

Arnaques et deepfakes

Les reconnaître sans paniquer.

Le bon réflexe en 3 étapes

STOPPER · VÉRIFIER · SIGNALER

COMPRENDRE

Une apparence crédible ne prouve rien.

L'IA permet aujourd'hui d'imiter une voix, une image ou un style d'écriture. Elle peut rendre une arnaque plus convaincante, mais elle ne rend pas la demande vraie.

Un deepfake, c'est quoi ?

Un contenu créé ou modifié par ordinateur pour faire croire qu'une personne a parlé, écrit ou agi. La voix de votre proche, un faux journaliste, une vidéo de personnalité : tous peuvent être imités.

LES SITUATIONS LES PLUS FRÉQUENTES

1

Le faux proche

Un appel ou un message urgent : « J'ai un problème, envoie de l'argent et n'en parle à personne. »

2

Le faux service

Banque, livraison, impôts ou support informatique : on vous pousse à cliquer, rappeler ou donner un code.

3

La fausse vidéo

Une personnalité semble recommander un placement, un produit miracle ou une méthode pour gagner de l'argent.

À retenir

Un appel qui vous surprend ou vous fait peur mérite une pause. Ne décidez jamais pendant l'appel ou juste après le message.

REPÉRER

Les 7 signaux d'alerte

Un seul signe ne suffit pas toujours. Plusieurs signes ensemble doivent vous faire ralentir.

1. L'urgence

« Tout de suite », « avant ce soir », « sinon vous perdez... »

2. Le secret

On vous demande de ne parler à personne ou de sortir de l'application habituelle.

3. Un code demandé

Votre banque, un proche ou une administration ne doit pas vous faire transmettre un code de sécurité.

4. Un nouveau lien

L'adresse est inhabituelle, abrégée ou comporte une petite faute.

5. Un paiement différent

Nouveau RIB, carte cadeau, cryptoactifs ou virement « exceptionnel ».

6. Une voix presque juste

Le son est étrange, le message reste vague, l'interlocuteur évite les questions simples.

7. Une offre incroyable

Gain facile, remboursement inattendu ou produit exceptionnel : vérifiez ailleurs.

Le test le plus simple

Raccrochez. Fermez le message. Puis contactez vous-même la personne ou le service avec un numéro ou un site que vous connaissez déjà.

RÉAGIR

Le réflexe : 3 étapes, dans cet ordre

Même si vous n'êtes pas certain qu'il s'agit d'une arnaque, ces gestes ne vous feront rien perdre.

1**STOPPER**

Ne cliquez plus, ne répondez plus, ne communiquez aucun code. Ne payez pas et n'installez aucun logiciel.

2**VÉRIFIER**

Appelez la personne ou l'organisme par un numéro trouvé sur son site officiel, un relevé ou votre carte bancaire. Ne rappelez pas le numéro reçu.

3**SIGNALER**

Gardez captures, adresse du site, numéro et preuve de paiement. Contactez votre banque sans attendre si vos données bancaires ont été données.

Pour aller plus loin

Conseils et assistance : cybermalveillance.gouv.fr. Informations et signalements officiels : service-public.fr. En cas de danger immédiat, appelez les secours adaptés à la situation.

Votre avis compte Ce guide vous a aidé ? Dites-nous ce qui était clair ou manquait sur lia-cest-simple.fr/avis.