



Sécurité Numérique

pour Tous

Comprendre les risques · Adopter les bons gestes · Protéger sa vie numérique



Au programme aujourd'hui

- 1 Pourquoi la sécurité numérique nous concerne tous
- 2 Les menaces courantes (virus, arnaques, espionnage)
- 3 Se protéger : les gestes essentiels
- 4 Mots de passe & double vérification
- 5 Vos appareils (PC, smartphone, tablette)
- 6 Internet & Wi-Fi public
- 7 Vos données personnelles et vos droits
- 8 Communiquer en sécurité
- 9 Protéger sa vie privée en ligne
- 10 Enfants & familles
- 11 Que faire en cas de problème ?
- 12 Checklist & outils recommandés

Pourquoi ça nous concerne tous ?



On utilise le numérique pour tout

banque, santé, photos, communications, travail...



Tout le monde est visé

pas seulement les entreprises : les particuliers aussi



Une seule erreur peut coûter cher

vol d'argent, usurpation d'identité, perte de données



Notre comportement protège aussi les autres

famille, amis, collègues

Les dangers numériques en un coup d'œil

Connaître les risques, c'est déjà se protéger.



Virus & logiciels malveillants



Hameçonnage (phishing)



Rançongiciels (ransomware)



Arnaques par téléphone/SMS



Wi-Fi espionné



Vol de données personnelles

90%

des attaques débutent
par un e-mail piégé

1/3

des Français touchés
par une arnaque en ligne chaque année

L'hameçonnage (phishing)

La plus courante des arnaques

 Un message suspect ressemble à :

De : **support@ma-banque-secure-pro.xyz** ⚠

Objet : **URGENT — Votre compte est bloqué !**

Cher(e) client(e),

Votre compte a été suspendu. Cliquez ici

immédiatement pour le réactiver :

👉 **<http://ma-banque.xyz/verification>**

Signes d'alerte

- ⚠ Adresse e-mail bizarre
- ⚠ Ton urgent/alarmiste
- ⚠ Fautes d'orthographe
- ⚠ Lien inconnu ou raccourci
- ⚠ Demande d'infos perso
- ⚠ Pièce jointe inattendue

✅ En cas de doute : ne cliquez pas. Allez directement sur le site officiel.

Virus, logiciels espions et rançongiciels



Virus

Se glisse dans vos fichiers et les endommage.
Arrive souvent par pièces jointes ou logiciels piratés.



Logiciel espion

Se cache sur votre appareil et vole vos mots de passe, données bancaires, photos...



Rançongiciel

Chiffre tous vos fichiers et réclame une rançon pour les récupérer.
Ne payez jamais !

Arnaques par SMS et appels téléphoniques



Exemple de SMS piégé

"Votre colis n'a pas pu être livré.
Cliquez ici pour reprogrammer :
<http://livraison-rapide.net>"

⚠ Lien suspect · Aucune commande passée ?

→ **NE CLIQUEZ PAS**

Smishing = phishing par SMS



Arnaque par téléphone (vishing)

- Se font passer pour votre banque
- Prétendent détecter une fraude
- Demandent votre code par SMS
- Créent une urgence artificielle



Ne jamais donner un code reçu !

Les menaces liées à l'informatique

Questions / Reponses

3 piliers de votre protection

1



Mettre à jour

Systèmes, applis, appareils

Les mises à jour corrigent des failles.
Activez les mises à jour automatiques
!

2



Sauvegarder

Vos données importantes

Disque externe + cloud =
vous ne perdrez jamais vos souvenirs.

3



Antivirus

Sur chaque appareil

Un bon antivirus gratuit vaut mieux
que rien du tout. Gardez-le actif.

Les protections face aux menaces

Questions / Reponses

Un bon mot de passe : simple à retenir, impossible à deviner

✗ Les erreurs classiques

- ✗ 123456 ou qwerty
- ✗ Prénom + année de naissance
- ✗ Mot du dictionnaire seul
- ✗ Même mot de passe partout
- ✗ Suites évidentes : P@ssw0rd

✓ La bonne méthode : la phrase de passe

Assemblez 4 mots aléatoires :

café · robot · lune · atlas

- ✓ 16 caractères → très difficile à pirater
- ✓ Facile à retenir avec une image mentale
- ✓ 1 mot de passe différent par site
- ✓ Utilisez un gestionnaire de mots de passe

Le gestionnaire de mots de passe et la double vérification

Gestionnaire de mots de passe

**Vous n'avez à retenir
qu'UN SEUL mot de passe maître !**

- ✓ Il génère des mots de passe forts pour vous
- ✓ Il les remplit automatiquement
- ✓ Sécurisé et chiffré
- ✓ Exemples : Bitwarden (gratuit), 1Password

Double vérification (2FA / MFA)

**Même si quelqu'un vole votre mot
de passe, il ne peut pas entrer !**

Comment ça marche ?

1. Saisir votre mot de passe
2. Recevoir un code sur votre téléphone
3. Saisir ce code = accès accordé !

 **Activez la double vérification sur votre e-mail, votre banque, et vos réseaux sociaux.**

Les conseils concernant les mots de passe

Questions / Reponses

Sécuriser votre PC, smartphone et tablette



Verrouillez l'écran

Code PIN, empreinte ou visage. L'écran doit se verrouiller après 30 secondes sans utilisation.



Mises à jour automatiques

Activez-les pour l'appareil ET les applications. Ça prend 5 minutes et corrige des failles importantes.



Applications officielles

Téléchargez uniquement depuis l'App Store (Apple) ou le Google Play Store. Évitez les autres sources.



Autorisations des applis

Une lampe de poche n'a pas besoin d'accéder à vos contacts. Limitez les permissions au minimum.



Wi-Fi et Bluetooth

Désactivez le Bluetooth et le Wi-Fi quand vous ne les utilisez pas pour éviter les connexions non voulues.



Sauvegarde chiffrée

Activez la sauvegarde automatique (iCloud, Google, PC). Même chiffrée si possible.

Naviguer en sécurité sur Internet

⚠ Wi-Fi public : attention !

⚠ Vos données peuvent être interceptées

⚠ Un faux Wi-Fi peut imiter le vrai

⚠ Évitez les banques et achats en ligne

⚠ Préférez votre 4G/5G pour ces actions

Si vous devez utiliser un Wi-Fi public : utilisez un VPN.

✓ Bons réflexes à la maison

🔒 Changez le mot de passe de votre box

🔒 Activez le chiffrement WPA3 ou WPA2

📶 Créez un réseau invité pour vos visiteurs

🔄 Mettez à jour votre box/routeur

🌐 Vérifiez le cadenas 🔒 dans le navigateur

Vos données personnelles : qu'est-ce qui est précieux ?

Peu sensible

- Prénom public
- Intérêts généraux
- Ville de résidence

Sensible

- Adresse exacte
- Numéro de téléphone
- Historique d'achats

Très sensible

- Mots de passe
- N° de sécurité sociale
- Données bancaires
- Santé, biométrie

Vous avez des droits sur vos données !

En France et en Europe, la loi RGPD vous protège.



Droit d'accès

Savoir quelles données un service possède sur vous.



Droit de rectification

Corriger des informations inexactes vous concernant.



Droit à l'effacement

Demander la suppression de vos données ("droit à l'oubli").



Droit à la portabilité

Récupérer vos données dans un format réutilisable.



Droit d'opposition

Refuser que vos données soient utilisées pour la publicité.



Droit de réclamation

Porter plainte à la CNIL si un service ne respecte pas vos droits.



Pour exercer vos droits : cherchez « confidentialité » ou « données personnelles » sur le site du service concerné.

Appels et messages : communiquer sans crainte



Chiffrement de bout en bout (E2EE) :

Votre message est chiffré sur votre téléphone et ne peut être lu que par votre destinataire. Personne d'autre — pas même l'application — ne peut lire le contenu.

Idéal

Signal

E2EE par défaut, messages + appels

Bien

WhatsApp

E2EE activé, mais métadonnées collectées

Partiel

Telegram

E2EE seulement en mode « Secret »

Limité

E-mail classique

Non chiffré par défaut, vulnérable



Conseil : utilisez Signal pour les conversations sensibles. Pour le reste, WhatsApp reste acceptable.

Vous êtes suivi partout sur Internet : comment limiter ça ?



Cookies et traceurs publicitaires

Des petits fichiers invisibles suivent vos visites de site en site pour vous afficher des publicités ciblées. Ils analysent vos habitudes, vos achats, vos lectures...



Bloqueur de publicités

uBlock Origin (gratuit) bloque la majorité des traceurs. Installez-le sur votre navigateur.



Cookies tiers : désactiver

Dans les paramètres de votre navigateur, désactivez les cookies tiers. Simple et efficace.



Mode navigation privée

Supprime l'historique local après fermeture, mais ne vous rend pas invisible sur Internet.



Autorisations des apps

Une app qui demande votre localisation en permanence collecte vos données. Accordez « pendant l'utilisation » seulement.

Réseaux sociaux : ce que vous partagez compte

✗ Réglages dangereux

- ✗ Profil public visible par tout le monde
- ✗ Date de naissance complète visible
- ✗ Géolocalisation activée sur vos photos
- ✗ Vos amis peuvent partager vos posts sans accord

✓ Bons réglages

- ✓ Profil visible uniquement par vos amis ✓
- ✓ Double vérification activée ✓
- ✓ Applis tierces non utilisées supprimées ✓
- ✓ Publicité ciblée désactivée ✓

💡 À faire : vérifiez vos paramètres de confidentialité sur chaque réseau social, une fois par an.

Protéger ses enfants sur Internet



Outils parentaux

- Android : Google Family Link
- iPhone/iPad : Screen Time (Temps d'écran)
- Windows : Microsoft Family Safety
- Tous : filtrage web activé
- Approuver les téléchargements d'apps



Ce qu'enseigner aux enfants

- Ne jamais partager son adresse ou son école
- Ne pas accepter d'inconnus en ligne
- Dire à un adulte si quelque chose gêne
- Signaler le harcèlement, ne pas répondre
- Ne jamais se rencontrer sans un adulte

Quel usage numérique selon l'âge ?

3–5 ans

🕒 15–30 min/jour

Toujours avec un adulte · Apps éducatives uniquement · Pas de réseaux sociaux

6–10 ans

🕒 30–60 min/jour

Supervision active · Apps contrôlées · Règles claires sur le partage d'infos

11–14 ans

🕒 1–2 h/jour

Profils privés · Discussions régulières · Pas de rencontres sans adulte

15–17 ans

🕒 2–3 h/jour

Autonomie croissante · 2FA obligatoire · Comportement responsable encouragé



L'outil le plus efficace reste le dialogue. Parlez régulièrement avec vos enfants de ce qu'ils font en ligne.

Mon compte a été piraté : les 8 étapes à suivre

1

Déconnectez-vous partout

Option « déconnecter toutes les sessions » dans les paramètres du compte

3

Activez le 2FA

Ajoutez une application d'authentification (ou clé physique) maintenant.

5

Vérifiez les paramètres

Adresse de récupération, numéro, règles de renvoi des e-mails.

7

Prévenez vos contacts

Si des messages frauduleux ont été envoyés, avertissez-les.

2

Changez le mot de passe

Depuis un autre appareil si possible. Choisissez une phrase de passe longue et unique.

4

Révoquez les accès tiers

Supprimez les applications tierces liées à ce compte.

6

Scannez vos appareils

Lancez un antivirus sur tous vos appareils connectés.

8

Surveillez pendant 1 mois

Vérifiez vos comptes bancaires et alertes de connexion.

Un rançongiciel a bloqué mes fichiers !

Que faire ?

 **Ne payez JAMAIS la rançon — cela ne garantit pas la récupération de vos fichiers et encourage les criminels.**

1



Débranchez l'appareil du réseau et désactivez le Wi-Fi immédiatement pour limiter la propagation.

2



Prenez en photo le message de rançon. Notez l'heure et ce qui s'est passé juste avant.

3



Appelez un technicien ou votre prestataire informatique. Ne tentez pas de réparer seul.

4



Signalez aux autorités : portez plainte à la gendarmerie ou au commissariat.

5



Restaurez vos fichiers depuis votre sauvegarde (disque externe propre ou cloud).

Qui contacter en cas de cyberattaque ou arnaque ?



Votre banque

Fraude bancaire, carte compromise

→ Numéro au dos de votre carte → Blocage immédiat



Gendarmerie / Police

Toute cyberattaque, escroquerie

→ Portez plainte avec preuves (captures d'écran)



CNIL (France)

Fuite de données personnelles

→ www.cnil.fr → Déposer une plainte en ligne



Cybermalveillance.gouv.fr

Tout incident numérique

→ Diagnostic en ligne + liste de prestataires

Mes bons réflexes numériques au quotidien



Un mot de passe différent pour chaque compte important



Double vérification (2FA) activée sur e-mail et banque



Mises à jour activées en automatique sur tous mes appareils



Sauvegarde régulière de mes photos et documents



Je ne clique jamais sur un lien douteux sans vérifier



J'installe uniquement depuis les boutiques officielles



Mon Wi-Fi domestique est protégé par un bon mot de passe



Je vérifie mes paramètres de confidentialité 1 fois par an

Les outils du quotidien pour rester en sécurité



Gestionnaire de mots de passe

- Bitwarden — Gratuit, sécurisé, recommandé
- 1Password — Très facile à utiliser
- KeePass — Contrôle total (plus technique)



Double authentification (2FA)

- Google Authenticator — Simple, gratuit
- Authy — Sauvegarde des codes incluse
- Clé physique YubiKey — Niveau max de sécurité



Navigateur & confidentialité

- Extension uBlock Origin — Bloque traceurs et pubs
- Firefox / Brave — Navigateurs axés vie privée
- HTTPS partout — Connexion sécurisée toujours



VPN (réseau sécurisé)

- ProtonVPN — Gratuit et respectueux
- NordVPN / Surfshark — Bon équilibre prix/qualité
- Mullvad — Le plus anonyme

La loi vous protège : le RGPD expliqué simplement

Le RGPD (Règlement Général sur la Protection des Données) s'applique à toutes les entreprises qui traitent vos données en Europe.



But précis

Vos données ne peuvent être collectées que pour un but défini et légitime.



Minimum nécessaire

Un service ne peut récolter que les données dont il a vraiment besoin.



Transparence

Vous devez être clairement informé de qui collecte quoi et pourquoi.



Consentement

Les cases pré-cochées sont interdites. Votre accord doit être explicite.



Sécurité obligatoire

Les entreprises doivent protéger vos données avec des mesures techniques.



Alerte en cas de fuite

Si vos données sont volées, le service doit vous en informer sous 72h.

5 actions à faire DÈS AUJOURD'HUI

1



Mettez à jour votre téléphone et votre ordinateur maintenant.

2



Activez la double vérification sur votre e-mail principal.

3



Installez un gestionnaire de mots de passe (Bitwarden, gratuit).

4



Sauvegardez vos photos et documents importants sur un disque ou dans le cloud.

5



Vérifiez vos paramètres de confidentialité sur vos réseaux sociaux.

Ce qu'il faut retenir :

10 messages clés

1 Mot de passe long et unique pour chaque compte

3 Mises à jour régulières de tous vos appareils

5 Téléchargez uniquement depuis les boutiques officielles

7 Sécurisez votre Wi-Fi domestique (mot de passe fort)

9 Vérifiez vos paramètres de confidentialité chaque année

2 Double vérification (2FA) sur e-mail et banque

4 Méfiez-vous des liens et pièces jointes inattendus

6 Sauvegardez régulièrement vos données importantes

8 Limitez les informations partagées en ligne

10 En cas de problème : signalez, ne payez pas

Mémo imprimable — Que faire en cas d'urgence numérique ?



Mon compte a été piraté :

- ☐ 1. Déconnecter toutes les sessions
- ☐ 2. Changer le mot de passe
- ☐ 3. Activer le 2FA
- ☐ 4. Prévenir ma banque si nécessaire
- ☐ 5. Signaler à la police



Contacts clés :

- | | |
|-----------------|---|
| Banque : | N° au dos de votre carte |
| Police : | 17 ou 15 si urgence |
| Cyber : | cybermalveillance.gouv.fr |
| CNIL : | www.cnil.fr |

Pour aller plus loin : ressources gratuites et fiables



cybermalveillance.gouv.fr

Le portail officiel français · Diagnostic, conseils, prestataires de confiance · Signaler une attaque



cnil.fr

Informations sur vos droits · Déposer une plainte pour violation de données · Guides pratiques



haveibeenpwned.com

Vérifiez si votre e-mail a été exposé dans une fuite de données (en anglais, gratuit)



security.google.com/settings

Bilan de sécurité de votre compte Google · Gratuit et simple à utiliser

✓ Tous ces sites sont gratuits et officiels. Signetez-les dans votre navigateur !



La sécurité numérique, c'est l'affaire de tous.



Pas besoin d'être expert.
Quelques gestes simples suffisent à protéger
votre vie numérique et celles de vos proches.



Mots de passe uniques + 2FA



Mises à jour automatiques



Sauvegardes régulières

Merci pour votre attention · Des questions ?

cybermalveillance.gouv.fr · cnil.fr