



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

Formation au phishing pour le cabinet : note de décision

Pour la réunion des associés · Version du 09.10.2026 · une page

Situation de départ

Notre cabinet conserve des données de clients qui ont une valeur marchande pour les criminels : dossiers, données de paie avec coordonnées bancaires, comptes annuels, accès aux portails professionnels. Presque chaque incident connu dans un cabinet a commencé par un e-mail qu'une personne a pris pour authentique. Nous sommes personnellement responsables du secret professionnel (§ 203 StGB (Code pénal allemand), droit de la profession) ; en cas de sinistre, l'autorité de contrôle de la protection des données, l'assurance responsabilité civile professionnelle et l'assureur cyber demandent ce que nous avons fait sur le plan organisationnel. Une formation documentée de tous les collaborateurs est la réponse à cette question.

Proposition

Tous les professionnels et collaborateurs suivent une formation en ligne (environ 45 minutes par personne, en plusieurs étapes), suivie d'un test de phishing dans leur propre boîte de réception. Prestataire : secureIT (Patrick Ihle, Ballrechten-Dottingen). Aucun accès à nos systèmes, aucune installation, le prestataire informatique n'a rien à configurer. Résultat : attestation de formation horodatée pour le dossier du cabinet, certificat vérifiable pour chaque personne, accord de sous-traitance (DPA).

Coûts (paiement unique, HT, sans abonnement)

TAILLE DU CABINET	PRIX	INCLUS
12 personnes	588 €	Formation, test de phishing, six mois de rappels mensuels, attestation et certificats. Renouvellement l'année suivante : 22 € par personne.
25 personnes	1 225 €	
40 personnes	1 960 €	

Charge de travail

- **Cabinet** : enregistrer l'équipe et activer le cours, environ une heure, délégable à la gestion du cabinet.
- **Chaque personne** : environ 45 minutes de cours en ligne, interruptible. Le test de phishing qui suit ne coûte pas de temps de travail.
- **Délai jusqu'à l'attestation** : généralement une semaine.

Ce qu'apporte la campagne

- Sensibilisation de tous les collaborateurs, documentée avec horodatage
- Taux d'équipe du test de phishing, sans noms : personne n'est mis au pilori
- Règle du rappel avant les virements, procédure de signalement en cas de soupçon
- Attestation pour l'autorité de contrôle, l'assurance responsabilité civile, l'assureur cyber, les grands clients

Ce qu'elle n'est pas

- Pas un substitut au chiffrement, aux sauvegardes et aux mises à jour (prestataire informatique)
- Pas un engagement formel de confidentialité des collaborateurs (nous nous en chargeons nous-mêmes)
- Pas une formation continue professionnelle reconnue pour les professionnels
- Pas un conseil juridique

Proposition de décision

Les associés décident que tous les professionnels et collaborateurs du cabinet suivront la formation au phishing avec test d'ici le _____. Responsable de la mise en place : _____. L'attestation est versée au dossier du cabinet et présentée au courtier en assurances.

Décidé le _____ Signatures : _____

À vérifier au préalable : autotest gratuit avec trois e-mails de phishing simulés sur [secureit.icu/kostenlos-testen](#), modèle d'attestation sur [secureit.icu/beispiele](#), accord de sous-traitance sur [secureit.icu/auftragsverarbeitung](#). Prestataire : secureIT UG (haftungsbeschränkt), Ballrechten-Dottingen.





secureIT

Daten und User schützen. Mit Sicherheit.

Prix HT, plus 19 % de TVA.



secureIT

Daten und User schützen. Mit Sicherheit.