Firm:** enter the team and activate the course, around one hour, can be delegated to the office management.
- **Each person:** around 45 minutes of online course, can be interrupted. The subsequent phishing test takes up no working time.
- **Time until proof is available:** typically one week.

What the test run delivers

- Awareness raising for all employees, documented with a time stamp
- Team rate of the phishing test, without names: nobody is singled out
- Call-back rule before bank transfers, reporting channel in case of suspicion
- Proof for the supervisory authority, liability insurer, cyber insurer, major clients

What it is not

- No substitute for encryption, backups and updates (IT service provider)
- No formal confidentiality undertaking by employees (we handle that ourselves)
- No recognised continuing professional education for professionals
- No legal advice

Proposed resolution

The partners resolve to have all professionals and employees of the firm complete the phishing training with test by _____. Responsible for the set-up: _____. The proof of training will be placed in the firm's records and presented to the insurance broker.

Resolved on _____ Signatures: _____

Check in advance: free self-test with three simulated phishing e-mails at secureit.icu/kostenlos-testen, sample proof of training at secureit.icu/beispiele, data processing agreement at secureit.icu/auftragsverarbeitung. Provider: secureIT UG (haftungsbeschränkt), Ballrechten-Dottingen. Prices net plus 19% VAT.

