



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

Formation et test de phishing : ce qui nous attend

Information à l'attention de tous les salariés · Version du 09.10.2026

Dans les semaines à venir, nous suivrons ensemble une courte formation en ligne sur le phishing et la sécurité informatique. Ensuite, quelques e-mails de phishing **simulés** arriveront dans les boîtes de réception, afin que chacun puisse mettre en pratique ce qu'il a appris, en toute tranquillité. Cette fiche explique ce qui se passe et ce qui, expressément, ne se passe pas.

Pourquoi le faisons-nous ?

Le phishing est la voie d'attaque la plus fréquente contre les entreprises : une fausse facture, un prétendu message du patron, un « Votre mot de passe expire ». La technique en intercepte beaucoup, mais pas tout. Le reste dépend de nous. Par ailleurs, les assureurs et les donneurs d'ordre exigent une attestation prouvant que nous sommes formés.

Comment cela se déroule-t-il ?

- **D'abord la formation** : chaque personne reçoit un lien vers le cours en ligne. Durée : environ une heure, à son propre rythme, pendant le temps de travail.
- **Ensuite le test** : après la formation, quelques e-mails de phishing simulés arrivent au cours des semaines suivantes. Ils ont l'air authentiques, mais sont inoffensifs.
- **Si vous cliquez** : une page d'explication s'ouvre et montre à quels indices on aurait pu reconnaître la contrefaçon. C'est tout. Un clic malheureux est une occasion d'apprendre, pas un incident.
- **Certificat** : à l'issue de la formation, vous recevez un certificat de participation personnel.

Ce qui se passe

- La direction voit un taux pour l'équipe (« 12 sur 20 ont signalé la contrefaçon »).
- Vous voyez vous-même votre propre résultat.
- Votre nom et votre adresse e-mail professionnelle sont enregistrés pour l'envoi et pour l'attestation de formation, sur des serveurs situés en Allemagne.

Ce qui ne se passe pas

- Personne ne reçoit de liste indiquant qui a cliqué.
- Rien n'est versé au dossier personnel, ni utilisé dans les évaluations ou les entretiens sur la performance.
- Aucune mise au pilori devant les collègues, aucun « classement ».
- Aucune surveillance du reste de votre correspondance électronique.

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

Exactement ce qui serait juste lors d'une véritable attaque : ne pas cliquer, ne pas répondre, signaler. Comment et à qui signaler est expliqué dans la formation et vaut aussi bien pour les vrais e-mails que pour le test.

Des questions ? Interlocuteur dans l'entreprise : · Comité social et économique (CSE) :

La formation et la simulation sont réalisées par secureIT UG (haftungsbeschränkt) pour le compte de l'entreprise. Plus d'informations sur le déroulement et la protection des données : secureit.icu/fuer-betriebsraete

