



Cette traduction est fournie à titre indicatif. Seule la version allemande fait foi. [Voir la version allemande](#)

Formation au phishing et test de phishing : ce qui attend l'équipe enseignante

Information pour tous les enseignants · Version du 09.10.2026

Au cours des prochaines semaines, nous suivrons ensemble une courte formation en ligne sur le phishing et la sécurité informatique. Ensuite, trois e-mails de phishing **simulés** arriveront dans la boîte de messagerie professionnelle, afin que chacune et chacun puisse mettre en pratique sereinement ce qui a été appris. Cette fiche explique ce qui se passe et ce qui, expressément, ne se passe pas.

Pourquoi faisons-nous cela ?

Les écoles sont une cible prisée : faux e-mails de l'« organisme gestionnaire de l'école » (Schulträger), prétendus messages de la direction de l'établissement, un « Votre mot de passe pour le portail scolaire expire ». La technique intercepte beaucoup de choses, mais pas tout. Le reste dépend de nous. Et qui reconnaît lui-même le phishing peut l'enseigner de manière crédible à sa classe. La formation s'inscrit dans la perspective directrice « Vivre et apprendre dans un monde numérisé ».

Comment cela se déroule-t-il ?

- **D'abord la formation** : chaque personne reçoit un lien personnel vers le cours en ligne. Durée d'environ 45 minutes, à son propre rythme, sur le temps de service.
- **Ensuite le test** : après le cours, trois e-mails de phishing simulés arrivent dans un délai de quelques semaines. Ils ont l'air authentiques, mais sont inoffensifs.
- **Si vous cliquez** : une page explicative s'ouvre et montre à quoi on aurait pu reconnaître la falsification. C'est tout. Un clic malheureux est un moment d'apprentissage, pas un incident.
- **Attestation** : après le cours et le test, vous téléchargez votre attestation de formation personnelle (personne, thème, contenu, durée) pour votre portfolio de qualification.

Ce qui se passe

- La direction de l'établissement voit qui a terminé le cours et combien de personnes ont terminé le test.
- Vous voyez vous-même votre propre résultat.
- Votre nom et votre adresse e-mail professionnelle sont enregistrés pour l'envoi et l'attestation, sur des serveurs en Allemagne.

Ce qui ne se passe pas

- Personne ne reçoit de liste de qui a cliqué.
- Rien n'est versé au dossier personnel, ni dans les évaluations professionnelles ou les entretiens sur la performance.
- Aucune mise au pilori au sein de l'équipe enseignante, aucun « classement ».
- Aucune surveillance de vos autres échanges d'e-mails ; lors de la simulation, aucun mot de passe n'est jamais enregistré.

Que dois-je faire si un e-mail me semble bizarre ?

Exactement ce qui serait juste en cas d'attaque réelle : ne pas cliquer, ne pas répondre, signaler. La manière de signaler et le destinataire du signalement sont indiqués dans le cours et valent aussi bien pour les e-mails réels que pour le test.

Des questions ? Interlocuteur à l'école : · Conseil du personnel (Personalrat) :

La formation et la simulation sont réalisées par secureIT UG (haftungsbeschränkt) pour le compte de l'école, gratuitement pour les écoles. Plus d'informations sur le déroulement et la protection des données : secureit.icu/schulen/datenschutz

