Reconnaître
une arnaque en ligne

"Votre colis est bloqué." "Votre compte a été suspendu." "Vous avez gagné un iPhone." Ces messages ont l'air vrais. Ils ne le sont pas. Le phishing est la technique numéro 1 des pirates — et ça marche, parce que c'est de mieux en mieux imité. Voici comment les démasquer.

01 Repérer les signes d'un faux message

Les arnaques par email ou SMS (appelées phishing) cherchent à vous faire cliquer sur un lien ou à vous faire communiquer des informations personnelles. Elles imitent des organismes connus : banques, La Poste, impôts, Ameli, Netflix...

Les signaux d'alarme :
Un sentiment d'urgence : "Agissez maintenant", "Votre compte sera fermé dans 24h", "Dernière chance". La pression est volontaire — elle vous empêche de réfléchir.
Une demande d'informations sensibles : mot de passe, numéro de carte bancaire, code de sécurité. Aucun organisme sérieux ne vous demandera ça par email ou SMS.
Des fautes d'orthographe ou un style bizarre : traduction automatique approximative, formules étranges, mise en page bâclée.

Le test infaillible :
Posez-vous la question : *est-ce que j'attendais ce message ?* Si la réponse est non — livraison surprise, remboursement inattendu, alerte de sécurité — méfiez-vous immédiatement.

Attention : Un vrai organisme (banque, impôts, Ameli, La Poste) ne vous demandera jamais vos informations sensibles par email ou SMS. Jamais.

02 Vérifier les liens et l'expéditeur

L'adresse email et le lien dans le message sont les deux endroits où les arnaques se trahissent le plus facilement. Prenez 10 secondes pour les regarder.

L'adresse de l'expéditeur :
Cliquez sur le nom de l'expéditeur pour voir l'adresse email complète. Un email de votre banque vient de **@nomdelabanque.fr** — pas de **@gmail.com**, pas de **@orange-remboursement.com**, pas d'un nom avec des chiffres aléatoires.

Le lien dans le message :
Avant de cliquer, **passez votre souris sur le lien** sans cliquer (sur PC). L'adresse réelle s'affiche en bas de l'écran. Si le message prétend venir de La Poste mais que le lien pointe vers **laposte-livraison-colis.ru** ou une adresse bizarre — c'est une arnaque. Sur téléphone : appuyez longuement sur le lien pour voir l'adresse complète.

Bon à savoir : En cas de doute, ne cliquez pas sur le lien du message. Allez directement sur le site officiel en tapant vous-même l'adresse dans votre navigateur.

03 Les bons réflexes si vous avez cliqué

Ça arrive aux meilleurs. Si vous avez cliqué sur un lien douteux ou entré des informations, voici quoi faire dans l'ordre, sans paniquer.

Vous avez cliqué mais rien saisi :
Fermez la page immédiatement. Lancez une analyse antivirus. Dans la majorité des cas, cliquer sans rien saisir ne suffit pas à infecter votre PC.

Vous avez saisi un mot de passe :
Changez ce mot de passe immédiatement sur le vrai site. Si vous utilisez ce même mot de passe ailleurs, changez-le partout. Activez la double authentification sur le compte concerné.

Vous avez donné vos coordonnées bancaires :
Appelez votre banque **immédiatement** pour faire opposition. Signalez l'arnaque sur **cybermalveillance.gouv.fr** — le site officiel du gouvernement français pour les victimes de cyberattaques.

Bon à savoir : Signalez les faux emails à **signalement.signal-spam.fr** et les faux SMS au **33700** (transfert du message). Vous aidez à protéger les autres utilisateurs.

Vous avez reçu un message suspect ou vous avez un doute ?
Envoyez-nous une capture d'écran — on vous dit si c'est une arnaque.
Appelez-nous : 09.81.65.35.09