



Smartphone et sécurité

Les pièges d'aujourd'hui et les bons réflexes

[Reconnaitre piratage](#)



Ça n'arrive pas qu'aux autres !

504 000

Demandes d'assistance sur
17cyber.gouv.fr en 2025 (+20 %)

93 %

Viennent de particuliers



Ce qui a changé

Les fuites de données alimentent les arnaques

→ **Hameçonnage : 1ère menace avec 33 % des cas de signalement**

Ils connaissent votre nom et votre banque.
Le message a l'air vrai.

(Quelques exemples... Free, Impôts, Fédérations sportives)

L'hameçonnage

Un message imite un organisme connu
(banque, impôts, colis, santé)

Il vous pousse à cliquer et à saisir
vos identifiants ou votre carte

Toujours différer votre action !

Arnaque ou pas ?

Arnaque ou pas ?

1 / 4

«ANTAI : vous avez une amende impayée de 35 €. Sans règlement sous 48 h, majoration à 180 €. Régularisez : antai-amendes-gouv.info »

Réponse : arnaque.

Un site public français finit par **.gouv.fr** — jamais par -gouv.info.

(Vrais sites : antai.gouv.fr pour les amendes, amendes.gouv.fr pour le paiement)

Arnaque ou pas ?

2 / 4

«Votre colis Colissimo n'a pas pu être livré,
frais de douane de 1,99 € à régler : colissimo-
suivi-fr.com/livraison »

Arnaque ou pas ?

2 / 4

Réponse : arnaque.

Une toute petite somme pour endormir la méfiance — l'objectif est votre numéro de carte.

Dois-je vraiment donner mon numéro de carte à quelqu'un qui m'a contacté le premier ?

Arnaque ou pas ?

3 / 4

SMS de la banque : « Un virement de 890 € a été initié. Si vous n'en êtes pas à l'origine, appelez le 01 xx xx xx xx »

Arnaque ou pas ?

3 / 4

Réponse : arnaque.

Il ne demande rien, il vous fait appeler, il vous rend acteur. C'est l'entrée en matière du faux conseiller bancaire.

Un vrai message de banque vous dit de passer par votre application ou votre agence
Seuls numéros à appeler : Au dos de votre carte ou de vos relevés bancaires papier.

Arnaque ou pas ?

4 / 4

« Votre relevé annuel est disponible dans votre espace client. »

Arnaque ou pas ?

4 / 4

Réponse : message normal.

Pas de lien, pas d'argent, pas de numéro, pas d'urgence.

Hameçonnage : les réflexes

- | Aucun clic sur un lien reçu
- | Taper soi-même l'adresse du site
- | Aucun organisme ne demande un mot de passe ou un code SMS
- | Dans le doute : raccrocher, rappeler le numéro du relevé bancaire

Enregistrez les vrais sites

Je vous fais noter les vraies adresses de vos sites habituels (banques, services publics etc).

On regarde ça.

Le faux conseiller bancaire

Après blabla et mise en confiance, il annonce une fraude et fait « valider » ou donner un code

+159 %, 15 000 cas par an

→ On ne valide rien. On ne donne aucune code. On raccroche. On rappelle sa banque.

Le faux support technique

« Votre téléphone est infecté » + un numéro à appeler

Au bout du fil : faux dépannage payant ou prise de contrôle de votre appareil

4e menace (5,9 %), +39 %

→ Une vraie alerte ne donne jamais de numéro. On ferme, on redémarre.

Arnaque ou pas ?

Page plein écran pendant la navigation :

1 / 2

ALERTE MICROSOFT — Votre appareil est infecté
par 3 virus. Ne redémarrez pas. Appelez
immédiatement le support agréé : 01 XX XX XX XX

Réponse : arnaque.

Un numéro de téléphone, l'interdiction de redémarrer, et un site web qui prétend analyser votre téléphone — il ne le peut pas.

Arnaque ou pas ?

2 / 2

Notification discrète en haut de l'écran :

« Mise à jour de sécurité disponible.
Appuyez pour installer. »

Réponse : légitime.

Elle vient des Paramètres du téléphone, pas d'une page web. À installer sans tarder. Dans le doute, cliquez vous même sur « Paramètres ».

Protéger ses comptes

Piratage de compte : 2e menace (11 %)

- | Un mot de passe différent par compte important
- | Double authentification activée
- | Le code reçu par SMS ne se communique à personne

La double authentification

Aujourd'hui on vérifie seulement si elle est active. On n'active rien en séance.

| **Android** : Paramètres → Google → Gérer votre compte → Sécurité

| **iPhone** : Réglages → votre nom → Connexion et sécurité

| L'activer sans préparation peut bloquer l'accès au compte.

À faire tranquillement chez soi, avec son mot de passe sous la main.

Les applications piégées

- Magasins officiels uniquement
- Les sites qui “offrent” des applis payantes les piègent
- Méfiance sur les autorisations : ex : un jeu de cartes n'a rien à faire dans vos contacts

Les autorisations d'une appli

Choisir une application que vous avez installée, pas une application du système.

| **Android** : Paramètres → Applications → l'appli → Autorisations

| **iPhone** : Réglages → Confidentialité et sécurité → Localisation

| Un jeu ou une lampe torche qui accède aux contacts : on refuse.

Refuser une autorisation n'empêche presque jamais l'application de fonctionner.

Vol : préparer AVANT

- | Code de déverrouillage + code PIN (ni 0000 ni 1234)
- | Verrouillage automatique de l'appareil
- | Mises à jour et sauvegardes des données
- | Noter l'IMEI (identifiant du téléphone) : *#06#

Le verrouillage automatique

Objectif : l'écran se verrouille tout seul après 1 ou 2 minutes.

| **Android** : Paramètres → Affichage → Mise en veille de l'écran

| **iPhone** : Réglages → Affichage et luminosité → Verrouillage automatique

| Choisir 1 ou 2 minutes. Le résultat se voit tout de suite.

Sans code de déverrouillage, ce réglage ne protège rien.

Afficher son IMEI

L'IMEI est le numéro de série du téléphone. Il permet de le faire bloquer en cas de vol.

- | Ouvrir le clavier du téléphone, comme pour appeler
- | **Composer :** *#06#
- | Le numéro s'affiche aussitôt. Aucun appel n'est passé.
- | Le recopier sur un papier, à garder chez soi.

Identique sur Android et sur iPhone.

Vol ou perte : ce qu'on fait APRÈS

- | La fonction de localisation doit avoir été activée avant.
- | Android : appli Localiser — localiser, verrouiller, effacer les données
- | iPhone : appli Localiser — Si vous le récupérez, il restera inutilisable sans votre mot de passe Apple

Puis : prévenir l'opérateur, faire opposition, déposer plainte.

La localisation à distance

Elle doit être active AVANT la perte. Aujourd'hui on vérifie seulement.

| **Android** : Paramètres → Google → Localiser mon appareil

| **iPhone** : Réglages → votre nom → Localiser → Localiser mon iPhone

| On regarde que l'interrupteur est bien activé. On ne teste rien.

Les noms de menus varient un peu selon la marque du téléphone.

À retenir

1. Aucun lien reçu par message
2. Aucun code communiqué par telephone
3. Mises à jour et sauvegardes
4. Magasins officiels uniquement
5. Verrouillage + localisation activés à l'avance

Un problème ?

📍 17cyber.gouv.fr (conseils et porter plainte)

📍 Cybermalveillance.gouv.fr