



Phishing-Fortbildung und Phishing-Test: Was auf das Kollegium zukommt

Information für alle Lehrkräfte · Stand 03.10.2026

In den nächsten Wochen machen wir gemeinsam eine kurze Online-Fortbildung zu Phishing und IT-Sicherheit. Danach kommen drei **simulierte** Phishing-Mails ins dienstliche Postfach, damit jede und jeder das Gelernte in Ruhe ausprobieren kann. Dieses Blatt erklärt, was passiert und was ausdrücklich nicht passiert.

Warum machen wir das?

Schulen sind ein beliebtes Ziel: gefälschte Mails vom „Schulträger“, angebliche Nachrichten der Schulleitung, ein „Ihr Passwort für das Schulportal läuft ab“. Technik fängt vieles ab, aber nicht alles. Der Rest hängt an uns. Und wer Phishing selbst erkennt, kann es der Klasse glaubwürdig beibringen. Die Fortbildung passt zur Leitperspektive „Leben und Lernen in einer digitalisierten Welt“.

Wie läuft es ab?

- **Fortbildung zuerst:** Jede Person bekommt einen persönlichen Link zum Online-Kurs. Dauer etwa 45 Minuten, in eigenem Tempo, als Dienstzeit.
- **Dann der Test:** Nach dem Kurs treffen innerhalb einiger Wochen drei simulierte Phishing-Mails ein. Sie sehen echt aus, sind aber harmlos.
- **Falls Sie klicken:** Es öffnet sich eine Erklärungsseite, die zeigt, woran man die Fälschung hätte erkennen können. Das war's. Ein Fehlklick ist ein Lernmoment, keine Panne.
- **Bescheinigung:** Nach Kurs und Test laden Sie sich Ihre persönliche Fortbildungsbescheinigung herunter (Person, Thema, Inhalt, Dauer), für das Qualifizierungsportfolio.

Das passiert

- Die Schulleitung sieht, wer den Kurs abgeschlossen hat, und wie viele den Test beendet haben.
- Sie selbst sehen Ihr eigenes Ergebnis.
- Ihr Name und Ihre dienstliche E-Mail-Adresse werden für den Versand und die Bescheinigung gespeichert, auf Servern in Deutschland.

Das passiert nicht

- Niemand bekommt eine Liste, wer geklickt hat.
- Nichts wandert in die Personalakte, in dienstliche Beurteilungen oder Gespräche über Leistung.
- Keine Bloßstellung im Kollegium, keine „Ranglisten“.
- Keine Überwachung Ihres sonstigen E-Mail-Verkehrs; bei der Simulation wird nie ein Passwort gespeichert.

Was soll ich tun, wenn mir eine Mail komisch vorkommt?

Genau das, was auch bei einem echten Angriff richtig wäre: nicht klicken, nicht antworten, melden. Wie und an wen gemeldet wird, steht im Kurs und gilt für echte Mails genauso wie für den Test.

Fragen? Ansprechpartner in der Schule: · Personalrat:

Fortbildung und Simulation werden von secureIT UG (haftungsbeschränkt) im Auftrag der Schule durchgeführt, für Schulen kostenlos. Weitere Informationen zu Ablauf und Datenschutz: secureit.icu/schulen/datenschutz

