

Fiche réflexe contre l'hameçonnage

Pour les salariés : examiner les messages suspects, signaler sans risque et réagir rapidement après une erreur possible. Avant diffusion, l'informatique ou la sécurité doit compléter les canaux de signalement internes.

Avant de cliquer

Demande inattendue, urgence, nouvelles coordonnées bancaires ou demande d'identifiants ? Faites une pause. Une adresse connue et une rédaction soignée ne prouvent pas l'authenticité.

Vérifiez auprès d'un contact connu ou dans une application officielle ouverte par vos soins. N'utilisez ni le numéro, ni la fonction de réponse, ni le lien de connexion du message suspect.

N'ouvrez pas les liens, pièces jointes ou destinations des codes QR pour les essayer. Ne communiquez jamais de mot de passe ni de code MFA ; refusez les demandes MFA inattendues.

Signaler le soupçon en interne

Utilisez le bouton de signalement autorisé ou le contact informatique convenu. Indiquez l'heure, le service touché et vos actions. Conservez ou transmettez le message selon les instructions internes ; ne le diffusez pas aux collègues. Ne dialoguez pas avec l'expéditeur.

Si vous avez déjà agi

Situation	Que faire maintenant
Lien ouvert	Cessez toute interaction, ne saisissez plus rien et prévenez rapidement l'informatique. Un clic seul ne prouve pas une infection ; l'informatique évalue la situation.
Mot de passe saisi ou MFA approuvée	Prévenez immédiatement l'informatique. Modifiez les mots de passe concernés par une voie connue, sur un appareil fiable, y compris les mots de passe réutilisés. Faites vérifier et révoquer les sessions ou accès actifs si nécessaire.
Fichier ouvert ou argent envoyé	Contactez immédiatement l'informatique et suivez ses consignes pour l'appareil. Ne tentez pas de nettoyage et n'effacez aucune preuve. Pour un paiement, contactez aussi la finance et la banque via leurs coordonnées connues.

Contact / bouton de signalement : _____

Contact de secours et téléphone : _____

Signalement interne d'hameçonnage

Cette fiche facilite la transmission à l'informatique. Signalez immédiatement les cas urgents par le canal convenu ; n'attendez pas que tous les champs soient remplis.

Champ	Vos informations
Heure et coordonnées pour vous rappeler	
Canal et expéditeur affiché	
Objet ou brève description	
Compte ou appareil concerné	
Actions effectuées et heures	
Effets ou alertes observés	
Contact déjà prévenu et référence du dossier	

Ne saisissez ni mots de passe, ni codes MFA, ni dossiers clients complets. Transmettez les messages originaux et les pièces jointes uniquement par la voie autorisée par l'informatique.

Exemple de signalement bref

Exemple fictif : « 09 h 15, courriel prétendant venir d'un fournisseur et demandant de changer ses coordonnées bancaires. Je l'ai lu, sans ouvrir de lien ni effectuer de paiement. Merci de vérifier. Vous pouvez me joindre par mon contact professionnel interne. »

Adapter et partager

Modèle original de Paragamix GmbH. Utilisation interne, adaptation et partage avec les clients gratuits. Complétez et vérifiez les contacts et procédures internes avant utilisation. Un lien vers la source est apprécié, sans être obligatoire.

[NIST sur l'hameçonnage \(anglais\)](#) | [Guide d'intervention BSI CSN \(allemand\)](#)

[Version actuelle et outils](#)