secureIT
Daten und User schützen. Mit Sicherheit.

Phishing-Schulung und Phishing-Test: Was auf uns zukommt

Information für alle Beschäftigten · Stand 01.11.2026

In den nächsten Wochen machen wir gemeinsam eine kurze Online-Schulung zu Phishing und IT-Sicherheit. Danach kommen ein paar **simulierte** Phishing-Mails ins 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?

Phishing ist der häufigste Weg, über den Betriebe angegriffen werden: eine gefälschte Rechnung, eine angebliche Chef-Nachricht, ein „Ihr Passwort läuft ab". Technik fängt vieles ab, aber nicht alles. Der Rest hängt an uns. Außerdem verlangen Versicherer und Auftraggeber einen Nachweis, dass wir geschult sind.

Wie läuft es ab?

- **Schulung zuerst:** Jede Person bekommt einen Link zum Online-Kurs. Dauer etwa eine Stunde, in eigenem Tempo, während der Arbeitszeit.
- **Dann der Test:** Nach der Schulung treffen innerhalb einiger Wochen ein paar 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.
- **Zertifikat:** Nach Schulung und Phishing-Test erhalten Sie ein persönliches Teilnahmezertifikat.

Das passiert	Das passiert nicht
• Die Leitung sieht, wer die Schulung abgeschlossen hat, und Zahlen ohne Namen für das Team („15 von 20 haben nicht geklickt"). • Sie selbst sehen Ihr eigenes Ergebnis. • Ihr Name und Ihre dienstliche E-Mail-Adresse werden für den Versand und den Schulungsnachweis gespeichert, auf Servern in Deutschland. Nur bei Test-Mails mit Sprachnachricht gehen Vorname und E-Mail-Adresse an einen Sprachdienst in den USA. • Gespeichert wird auch, ob Sie eine Test-Mail geöffnet oder angeklickt und auf der Übungsseite etwas eingegeben haben, mit technischen Daten wie IP-Adresse und Browser. Eingegebene Passwörter werden nicht gespeichert.	• Niemand bekommt eine Liste, wer geklickt hat. • Nichts wandert in die Personalakte, in Beurteilungen oder Gespräche über Leistung. • Keine Bloßstellung vor Kolleginnen und Kollegen, keine „Ranglisten". • Keine Überwachung Ihres sonstigen E-Mail-Verkehrs.

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 in der Schulung und gilt für echte Mails genauso wie für den Test.

Fragen? Ansprechpartner im Betrieb: · Betriebsrat:

Schulung und Simulation werden von secureIT UG (haftungsbeschränkt) im Auftrag des Betriebs durchgeführt. Weitere Informationen zu Ablauf und Datenschutz: secureit.icu/fuer-betriebsraete

secureIT
Daten und User schützen. Mit Sicherheit.