

Gratuit · 8 erreurs + vos réflexes · concret, sans jargon

Les 8 erreurs qui mènent au vol de votre identité

Usurpation, comptes vidés, crédits ouverts en votre nom : presque toujours, tout part d'une de ces 8 erreurs. La bonne nouvelle, c'est qu'elles s'évitent en quelques gestes.



Pourquoi ce guide

En France, l'usurpation d'identité touche environ 210 000 personnes par an, et les arnaques en ligne explosent. Le point commun de la plupart des victimes : une faille évitable.

Vous n'êtes pas une cible « parce que vous êtes important ». Les attaques sont automatisées et massives : elles testent des millions de personnes au hasard. Ce qui fait la différence, ce sont vos **réflexes**.

Ce guide est en trois temps :

1. Les 8 erreurs

Les pièges qui ouvrent la porte, du plus dangereux au plus sournois. Pour chacun : le risque, le signal d'alarme, la parade.

2. Détecter & réagir

Comment savoir si on vous a déjà piraté, et les premiers gestes si c'est le cas.

3. Vos réflexes

Les bonnes habitudes au quotidien, et un mini-glossaire pour ne plus être perdu.

1**Réutiliser le même mot de passe partout****CE QUE ÇA PEUT COÛTER**

Une seule fuite (un site piraté parmi des centaines) suffit : les pirates testent ensuite votre couple email + mot de passe sur votre banque, vos mails, vos réseaux. En cascade, tout tombe.

LE SIGNAL D'ALARME

Vous seriez incapable de dire combien de comptes partagent ce mot de passe.

LA PARADE

Un mot de passe unique par compte, généré au hasard et retenu par un gestionnaire. Vous ne mémorisez qu'un seul mot de passe maître.

2**Ne pas activer la double authentification****CE QUE ÇA PEUT COÛTER**

Sans elle, un mot de passe volé = accès direct. Avec elle, le pirate est bloqué même s'il a votre mot de passe. La protection la plus rentable, et trop souvent ignorée.

LE SIGNAL D'ALARME

Vous vous connectez à votre banque ou vos mails avec seulement un mot de passe.

LA PARADE

Activez-la en priorité sur votre boîte mail et votre banque. Préférez une application d'authentification au SMS.

3**Cliquer sur les liens des SMS et mails****CE QUE ÇA PEUT COÛTER**

Le faux SMS de colis, le faux mail de banque : un clic, un faux site, et vous livrez vous-même vos identifiants ou votre carte. La porte d'entrée numéro un des piratages.

LE SIGNAL D'ALARME

Un message crée l'urgence (« compte bloqué », « colis en attente ») et vous pousse à cliquer tout de suite.

LA PARADE

Ne cliquez jamais le lien. Allez sur le site officiel vous-même. Aucune banque ne demande vos codes par message.

4**Exposer trop d'informations personnelles****CE QUE ÇA PEUT COÛTER**

Date de naissance, adresse, nom de jeune fille, photos de documents : ce sont les briques exactes dont un escroc a besoin pour usurper votre identité.

LE SIGNAL D'ALARME

Vos profils sont publics, on peut reconstituer votre vie en quelques clics.

LA PARADE

Passez vos comptes en privé, limitez les infos visibles, et ne publiez jamais de photo de pièce d'identité.

5**Laisser ses appareils sans verrou ni mises à jour****CE QUE ÇA PEUT COÛTER**

Un téléphone volé non verrouillé, c'est l'accès à vos mails, donc à la réinitialisation de tous vos comptes. Un appareil non mis à jour, c'est une faille connue grande ouverte.

LE SIGNAL D'ALARME

Pas de code de verrouillage, des mises à jour repoussées depuis des mois.

LA PARADE

Code + biométrie sur chaque appareil, mises à jour automatiques, et la localisation/effacement à distance prêts en cas de vol.

6**Saisir sa carte sur n'importe quel site****CE QUE ÇA PEUT COÛTER**

Un faux site ou un marchand peu sûr, et votre numéro de carte est capturé puis revendu. S'ensuivent débits frauduleux et abonnements cachés.

LE SIGNAL D'ALARME

Vous payez sur un site inconnu trouvé via une pub, sans vérifier.

LA PARADE

Vérifiez le site, payez par carte (contestable) plutôt que par virement, et utilisez une carte virtuelle pour les sites inconnus.

7 Laisser traîner ses vieux comptes et ses données

CE QUE ÇA PEUT COÛTER

Chaque vieux compte oublié est une porte ouverte : s'il fuit, vos données (et un mot de passe peut-être réutilisé) se retrouvent en vente. Vos coordonnées circulent aussi chez les courtiers en données.

LE SIGNAL D'ALARME

Des dizaines de comptes créés « pour une fois » et jamais fermés. Vous recevez du spam très ciblé.

LA PARADE

Supprimez les comptes inutiles, vérifiez si votre email a fuité, et faites retirer vos données des courtiers.

8 Croire que « ça n'arrive qu'aux autres »

CE QUE ÇA PEUT COÛTER

L'erreur qui aggrave toutes les autres : sans réflexe, on réagit trop tard. Or en cas de fraude, chaque heure compte (opposition, plainte, blocage).

LE SIGNAL D'ALARME

Vous ne sauriez pas quoi faire, ni qui appeler, si votre compte était piraté demain.

LA PARADE

Sachez où trouver de l'aide (17Cyber, cybermalveillance.gouv.fr) et gardez le réflexe : agir vite, sans paniquer, dans le bon ordre.

Comment savoir si on vous a déjà piraté ?

Cinq signaux qui doivent vous alerter. Au moindre doute, changez le mot de passe concerné et activez la double authentification.

Les signaux côté comptes

- Vous ne pouvez plus vous connecter, ou votre mot de passe a « changé » seul.
- Des connexions depuis des lieux/ appareils inconnus dans l'historique.
- Vos proches reçoivent des messages bizarres « de votre part ».
- Des mails de « réinitialisation » que vous n'avez pas demandés.

Les signaux côté argent & appareils

- Des débits ou des commandes que vous ne reconnaissez pas.
- Votre téléphone perd le réseau sans raison (détournement de SIM).
- Pubs intempestives, apps inconnues, batterie qui fond.
- Un courrier pour un crédit ou abonnement que vous n'avez jamais ouvert.

Le réflexe : vérifiez régulièrement si votre adresse email apparaît dans une fuite connue. C'est le meilleur signal d'alerte précoce, et c'est gratuit sur cybercarapace.fr.

Si c'est déjà arrivé : les 4 premiers gestes

Dans l'ordre, et sans paniquer. Plus vous agissez vite, plus vous limitez les dégâts.

1 Reprenez la main sur l'email

C'est la clé de tous vos comptes. Récupérez l'accès, changez le mot de passe, déconnectez les sessions, et supprimez tout transfert/règle ajouté par le pirate.

2 Bloquez l'argent

En cas de paiement suspect : faites opposition auprès de votre banque et contestez par écrit. Le remboursement est la règle en cas de fraude signalée à temps.

3 Changez les mots de passe réutilisés

Partout où le mot de passe compromis servait. Activez la double authentification au passage.

4 Signalez et faites-vous aider

Rendez-vous sur 17cyber.gouv.fr (diagnostic + chat police/gendarmerie, 24h/24) et cybermalveillance.gouv.fr. Déposez plainte si nécessaire. Ces services publics sont gratuits.

Vos réflexes au quotidien

À faire une fois

- Installer un gestionnaire de mots de passe.
- Activer la double authentification sur l'email, la banque, les réseaux.
- Verrouiller et mettre à jour tous les appareils.
- Passer ses comptes sociaux en privé.

À garder en tête

- Urgence + lien reçu = on ne clique pas, on vérifie soi-même.
- Jamais de code ni de cryptogramme communiqué par téléphone.
- Payer par carte (contestable), jamais par virement à un inconnu.
- Vérifier ses fuites tous les quelques mois.

Mini-glossaire

Phishing (hameçonnage) : un faux message qui imite un organisme de confiance pour vous voler vos identifiants ou votre argent.

Double authentification (2FA) : un second code en plus du mot de passe : sans lui, impossible de se connecter.

Gestionnaire de mots de passe : un coffre chiffré qui crée et retient un mot de passe unique par compte à votre place.

Passkey (clé d'accès) : une connexion sans mot de passe, validée par votre empreinte ou votre visage, insensible au phishing.

VPN : il chiffre votre connexion et masque votre adresse IP, utile surtout sur les Wi-Fi publics.

Votre plan en 6 gestes

Faites-en un par soir : en moins d'une semaine, vous aurez corrigé l'essentiel.

- ☐ Installer un gestionnaire et mettre des mots de passe uniques sur l'email et la banque
- ☐ Activer la double authentification sur l'email, la banque et les réseaux
- ☐ Mettre à jour et verrouiller tous vos appareils
- ☐ Vérifier si votre adresse email a déjà fuité
- ☐ Passer vos réseaux sociaux en privé et limiter les infos publiques
- ☐ Repérer un faux message : urgence + lien = on ne clique pas

Allez plus loin, gratuitement

Mesurez votre niveau avec le Score Carapace, générez des mots de passe solides, testez votre flair anti-arnaque.

cybercarapace.fr

Information générale, sans conseil personnalisé. En cas de piratage avéré, les services publics gratuits cybermalveillance.gouv.fr et 17cyber.gouv.fr accompagnent les victimes. Cybercarapace est un guide indépendant : nous informons, comparons et vous orientons.