

SÉCURITÉ
INFORMATIQUEMesures essentielles pour assurer sa sécurité
numérique

Contexte et bonnes pratiques de base

Contexte de la menace numérique (2025)

- Plus de 348 000 atteintes numériques enregistrées en 2025 (hausse de 74 % en 5 ans), selon le rapport annuel de la CNIL.
- Le chiffre réel est probablement plus élevé : de nombreuses victimes ne portent pas plainte.
- 90 % des utilisateurs commettent des erreurs courantes en matière de sécurité, augmentant leur vulnérabilité.

Liste non exhaustive des organisations compromises en 2025 :

<https://bonjourlafuite.eu.org/>

Mesures de protection individuelle

Protéger ses accès avec des mots de passe
solides

- ☒ Utiliser des mots de passe différents par service → évite la compromission en chaîne.
- ☒ Longueur minimale : 12 à 14 caractères, mélange majuscules/minuscules/chiffres/caractères spéciaux.
- ☒ Méthodes de création :
 - Premières lettres d'une phrase : Un tiens vaut mieux que deux tu l'auras → 1tvmQ2tl'A
 - Phonétique : J'ai acheté huit CD pour cent euros cet après-midi → ght8CD%E7am
- ☒ Ne jamais communiquer son mot de passe — aucune entreprise sérieuse ne le demande.
- ☒ Changer son mot de passe au moindre soupçon de compromission.

Activer la double authentification (2FA)

- Renforce la sécurité : code provisoire reçu par SMS, e-mail, ou via une application (ex. Google Authenticator).

Ne pas utiliser ses mots de passe sur un
ordinateur partagé

- Utiliser le mode navigation privée.
- Fermer les sessions, ne pas enregistrer les mots de passe.
- Changer les mots de passe utilisés sur un ordinateur partagé dès retour sur un appareil personnel.

Utiliser un gestionnaire de mots de passe

- KeePassXC (<https://keepassxc.org/>)
- Bitwarden (<https://bitwarden.com/fr-fr/>)
- → Stocke vos mots de passe en toute sécurité, accessible avec un seul mot de passe maître.

Sauvegarder ses données régulièrement

- ☒ Sauvegardes manuelles (clé USB, disque dur externe) ou automatisées (solutions payantes/gratuites).
- ☒ Déconnecter le support de sauvegarde après utilisation → évite la contamination par un rançongiciel.
- ☒ Tester régulièrement les sauvegardes pour vérifier leur intégrité.

Mettre à jour logiciels et matériels

- ☒ Mettre à jour tous les appareils dès disponibilité.
- ☒ Activer les mises à jour automatiques.
- ☒ Ne télécharger les mises à jour que depuis les sites officiels.

Utiliser un antivirus

- Solutions gratuites recommandées :
 - Avira Free Security (<https://www.avira.com/fr/free-security>)
 - Bitdefender Antivirus Free (<https://www.bitdefender.com/fr-fr/consumer/free-antivirus>)
- Faire des scans réguliers.

Autres préconisations

- 📶 En mobilité : privilégier la 4G/5G aux WiFi publics → risque de capture de données.
- 🛡️ Si WiFi public obligatoire : ne pas effectuer d'opérations sensibles, utiliser un VPN.
- 🎯 Se protéger contre le hameçonnage :
 - Ne pas cliquer sur les liens/pièces jointes des e-mails suspects.
 - Vérifier le https:// et le cadenas lors des paiements en ligne.

IA et vie privée

- Opposition à l'utilisation de vos données pour entraîner des IA :
 - *Google / Gemini* : Paramètres → Activité → Désactiver et supprimer l'activité.
 - *Meta* (Instagram/Facebook) : Réglages → Centre de confidentialité → "S'opposer" + message type fourni.
 - *WhatsApp* (Meta) : Formulaire dédié → sélectionner "IA par Meta".
 - *OpenAI* (ChatGPT) : Paramètres → Gestion des données → décocher "Améliorer le modèle pour tous".
 - *Mistral* (Le Chat) : Paramètres → Préférences → décocher "Autoriser l'utilisation de vos interactions".

Ressources utiles

- 🛡️ **17 Cyber** : service public d'assistance aux victimes de cybermalveillance → <https://17cyber.gouv.fr/>
- 🔍 Vérifier si votre e-mail est compromis → <https://haveibeenpwned.com/>
- 🌱 **Euria** : IA éthique, open source, sans stockage, 100 % Suisse, énergie renouvelable → <https://www.infomaniak.com/fr/euria>

Mémo liste

- ☐ J'utilise un mot de passe différent pour chaque compte et service en ligne.
- ☐ Je choisis des mots de passe solides : 12 caractères, majuscules et minuscules, chiffres et caractères spéciaux (\$, *, !).
- ☐ J'utilise un gestionnaire de mots de passe.
- ☐ Je sauvegarde régulièrement mes données (photos, contacts, messagerie, documents, etc.) pour ne pas les perdre.
- ☐ Je télécharge les logiciels ou les applications sur les sites officiels des éditeurs.
- ☐ J'utilise un antivirus sur tous mes appareils.
- ☐ Je mets à jour mes appareils, logiciels et applications que j'utilise.
- ☐ Je ne fais pas d'opérations sensibles depuis un Wi-Fi public : paiement, saisie de données personnelles.
- ☐ Je ne clique pas sur les liens dans les courriels et je privilégie les connexions depuis les sites ou applications officiels.
- ☐ Je suis vigilant aux tentatives d'hameçonnage par courriel, sms, téléphone.
- ☐ Je verrouille mon ordinateur dès que je m'en éloigne et je l'éteins quand je ne m'en sers pas.
- ☐ Je range en lieu sûr les documents sensibles et les périphériques (clés USB, disque dur).
- ☐ Si j'utilise une IA générative, je ne la nourris pas de données personnelles.

