

RECONNAÎTRE LES ARNAQUES EN LIGNE

La brigade des arnaques

Le point commun de toutes les arnaques

On joue sur vos émotions (peur, urgence, envie, amour) pour vous faire agir sans réfléchir, et vous soutirer de l'argent ou des informations. Repérer le piège, c'est déjà l'éviter.

Les six arnaques à connaître

 **Le phishing.** Un faux message imite un tiers de confiance (banque, administration, commerçant) pour vous soutirer vos informations. Il arrive par mail, mais aussi par SMS (le « smishing ») ou par QR code (le « quishing »), joue sur l'urgence et contient un lien piégé. → Ne cliquez pas sur le lien, allez vous-même sur le site officiel en tapant son adresse.

 **Le piratage de compte.** Un mot de passe qui a fuité lors du piratage d'un site permet de prendre le contrôle de vos comptes, surtout si vous utilisez le même partout. Les signes : vous n'arrivez plus à vous connecter, ou vos proches reçoivent des messages que vous n'avez pas envoyés. → Un mot de passe différent par compte important, et la double authentification quand c'est possible.

 **L'arnaque aux sentiments.** Un escroc crée une fausse relation amoureuse pour vous soutirer de l'argent, aujourd'hui parfois avec des photos ou une voix fabriquées par intelligence artificielle. Il trouve toujours une excuse pour ne jamais vous rencontrer et cherche à vous éloigner de vos proches. → N'envoyez jamais d'argent à quelqu'un que vous n'avez pas rencontré en vrai, et parlez-en à un proche.

 **Le faux placement.** Une promesse d'argent facile habillée en vraie information : fausse publicité, faux article de presse, faux témoignages. On repère le « rendement garanti », la pression des « places limitées », puis la demande d'argent ou de papiers d'identité. → Sans risque et à fort rendement, ça n'existe pas : recoupez toujours l'information sur une source officielle.



Le faux conseiller bancaire. Un faux appel de votre banque prétend qu'une fraude est en cours pour vous faire valider des opérations ou livrer vos codes. Piège récent : l'escroc sait faire afficher le vrai numéro et le vrai nom de votre banque sur votre écran. → Raccrochez et appelez vous-même le numéro figurant au dos de votre carte.



Le faux support technique. Une fausse panne (fenêtre qui bloque l'écran, appel, mail) pour vous faire payer un faux dépannage ou prendre la main sur votre appareil. La même ruse sert de faux service après-vente avec de faux remboursements. → Ne rappelez pas le numéro affiché, n'installez aucun logiciel à distance, éteignez puis rallumez.



Les réflexes à retenir

1. Je ne donne jamais mes mots de passe ni mes codes bancaires, par mail, téléphone ou message.
2. Je ne clique pas dans l'urgence : je vais moi-même sur le site officiel.
3. J'utilise un mot de passe différent pour chaque compte important.
4. Une promesse trop belle cache une arnaque : je recoupe l'information avant d'y croire.
5. Ce qui s'affiche peut être faux (un nom, un numéro, une alerte) : dans le doute, je vérifie autrement.
6. En cas de doute ou de problème, je ne reste pas seul : je demande de l'aide.



Pour aller plus loin et se faire aider

- 17Cyber : le premier réflexe en cas de problème, vous décrivez votre situation et vous êtes orienté (cherchez « 17Cyber »).
- cybermalveillance.gouv.fr : conseils et fiches pratiques sur toutes les arnaques.
- Info Escroqueries : pour être conseillé par téléphone, 0 805 805 817 (gratuit).
- 33700 : pour signaler un SMS frauduleux (transférez-le au 33700).
- signal.conso.gouv.fr : pour signaler une arnaque à la consommation ou un site douteux.
- Une médiatrice numérique près de chez vous, pour un accompagnement gratuit (cartographie.societenumerique.gouv.fr).