



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

Phishing training and phishing test: what lies ahead for the teaching staff

Information for all teachers · version as of 09.10.2026

Over the next few weeks we will complete a short online training course on phishing and IT security together. Afterwards, three **simulated** phishing emails will arrive in our work mailboxes so that everyone can try out what they have learned at their own pace. This sheet explains what happens and what expressly does not happen.

Why are we doing this?

Schools are a popular target: fake emails from the “school authority”, supposed messages from the school management, a “Your password for the school portal is about to expire”. Technology catches a lot, but not everything. The rest is down to us. And anyone who can recognise phishing themselves can teach it convincingly to their class. The training fits the guiding perspective “Living and learning in a digitalised world” of the Baden-Württemberg curriculum.

How does it work?

- **Training first:** each person receives a personal link to the online course. It takes about 45 minutes, at your own pace, as working time.
- **Then the test:** after the course, three simulated phishing emails will arrive within a few weeks. They look real but are harmless.
- **If you click:** a page opens that explains how the fake could have been recognised. That’s it. A wrong click is a learning moment, not a mishap.
- **Certificate:** after the course and the test, you download your personal training certificate (person, topic, content, duration) for your professional development portfolio.

What happens

- The school management sees who has completed the course and how many have finished the test.
- You see your own result.
- Your name and work email address are stored for sending the emails and for the certificate, on servers in Germany.

What does not happen

- Nobody receives a list of who clicked.
- Nothing goes into your personnel file, official performance appraisals or performance reviews.
- No exposure in front of colleagues, no “rankings”.
- No monitoring of your other email traffic; no password is ever stored during the simulation.

What should I do if an email looks odd to me?

Exactly what would be right in a real attack too: don’t click, don’t reply, report it. How and to whom to report is explained in the course and applies to real emails just as it does to the test.

Questions? Contact person at the school: · Staff council (Personalrat):

The training and simulation are carried out by secureIT UG (haftungsbeschränkt) on behalf of the school, free of charge for schools. Further information on the procedure and data protection: secureit.icu/schulen/datenschutz

