
LA CYBERSECURITE POUR DEBUTANT

Table des matières

Qu’est-ce que la cybersécurité ?

La cybersécurité regroupe les moyens humains, techniques et organisationnels utilisés pour protéger les informations, les comptes, les appareils et les services numériques.

Trois objectifs simples

OBJECTIF	QUESTION À SE POSER
Confidentialité	Qui peut voir cette information ?
Intégrité	L’information a-t-elle été modifiée ?
Disponibilité	Puis-je encore y accéder quand j’en ai besoin ?

EXEMPLE : Un dossier partagé avec la mauvaise personne touche la confidentialité. Un fichier effacé touche la disponibilité.

Votre rôle

Les outils de sécurité aident, mais ils ne remplacent pas l’attention. Un doute signalé rapidement peut éviter un incident plus grave.

Ce que vous devez protéger

Les données

Documents de travail, photos et contrats ;
Coordonnées, dossiers clients ou usagers ;
Informations bancaires et données de santé.

Les accès

Adresse électronique ;
Comptes professionnels et personnels ;
Services administratifs, cloud et réseaux sociaux.

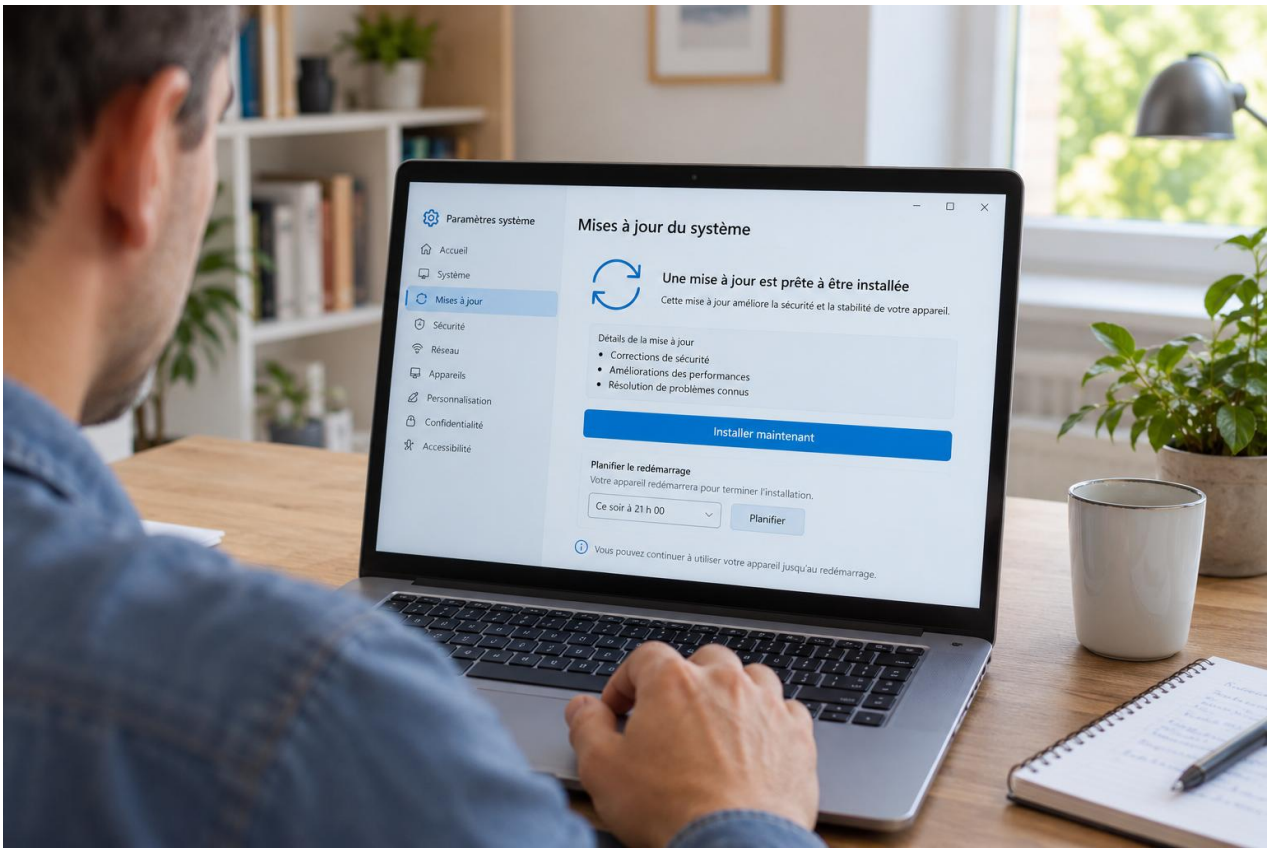
Les appareils

Ordinateur, téléphone et tablette ;
Clé USB, disque externe et imprimante ;
Box Internet et objets connectés.

À RETENIR Une information banale seule peut devenir sensible lorsqu’elle est combinée à d’autres informations.

Protéger son ordinateur et son smartphone

Mises à jour, antivirus, applications, Wi-Fi, clés USB et téléchargements



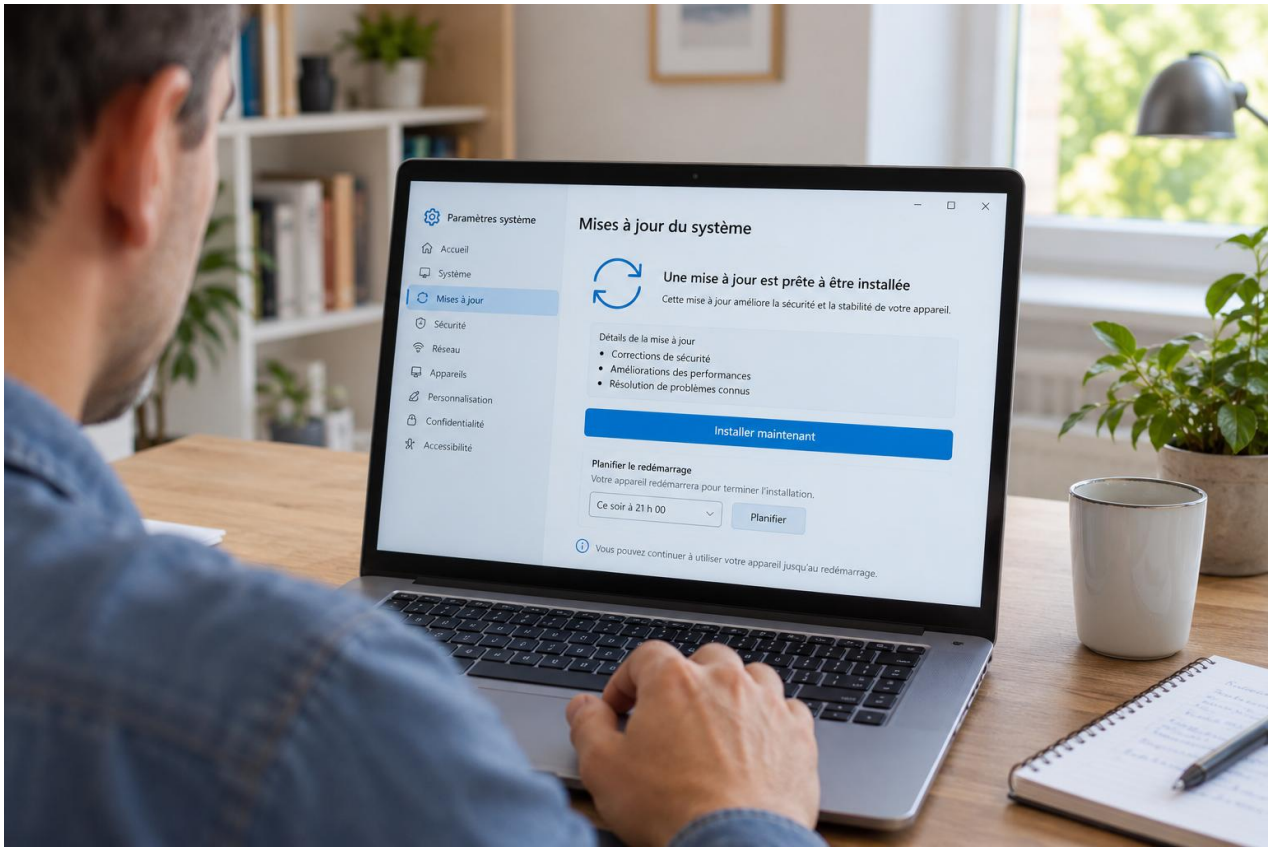
Maintenir le système à jour corrige des failles et améliore la stabilité de l'appareil.

Les protections complémentaires

Aucune protection ne suffit seule. La sécurité repose sur plusieurs barrières qui se complètent et limitent les conséquences d'une erreur.

BARRIÈRE	RÔLE
Mises à jour	Corriger les vulnérabilités connues
Antivirus	Détecter et bloquer certaines menaces
Verrouillage	Empêcher un accès direct à l'appareil
Sauvegarde	Retrouver les données après un incident
Prudence	Éviter les installations et connexions risquées

Mettre à jour son ordinateur



La page de mise à jour indique ce qui sera installé et permet souvent de planifier le redémarrage.

RÉFLEXE Enregistrez votre travail puis installez les mises à jour depuis les paramètres du système.

Procédure de mise à jour

Avant de commencer

☐ branchez l'ordinateur sur le secteur ;
☐ enregistrez et fermez les documents ;
☐ vérifiez que la connexion est stable ;
☐ prévoyez le temps nécessaire au redémarrage.

Dans les paramètres

- Ouvrez Paramètres puis la rubrique de mise à jour ;
- Lancez la recherche ;
- Installez les mises à jour proposées ;
- Redémarrez si cela est demandé ;
- Revenez vérifier qu'aucune action ne reste en attente.

Mettre à jour son smartphone

Le système

- Ouvrez les réglages ;
- Recherchez Mise à jour du système ou Mise à jour logicielle ;
- Sauvegardez les données importantes ;
- Branchez le téléphone et utilisez un Wi-Fi fiable ;
- Installez puis contrôlez la version.

Les applications

Activez les mises à jour automatiques si elles conviennent à votre forfait et aux règles de l'organisation.

ATTENTION : Une fausse alerte affichée dans le navigateur ne met pas le téléphone à jour. Utilisez uniquement les réglages officiels.

Pourquoi ne pas reporter longtemps

Une mise à jour de sécurité corrige souvent une faiblesse déjà connue. Plus elle est retardée, plus l'appareil reste exposé à des méthodes d'attaque documentées.

Bon compromis

- Laissez les mises à jour automatiques activées ;
- Planifiez le redémarrage à un moment adapté ;
- Ne coupez pas l'appareil pendant l'installation ;
- Vérifiez régulièrement les appareils rarement utilisés.

ENTREPRISE Ne contournez pas une mise à jour gérée par votre organisation.

Verrouiller l'appareil

Sur ordinateur

- Utilisez un code ou un mot de passe de session ;
- Activez le verrouillage automatique ;
- Verrouillez manuellement avant de vous éloigner ;
- Séparez les comptes des différents utilisateurs.

Sur smartphone

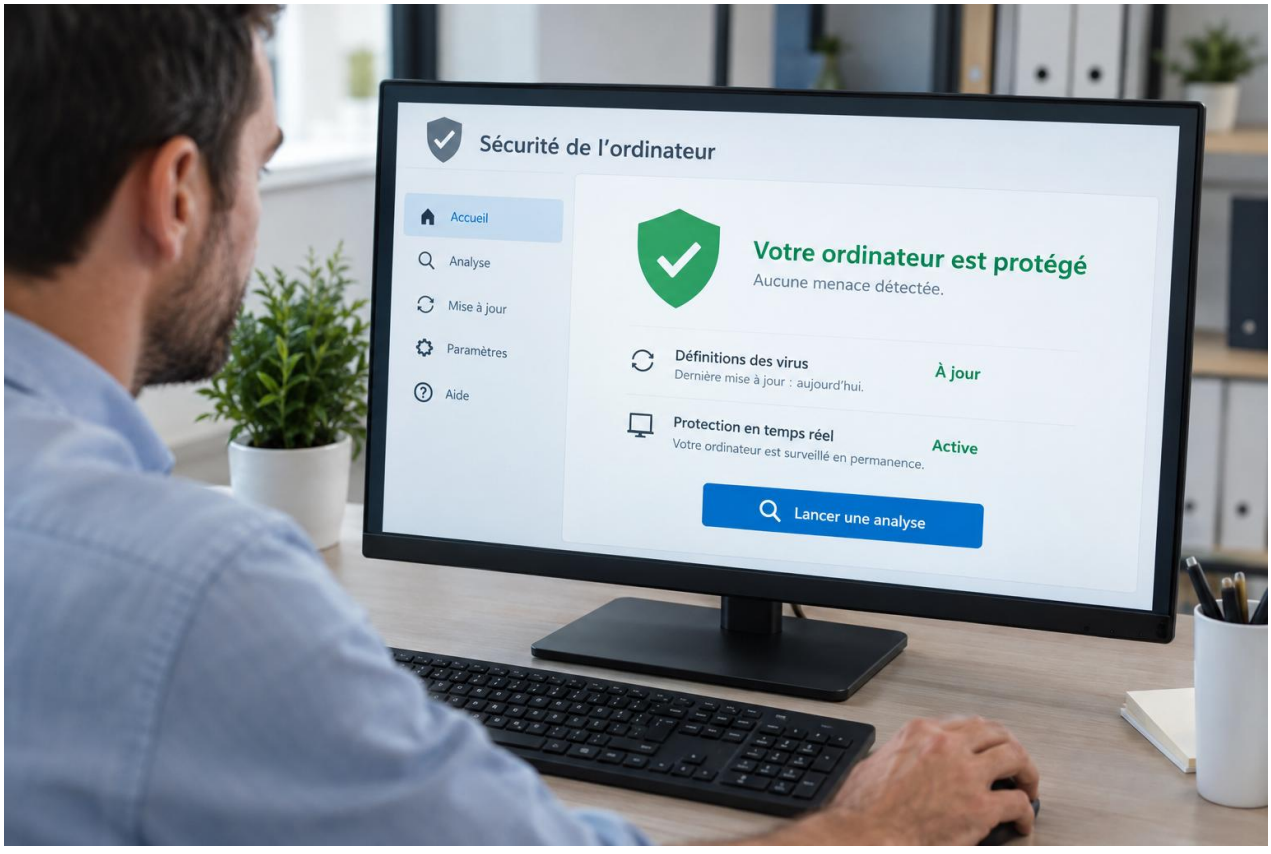
- Choisissez un code suffisamment long ;
- Activez la biométrie en complément ;
- Masquez le contenu sensible des notifications verrouillées ;
- Activez la fonction de localisation et d'effacement si elle est disponible.

Comprendre l’antivirus

L’antivirus surveille des fichiers et des comportements connus comme dangereux. Il réduit les risques, mais il ne remplace ni les mises à jour ni la vigilance.

FONCTION	UTILITÉ
Protection en temps réel	Contrôle les fichiers au moment de leur utilisation
Mises à jour de sécurité	Ajoute de nouvelles informations de détection
Analyse rapide	Contrôle les zones les plus exposées
Analyse complète	Examine davantage de fichiers et prend plus de temps
Quarantaine	Isole un élément détecté

Vérifier la protection



Les indicateurs essentiels sont la protection active, les définitions à jour et l’absence d’alerte.

À RETENIR Une icône verte aide, mais vérifiez aussi la date de la dernière mise à jour.

Lancer une analyse

Quand analyser

- Après l'ouverture d'un fichier douteux ;
- Si l'appareil ralentit ou se comporte étrangement ;
- Après avoir branché un support autorisé mais incertain ;
- Selon le calendrier prévu par l'organisation.

Procédure

☐ ouvrez l'outil de sécurité ;
☐ mettez les définitions à jour ;
☐ choisissez le type d'analyse ;
☐ laissez l'analyse se terminer ;
☐ lisez le résultat avant d'agir.

Réagir à une alerte antivirus

- Ne cliquez pas au hasard sur Autoriser ;
- Notez le nom de la menace et le fichier concerné ;
- Laissez l'outil isoler ou bloquer l'élément ;
- Redémarrez si cela est demandé ;
- Relancez une analyse ;
- Sur un appareil professionnel, prévenez le service informatique.

DANGER Ne restaurez jamais un fichier de quarantaine simplement parce qu'il semble important.

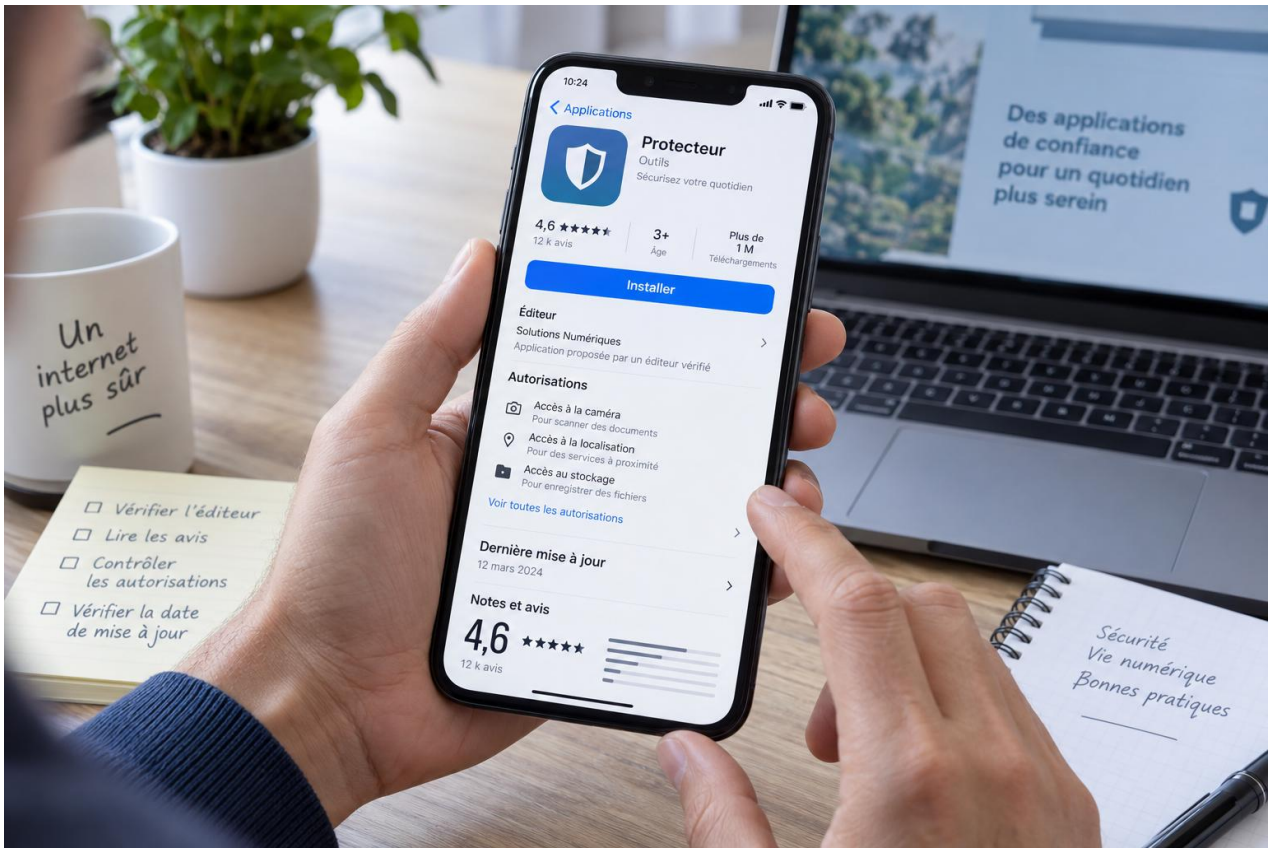
Éviter les faux antivirus

Une page web peut afficher une fausse analyse et prétendre que plusieurs virus ont été trouvés. Un site ne peut pas diagnostiquer instantanément tous les fichiers de votre appareil.

Si une alerte apparaît dans le navigateur

- Ne téléphonez pas au numéro affiché ;
- Ne téléchargez pas l'outil proposé ;
- Fermez l'onglet ou le navigateur ;
- Ouvrez vous-même l'outil de sécurité installé ;
- Lancez une analyse depuis cet outil.

Choisir une application



Avant d'installer, contrôlez l'éditeur, les autorisations, les avis et la date de mise à jour.

SOURCE Privilégiez la boutique officielle ou le site officiel de l'éditeur.

Vérifier avant l'installation

☐ le nom de l'application est-il exactement celui recherché ?
☐ l'éditeur est-il clairement identifié ?
☐ les avis paraissent-ils cohérents et détaillés ?
☐ l'application est-elle maintenue récemment ?
☐ les autorisations demandées correspondent-elles à sa fonction ?
☐ l'application est-elle réellement nécessaire ?

EXEMPLE Une lampe torche n'a normalement pas besoin de vos contacts ou de votre microphone.

Comprendre les autorisations

AUTORISATION	QUESTION À SE POSER
Caméra	La fonction doit-elle prendre des photos ?
Microphone	Doit-elle enregistrer du son ?
Localisation	La position est-elle nécessaire en permanence ?
Contacts	Pourquoi doit-elle lire mon carnet d'adresses ?
Fichiers	A-t-elle besoin de tous les documents ?
Notifications	Les messages seront-ils réellement utiles ?

RÉGLAGE Accordez le minimum nécessaire et préférez Pendant l'utilisation lorsque ce choix existe.

Supprimer une application inutile

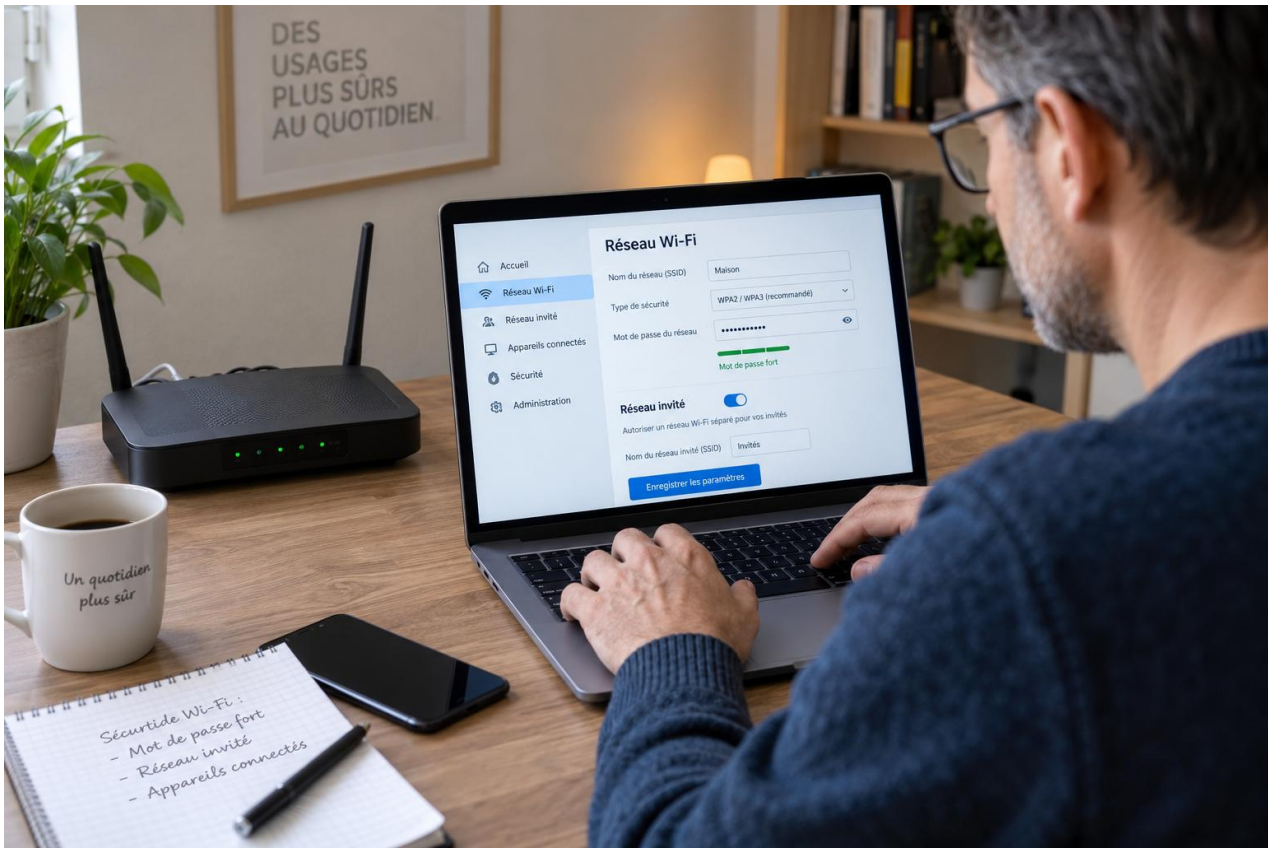
Pourquoi

Une application abandonnée, inconnue ou inutile augmente la surface d'exposition et peut continuer à accéder à des données.

Procédure

- Sauvegardez les données à conserver ;
- Désinstallez depuis les paramètres ou le menu officiel ;
- Révoquez les accès associés au compte si nécessaire ;
- Supprimez les fichiers d'installation restants ;
- Contrôlez les autorisations des applications conservées.

Sécuriser le Wi-Fi domestique



Le chiffrement moderne, un mot de passe fort et un réseau invité renforcent le Wi-Fi.

IMPORTANT Modifiez aussi le mot de passe d'administration fourni par défaut.

Réglages du routeur

☐ ouvrez l'interface avec l'adresse et les instructions du fabricant ;
☐ changez le mot de passe d'administration ;
☐ utilisez WPA2 ou WPA3 selon les appareils ;
☐ choisissez un mot de passe Wi-Fi long et unique ;
☐ désactivez les fonctions inutiles ;
☐ mettez le routeur à jour ;
☐ créez un réseau invité pour les visiteurs ou objets connectés.

PRUDENCE Ne modifiez pas un routeur professionnel sans autorisation.

Se connecter sur un WiFi public

Dans un lieu public, la prudence concerne à la fois le réseau, l'écran et l'environnement.

Un nom de réseau rassurant ne garantit pas qu'il appartient au café, à l'hôtel ou à la gare. Un faux point d'accès peut imiter le vrai.

PRÉFÉREZ : Le partage de connexion de votre téléphone ou le VPN validé par votre organisation.

Les bons gestes en mobilité

☐ vérifiez le nom du réseau auprès du personnel ;
☐ évitez les opérations sensibles sur un réseau public ;
☐ désactivez la connexion automatique au Wi-Fi et au Bluetooth ;
☐ verrouillez l'écran dès que vous vous éloignez ;
☐ utilisez un filtre de confidentialité si nécessaire ;
☐ ne laissez jamais l'appareil sans surveillance.

Sur smartphone

Protégez l'accès par un code robuste ou la biométrie, activez la localisation et l'effacement à distance lorsque c'est possible, et vérifiez les autorisations des applications.

REGARD DISCRET : Dans les transports, une personne peut lire un code ou photographier votre écran sans toucher à l'appareil.

Le risque des clés USB inconnues

Une clé trouvée ou offerte sans contrôle ne doit pas être branchée sur un appareil.

RÈGLE Remettez le support au service compétent ou à son propriétaire sans l'ouvrir.

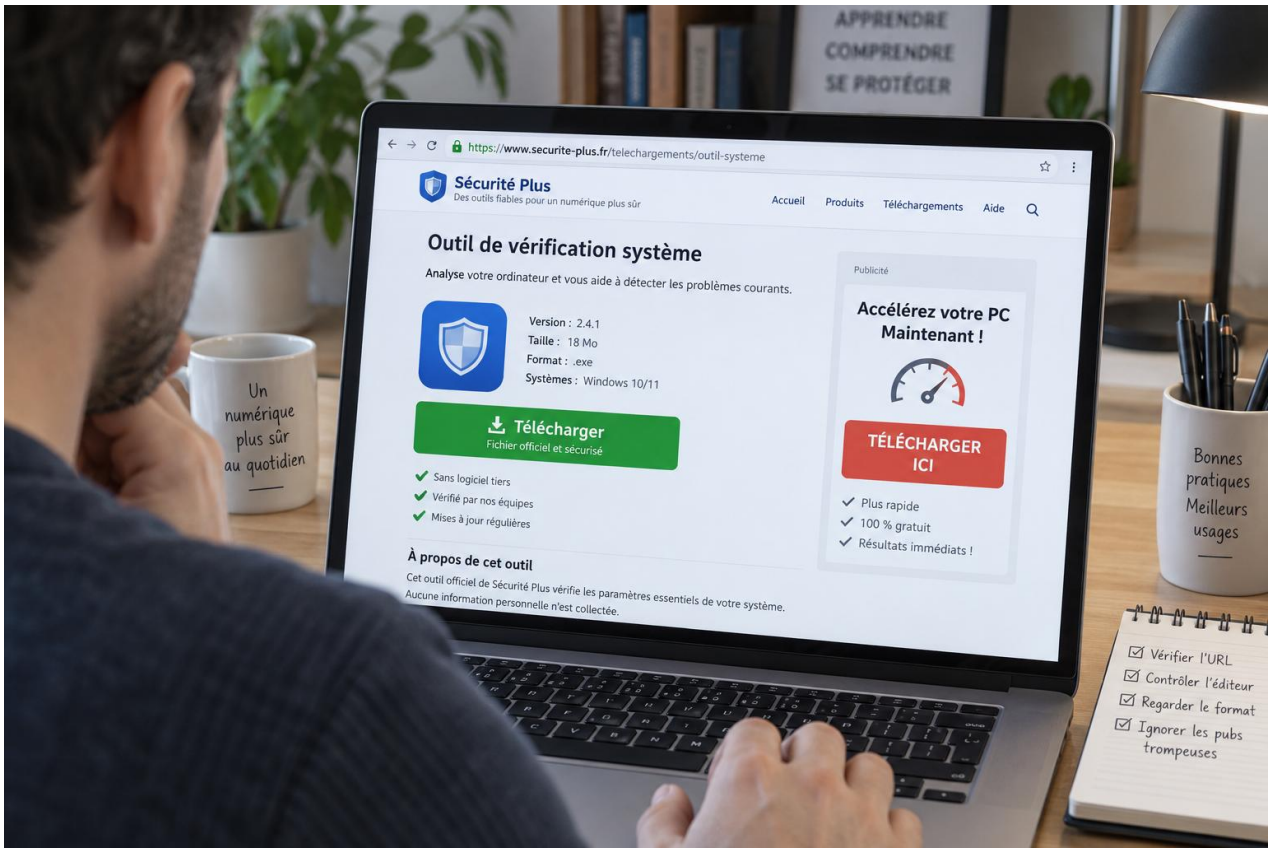
Utiliser une clé USB autorisée

☐ utilisez un support fourni ou validé ;
☐ mettez la protection antivirus à jour ;
☐ désactivez l'exécution automatique ;
☐ analysez la clé avant d'ouvrir les fichiers ;
☐ n'exécutez pas un programme inattendu ;
☐ éjectez le support correctement ;
☐ chiffrez les données sensibles selon les règles applicables.

À éviter

Ne mélangez pas les usages personnels et professionnels sur le même support sans autorisation.

Télécharger depuis la bonne source



Sur une page de téléchargement, distinguez le bouton officiel des publicités trompeuses.

VÉRIFICATION Contrôlez l'adresse du site, l'éditeur, le nom du fichier et son extension.

Contrôler un téléchargement

Avant

- Ouvrez le site officiel par votre chemin habituel ;
- Evitez les bibliothèques inconnues et les versions piratées ;
- Lisez le nom, la version et la compatibilité ;
- Repérez les boutons publicitaires.

Après

- Analysez le fichier si nécessaire ;
- Vérifiez l'extension ;
- Refusez les logiciels supplémentaires proposés ;
- Supprimez le programme d'installation devenu inutile.

Mémo des douze réflexes

☐ J’installe les mises à jour de sécurité.
☐ Je redémarre quand cela est nécessaire.
☐ Je verrouille mes appareils.
☐ Je vérifie la protection antivirus.
☐ Je traite les alertes sans autoriser au hasard.
☐ Je choisis les applications depuis une source officielle.
☐ Je limite les autorisations.
☐ Je sécurise le routeur et le Wi-Fi.
☐ Je reste prudent sur un Wi-Fi public.
☐ Je ne branche aucun support inconnu.
☐ Je vérifie chaque téléchargement.
☐ Je sauvegarde les données importantes.

Ressources publiques

cybermalveillance.gouv.fr • cyber.gouv.fr • cnil.fr

Sauvegarder pour pouvoir repartir

La sauvegarde est utile seulement si elle est régulière, séparée et testée.

Une sauvegarde est une copie indépendante de vos fichiers. Elle protège contre la panne, l’erreur, le vol et certains rançongiciels.

PRINCIPE 3–2–1 : 3 copies • 2 supports différents • 1 copie hors site ou déconnectée.

Organiser et tester ses sauvegardes

Plan minimal

QUESTION	VOTRE RÉPONSE
Quels fichiers sont indispensables ?	_____
Où se trouve la copie principale ?	_____
Où se trouve la copie séparée ?	_____
À quelle fréquence sauvegarder ?	_____
Qui vérifie la restauration ?	_____

Un test indispensable

Choisissez un fichier non sensible, sauvegardez-le, supprimez la copie de test puis restaurez-la. Vérifiez qu'elle s'ouvre correctement.

À RETENIR : Une synchronisation automatique n'est pas toujours une sauvegarde : une suppression ou un chiffrement peut aussi être synchronisé.

Réagir à tout incident

La méthode S.A.V.E.

ÉTAPE	ACTION
Stopper	Cessez l'action risquée et limitez les connexions.
Alerter	Prévenez rapidement le bon contact.
Vérifier	Notez les faits, l'heure, les messages et les appareils concernés.
Éviter d'aggraver	Ne supprimez pas de preuves et n'improvisez pas une réparation.

Fiche contact à compléter

Référent / support : _____
Téléphone : _____
Adresse de signalement : _____
Procédure interne située : _____

URGENCE : En cas de fraude bancaire, contactez rapidement l'établissement bancaire par son canal officiel et suivez les démarches appropriées.

Le mot de passe : votre première clé

Un mot de passe solide est long, unique et géré avec méthode.

Un bon mot de passe ne doit pas être devinable à partir de votre nom, de votre date de naissance ou d'informations publiques.

RÈGLE SIMPLE : Un mot de passe différent pour chaque service important. Si l'un fuit, les autres restent protégés.

Le rôle du mot de passe

Le mot de passe prouve que vous connaissez un secret associé à un compte. Il doit résister aux devinettes, aux essais automatisés et aux fuites de données.

Trois qualités essentielles

QUALITÉ	SIGNIFICATION
Long	Il offre beaucoup de combinaisons possibles.
Unique	Il n'est utilisé sur aucun autre service.
Imprévisible	Il ne contient pas d'information facile à deviner.

À RETENIR La longueur et l'unicité sont plus importantes qu'une transformation compliquée d'un mot courant.

Les erreurs fréquentes

- Utiliser le prénom d'un proche ou une date de naissance ;
- Ajouter seulement 1 ou ! A un mot courant ;
- Réutiliser le même secret partout ;
- Partager le mot de passe par courriel ou messagerie ;
- Le laisser visible sur un post-it ;
- Enregistrer ses secrets dans un document non protégé.

Pourquoi la réutilisation est risquée

Si un service subit une fuite, le même identifiant et le même mot de passe peuvent être testés automatiquement sur d'autres comptes.

RÉFLEXE Un compte égale un mot de passe différent.

Construire un mot de passe solide

Privilégiez la longueur

Utilisez une phrase de passe longue ou une suite aléatoire créée par un gestionnaire. Évitez les expressions célèbres, les suites de clavier et les variantes prévisibles.

Exemple pédagogique

À éviter : Soleil2026! • Principe préférable : plusieurs mots sans lien, suffisamment longs, avec une construction personnelle.

NE COPIEZ PAS Les exemples imprimés dans ce guide ne doivent jamais devenir vos vrais mots de passe.

Ne les partagez pas

Ni un collègue, ni une banque, ni un support sérieux ne doit vous demander votre mot de passe complet par message ou par téléphone.

Créer une phrase de passe

Une phrase de passe associe plusieurs mots sans lien évident. Elle est longue, mémorisable et différente pour chaque compte important.

Méthode pédagogique

choisissez plusieurs mots qui ne forment pas une expression connue ;
ajoutez une construction personnelle si le service l'exige ;
évitez noms, dates, citations et informations publiques ;
ne reprenez jamais les exemples d'un cours ou d'un site.

EXEMPLE DE PRINCIPE Objet + lieu + action + détail inattendu. Cet exemple décrit une méthode, pas un mot de passe à utiliser.

Vérifier sans révéler

Avant de valider

☐ la longueur est-elle suffisante ?
☐ ce secret est-il totalement unique ?
☐ peut-on le deviner à partir de mes réseaux sociaux ?
☐ ai-je prévu comment le conserver ?

Indicateur de robustesse

Une jauge affichée par un service peut aider, mais elle ne garantit pas qu'un mot de passe est unique ou inconnu. Ne testez jamais votre vrai mot de passe sur un site inconnu.

BON RÉFLEXE Utilisez le générateur intégré à un gestionnaire de confiance.

Quand changer un mot de passe

Il n'est pas nécessaire de changer un mot de passe uniquement parce qu'une date est arrivée, sauf règle interne. Changez-le sans attendre si vous suspectez une fuite, un hameçonnage, un appareil compromis ou une connexion inconnue.

Ordre conseillé

- Utilisez un appareil sain ;
- Changez d'abord le mot de passe de la messagerie ;
- Déconnectez les sessions inconnues ;
- Activez ou renforcez la double authentification ;
- Vérifiez les options de récupération.

URGENT Si le même mot de passe a été réutilisé, remplacez-le sur tous les comptes concernés.

Utiliser un gestionnaire de mots de passe

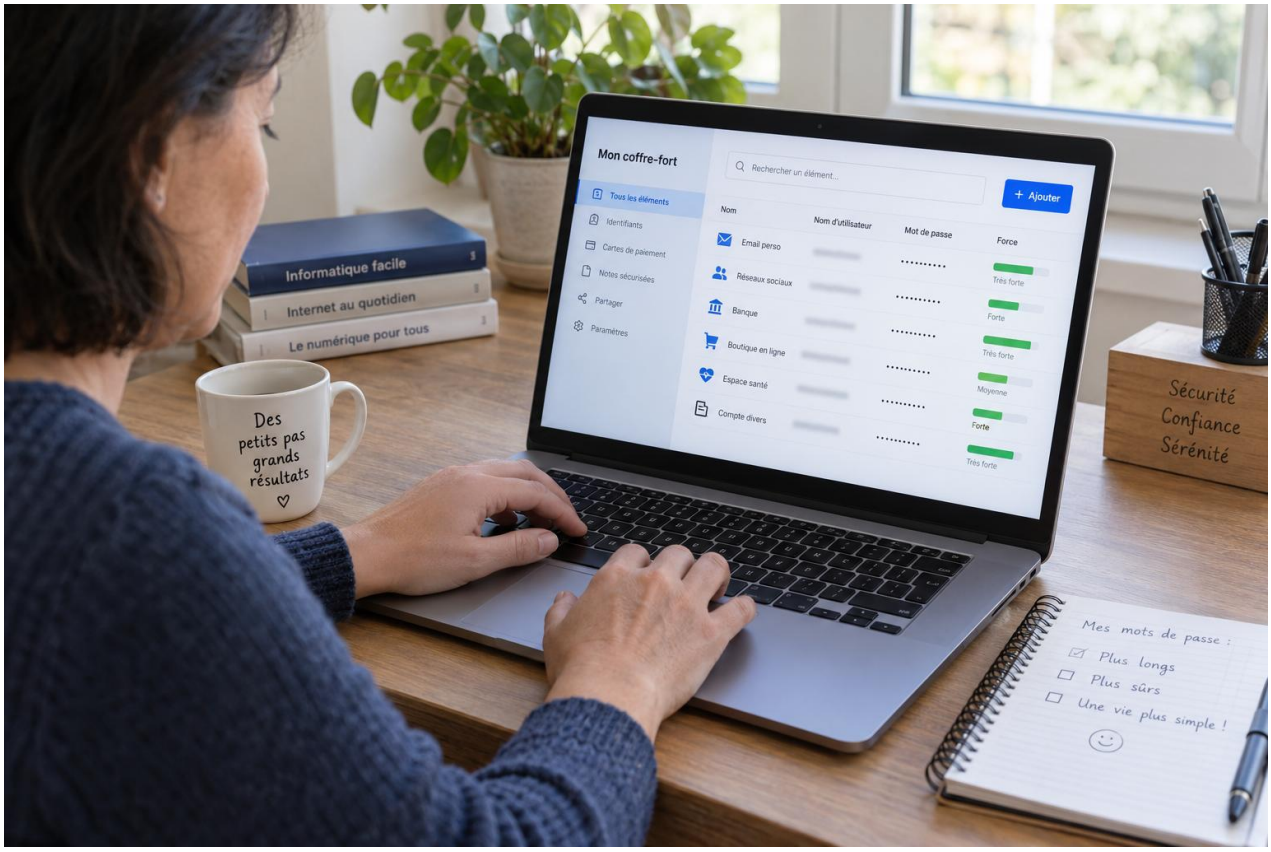
Un gestionnaire mémorise vos mots de passe dans un coffre chiffré. Vous retenez surtout le mot de passe principal.

Mise en place

- Choisissez un outil validé par votre organisation ;
- Créez un mot de passe principal long et unique ;
- Activez l'authentification multi facteur ;
- Enregistrez progressivement vos comptes ;
- Utilisez le générateur pour créer des mots de passe uniques ;
- Gardez la solution de récupération dans un endroit sûr.

POINT DE VIGILANCE : Le mot de passe principal protège tout le coffre : ne le réutilisez nulle part ailleurs.

Découvrir le gestionnaire



Le gestionnaire rassemble les identifiants dans un coffre protégé.

Le gestionnaire crée, mémorise et renseigne des mots de passe uniques. Il réduit la tentation d'utiliser partout le même secret.

CHOIX En entreprise, utilisez uniquement la solution validée par l'organisation.

Installer et préparer le coffre

☐ choisissez la solution autorisée ou reconnue ;
☐ installez-la depuis la source officielle ;
☐ créez un mot de passe principal très long et unique ;
☐ activez immédiatement la double authentification ;
☐ repérez la procédure de récupération ;
☐ enregistrez les codes de secours hors du coffre.

POINT CRITIQUE Le mot de passe principal ne doit être utilisé nulle part ailleurs.

Enregistrer un compte

Pas à pas

- Ouvrez le service depuis son adresse habituelle ;
- Créez une nouvelle entrée dans le gestionnaire ;
- Indiquez le nom du service et l'identifiant ;
- Générez un mot de passe long et aléatoire ;
- Enregistrez puis testez la connexion ;
- Supprimez toute ancienne copie non protégée.

VÉRIFICATION Fermez la session, reconnectez-vous avec le gestionnaire et confirmez que tout fonctionne.

Remplissage automatique et faux sites

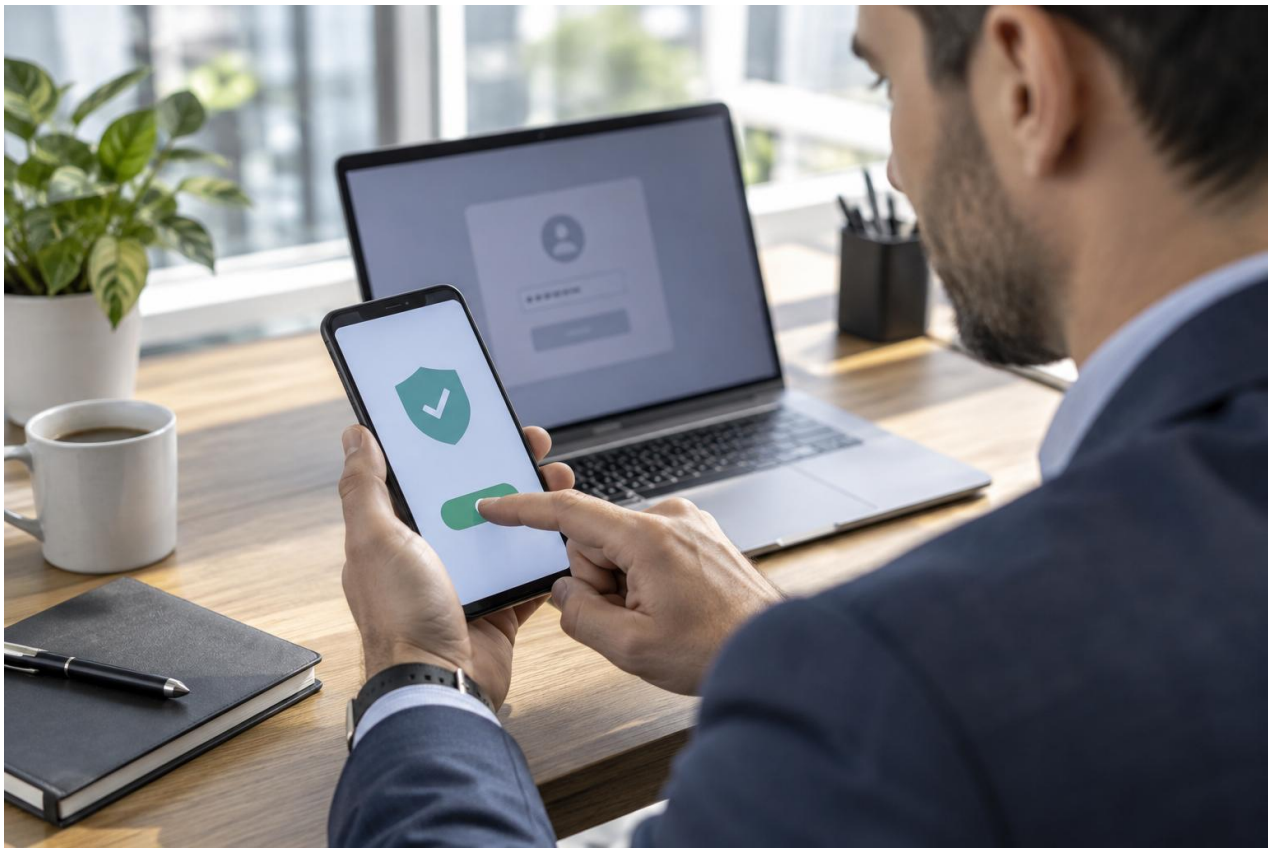
Le remplissage automatique peut aussi servir d'alerte. Si le gestionnaire ne reconnaît pas le domaine, vérifiez l'adresse avant toute saisie.

À contrôler

- Le nom de domaine exact ;
- La présence d'une redirection inattendue ;
- L'origine du lien reçu ;
- Le compte proposé par le gestionnaire.

ATTENTION Ne forcez pas le collage d'un mot de passe sur une page que le gestionnaire ne reconnaît pas.

Ajouter une deuxième vérification

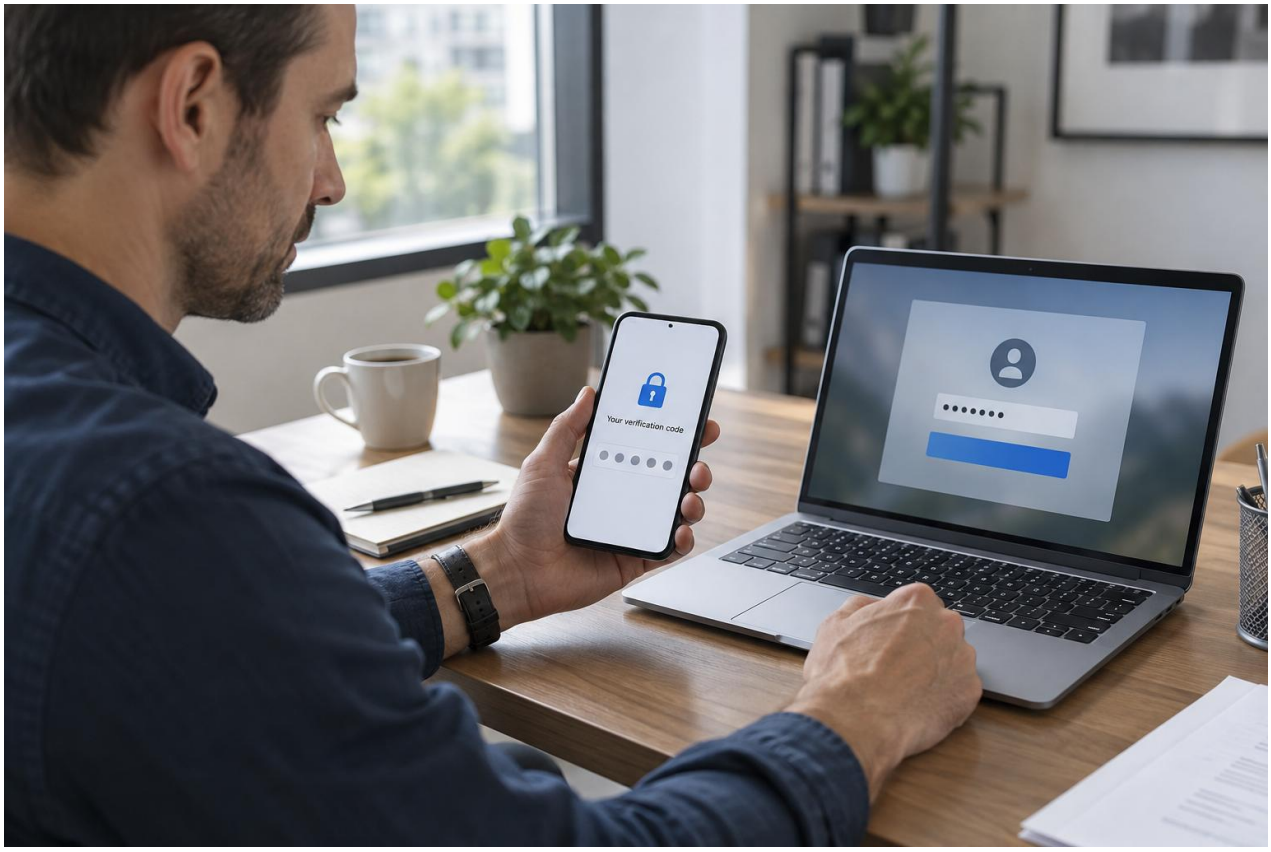


Après le mot de passe, une seconde preuve confirme que c'est bien vous.

L'authentification à deux facteurs (2FA) ou multi facteur (MFA) ajoute une seconde preuve : application d'authentification, clé de sécurité, notification ou code à usage unique.

PRIORITÉ : Activez-la d'abord sur votre messagerie, votre gestionnaire de mots de passe, vos comptes bancaires et vos services professionnels.

Comprendre la double authentification



La double authentification ajoute une preuve liée à ce que vous possédez ou à ce que vous êtes. Un mot de passe volé devient alors insuffisant dans de nombreux cas.

Les différentes méthodes

MÉTHODE	À SAVOIR
Application d'authentification	Génère un code temporaire ou valide une demande.
Clé de sécurité	Objet physique très résistant à l'hameçonnage.
Notification	Demande une validation sur un appareil connu.
SMS	Mieux que le mot de passe seul, mais moins robuste que certaines alternatives.
Biométrie	Déverrouille localement un appareil ou une preuve.

CHOIX Utilisez la méthode la plus forte proposée et compatible avec votre situation.

Activer une application d’authentification

Procédure générale

☐ ouvrez la rubrique Sécurité du compte ;
☐ choisissez Authentification à deux facteurs ;
☐ sélectionnez Application d’authentification ;
☐ scannez le QR code avec l’application ;
☐ saisissez le code temporaire demandé ;
☐ téléchargez ou notez les codes de secours ;
☐ testez une nouvelle connexion.

IMPORTANT Ne photographiez pas et ne partagez pas le QR code d’activation.

Face à une demande de validation

Une notification inattendue peut signifier qu’une personne possède déjà votre mot de passe.

Si vous n’êtes pas à l’origine de la demande

- Refusez la demande ;
- Ne communiquez aucun code ;
- Changez le mot de passe depuis un appareil sain ;
- Déconnectez les sessions inconnues ;
- Prévenez le support si le compte est professionnel.

DANGER Un interlocuteur qui vous demande de lire un code reçu tente peut-être de contourner la protection.

Codes de secours

Les codes de récupération sont conservés séparément et hors de vue.

Un code de secours permet d'accéder au compte lorsque le téléphone ou la clé de sécurité n'est plus disponible. Chaque code est généralement utilisable une seule fois.

RÈGLE Conservez-les hors du compte qu'ils permettent de récupérer.

Conserver les codes en sécurité

☐ imprimez-les ou notez-les dans un emplacement physique sûr ;
☐ ou stockez-les dans un espace chiffré séparé ;
☐ ne les laissez pas dans le dossier Téléchargements ;
☐ ne les envoyez pas par courriel ;
☐ remplacez la série après utilisation ou suspicion de copie.

À éviter

Une photo dans la galerie du téléphone, une capture d'écran synchronisée ou un document ouvert dans le cloud peuvent être accessibles au même moment que le compte.

Récupération du compte

Préparez avant la panne

- Vérifiez l'adresse et le numéro de récupération ;
- Ajoutez une seconde méthode de double authentification ;
- Conservez les codes de secours ;
- Notez le canal officiel du support ;
- Supprimez les anciennes méthodes devenues inaccessibles.

TEST Vérifiez les options, mais ne lancez pas une récupération réelle sans nécessité.

Activité Construire son plan

Complétez sans écrire aucune donnée secrète.

COMPTE PRIORITAIRE	ACTION À PRÉVOIR
Messagerie	_____
Gestionnaire	_____
Banque ou administration	_____
Compte professionnel	_____
Réseau social	_____

Mes prochaines actions

☐ J’installe ou je vérifie mon gestionnaire.
☐ J’active le 2FA sur ma messagerie.
☐ Je range mes codes de secours.
☐ Je contrôle les sessions ouvertes.

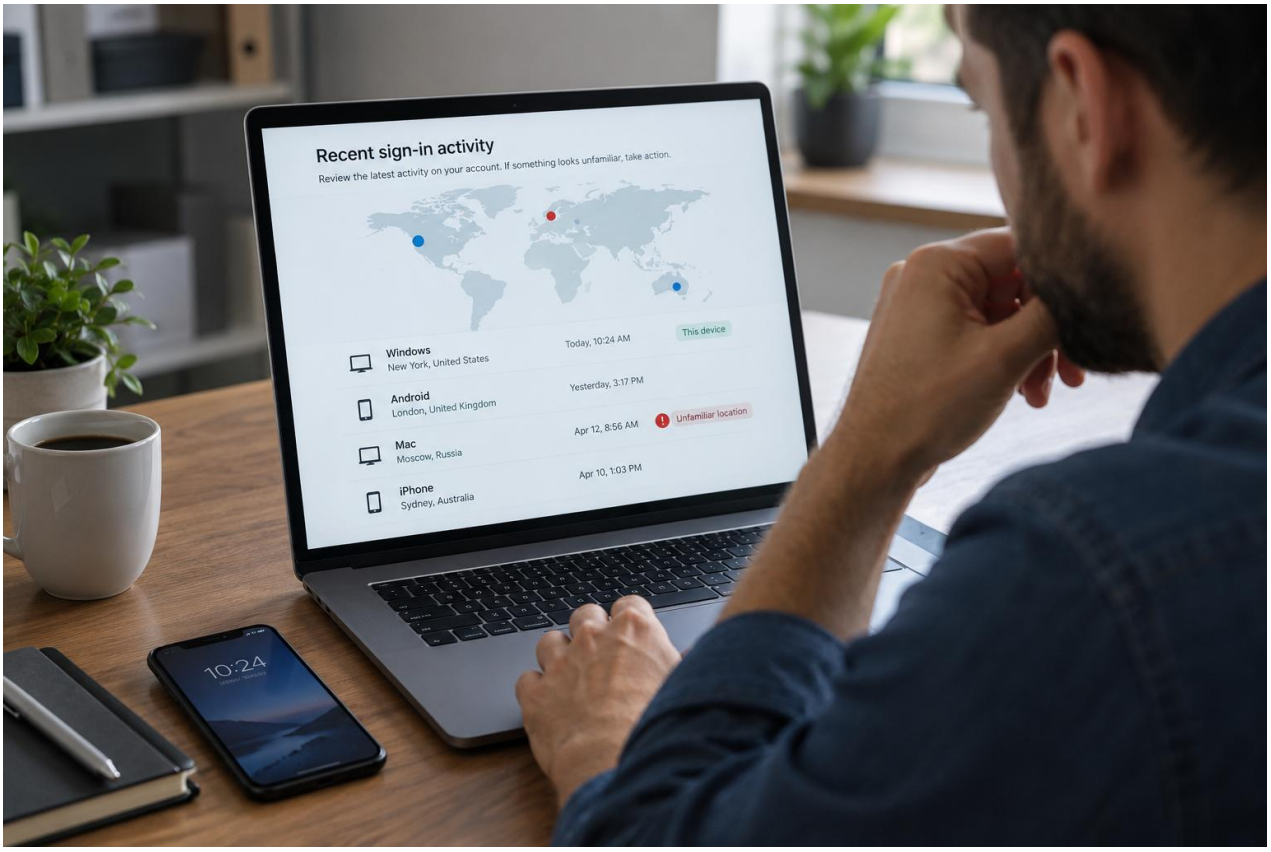
Mémo des dix réflexes

☐ Un mot de passe long et unique par service.
☐ Un gestionnaire validé et protégé.
☐ Un mot de passe principal jamais réutilisé.
☐ La double authentification sur les comptes importants.
☐ Aucun code communiqué par téléphone ou message.
☐ Les demandes inattendues toujours refusées.
☐ Des codes de secours conservés séparément.
☐ Des méthodes de récupération à jour.
☐ Des sessions contrôlées régulièrement.
☐ Un signalement rapide en cas de doute.

Ressources publiques

cyber.gouv.fr • cybermalveillance.gouv.fr • cnil.fr

Contrôler les connexions



Une activité inconnue doit être examinée puis traitée rapidement.

Les services importants proposent souvent une liste des appareils, lieux approximatifs et sessions connectées.

À SAVOIR Une localisation peut être approximative. Croisez la date, l'heure, l'appareil et votre activité.

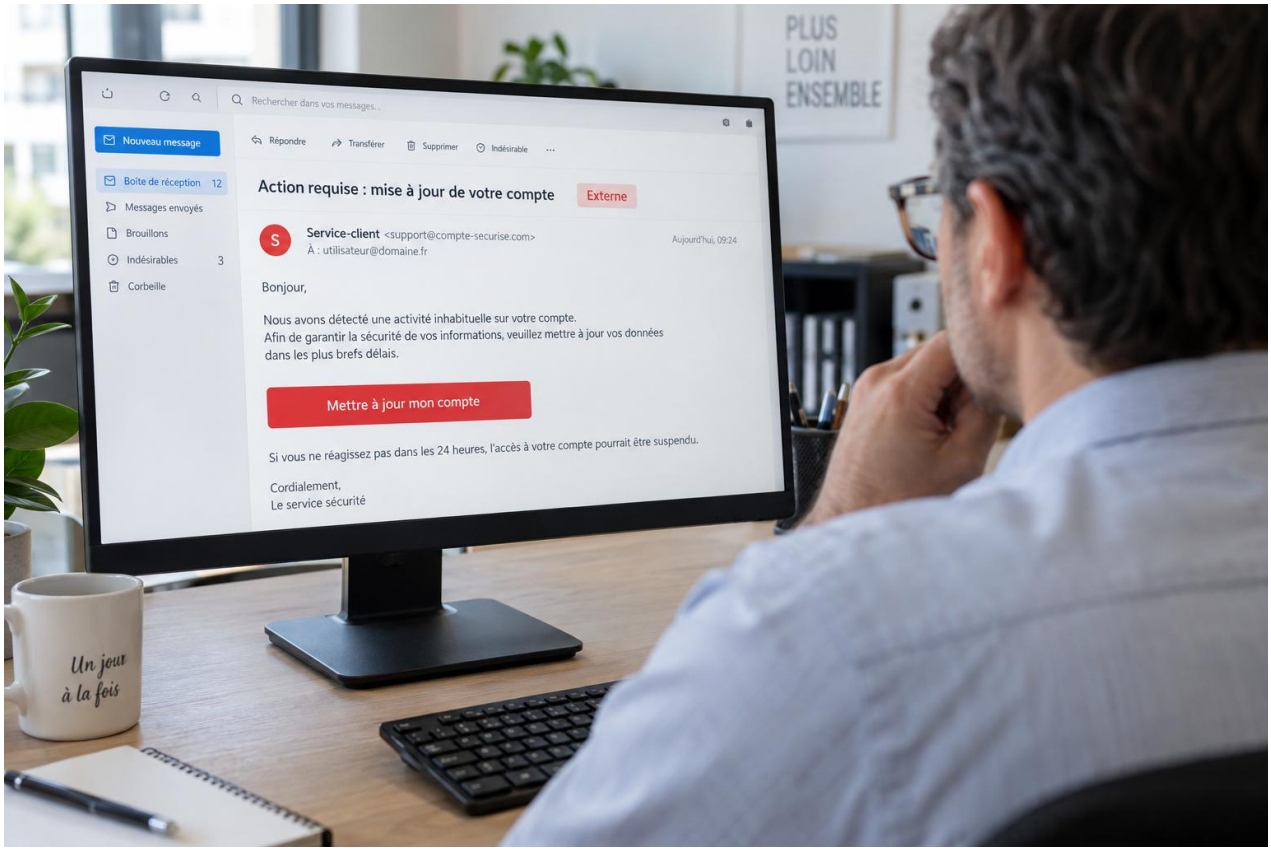
Déconnecter une session inconnue

- Faites une capture ou notez les informations utiles ;
- Déconnectez la session inconnue ;
- Changez le mot de passe ;
- Vérifiez les règles de transfert de messagerie ;
- Contrôlez les méthodes de récupération ;
- Révoquez les applications inconnues ;
- Prévenez le support si nécessaire.

MESSAGERIE Vérifiez-la en premier : elle permet souvent de réinitialiser les autres comptes.

Hameçonnage et arnaques numériques

Faux courriels, SMS frauduleux, QR codes, faux sites et ingénierie sociale



Un message peut sembler professionnel tout en cherchant à provoquer un clic rapide.

Comprendre l'hameçonnage

L'hameçonnage est une tentative de tromper une personne pour lui faire révéler une information, ouvrir un fichier, visiter un faux site ou effectuer une action dangereuse.

Ce que recherche l'arnaqueur

CIBLE	EXEMPLE
Identifiants	Adresse électronique et mot de passe
Codes	Code de double authentification ou de validation
Argent	Paiement, virement ou achat de coupons
Accès	Ouverture d'une pièce jointe ou installation d'un outil
Informations	Identité, coordonnées ou données professionnelles

Les leviers de manipulation

L’arnaque repose souvent moins sur la technique que sur une émotion qui empêche de vérifier.

LEVIER	MESSAGE TYPIQUE	BON RÉFLEXE
Urgence	Agissez dans 30 minutes	Faire une pause
Peur	Votre compte sera bloqué	Ouvrir le site habituel
Gain	Vous avez gagné	Ne rien payer
Autorité	Le directeur exige ce virement	Confirmer autrement
Aide	Je suis en difficulté	Contacter la personne connue

À RETENIR Une demande urgente mérite davantage de vérifications, pas moins.

La méthode STOP

S Suspendre l’action

Ne cliquez pas, ne répondez pas et ne communiquez aucun code.

T Trouver les indices

Examinez l’expéditeur, le contexte, l’adresse, le lien, la pièce jointe et la demande.

O Ouvrir par le chemin habituel

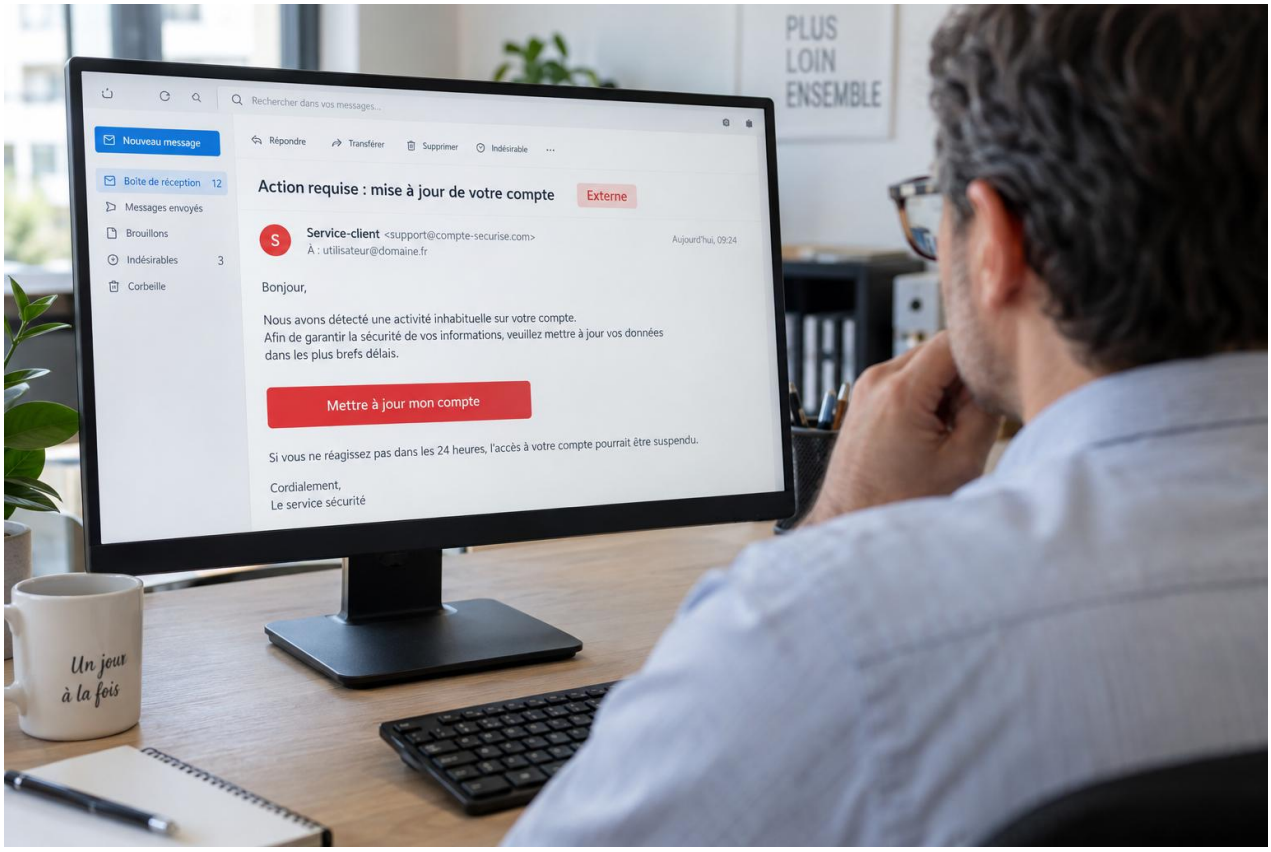
Utilisez votre favori, l’application officielle ou une adresse saisie vous-même.

P Prévenir et signaler

Alertez le service concerné, votre référent informatique ou la plateforme adaptée.

RÉFLEXE Le doute est une raison suffisante pour interrompre l’action.

Repérer un faux courriel



Observez l'adresse de l'expéditeur, l'urgence, la formule générique et le bouton proposé.

QUESTION Attendiez-vous réellement ce message et cette demande ?

Examiner l'expéditeur

Le nom affiché peut être imité. L'adresse complète est plus utile, mais elle doit elle aussi être examinée avec prudence.

Contrôle pas à pas

☐ affichez l'adresse complète de l'expéditeur ;
☐ lisez le domaine après le symbole @ ;
☐ repérez les lettres ajoutées, inversées ou remplacées ;
☐ comparez avec une adresse déjà connue ;
☐ méfiez-vous d'une adresse gratuite pour une demande professionnelle.

ATTENTION Un nom familier ne prouve pas que l'adresse est authentique.

Examiner un lien sans cliquer

Sur ordinateur

- Placez le pointeur sur le lien sans appuyer ;
- Lisez l'adresse affichée en bas de la fenêtre ;
- Repérez le véritable nom de domaine ;
- Annulez si l'adresse est masquée, inattendue ou mal orthographiée.

Sur smartphone

- N'effectuez pas un appui bref ;
- Si nécessaire, utilisez un appui prolongé pour afficher l'aperçu ;
- Ne choisissez pas ouvrir tant que l'adresse n'est pas vérifiée.

PLUS SÛR Fermez le message puis ouvrez le service depuis son application ou votre favori.

Pièces jointes et fausses factures

Une pièce jointe peut contenir un programme malveillant ou conduire vers une fausse page de connexion.

Signaux d'alerte

- Facture, livraison ou candidature inattendue ;
- Fichier compressé ou format inhabituel ;
- Demande d'activer les macros ou le contenu ;
- Mot de passe fourni dans le message pour ouvrir le fichier ;
- Pression pour traiter le document immédiatement.

RÈGLE N'ouvrez pas une pièce jointe inattendue avant d'avoir confirmé son origine par un autre canal.

Répondre au faux courriel

Ce qu'il faut faire

☐ ne cliquez sur aucun bouton ;
☐ ne répondez pas à l'expéditeur ;
☐ utilisez la fonction Signaler comme hameçonnage ;
☐ prévenez le service informatique si le compte est professionnel ;
☐ supprimez le message après le signalement.

Ce qu'il faut éviter

Ne transférez pas le message à vos collègues sans précaution : le lien dangereux resterait actif.

Reconnaître un SMS frauduleux

Petit paiement, urgence et lien raccourci : trois indices fréquents dans un SMS frauduleux.

RÉFLEXE Ne touchez pas le lien. Ouvrez directement l'application officielle du service.

SMS et messageries instantanées

Les arnaques circulent aussi par messagerie, réseau social ou conversation de groupe. Un compte connu peut avoir été piraté.

Situations fréquentes

- Colis bloqué ou frais de livraison ;
- Amende, remboursement ou carte vitale ;
- Proche ayant changé de numéro ;
- Vote, concours ou cadeau ;
- Offre d'emploi trop avantageuse ;
- Demande d'achat de cartes prépayées.

VÉRIFIER Contactez la personne ou l'organisme avec un numéro déjà enregistré, jamais avec celui du message.

Appels frauduleux et faux support

Aucun interlocuteur légitime ne doit obtenir votre code de vérification.

DANGER Un code reçu par SMS ou application est personnel et temporaire. Ne le dictez jamais.

Ingénierie sociale au téléphone

L'interlocuteur peut se présenter comme un conseiller bancaire, un technicien, un collègue ou un responsable. Il cherche à gagner votre confiance avant de demander une action.

Réponse conseillée

- Ne confirmez aucune information sensible ;
- Ne donnez aucun code ;
- Ne partagez pas votre écran ;
- Refusez l'installation d'un logiciel à distance ;
- Raccrochez calmement ;
- Rappelez avec le numéro officiel trouvé par vous-même.

Le piège du QR code

Un autocollant peut recouvrir le QR code d'origine et conduire vers un faux paiement.

OBSERVATION Avant de scanner, recherchez une étiquette ajoutée, décollée ou superposée.

Vérifier un QR code

Avant le scan

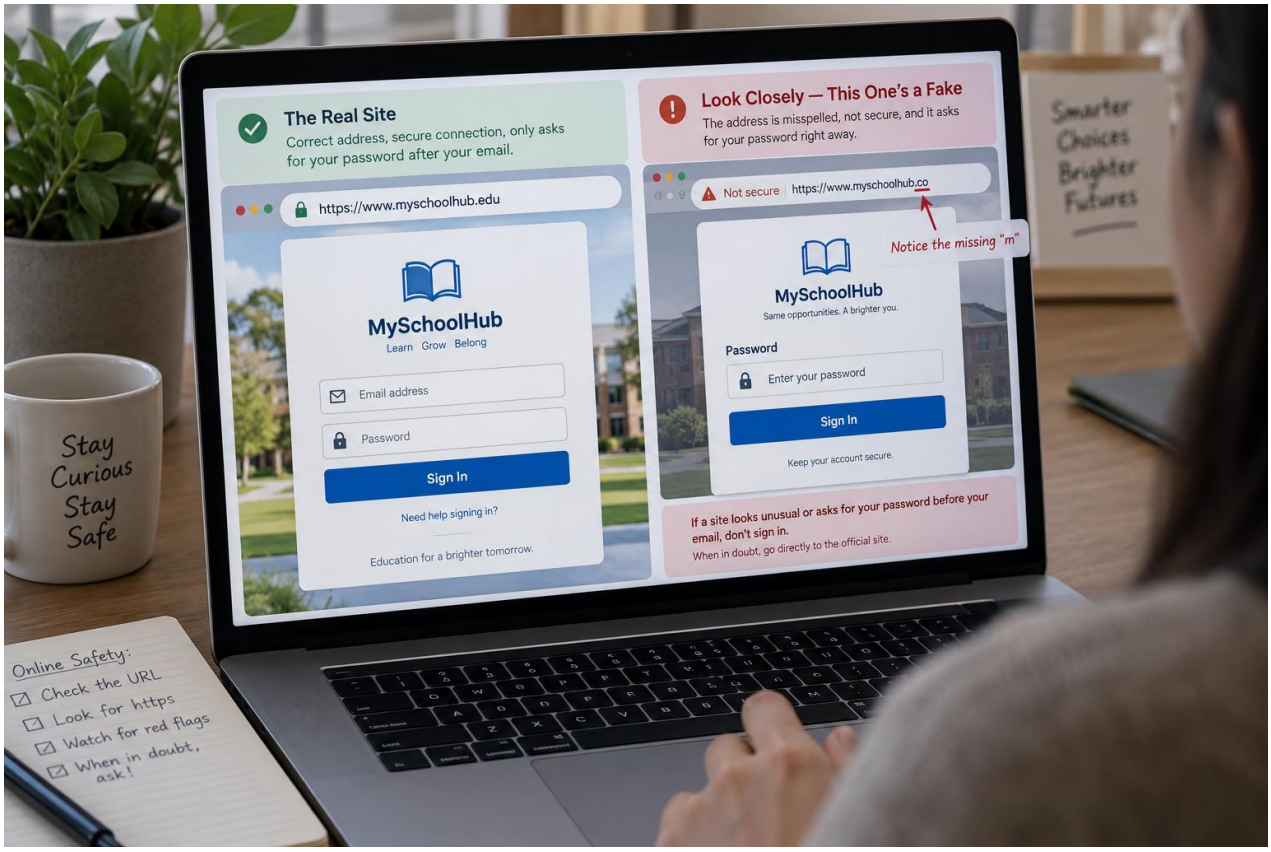
- Contrôlez le support physique ;
- Demandez-vous si un qr code est nécessaire ;
- Préférez l'application officielle quand elle existe.

Après le scan mais avant de continuer

- Lisez l'adresse proposée ;
- Annulez si le domaine est inconnu ;
- Ne saisissez ni mot de passe ni carte bancaire sur une page douteuse ;
- Fermez la page si elle demande une action inattendue.

À SAVOIR Un QR code est un lien invisible : il faut vérifier sa destination.

Reconnaître un faux site



Le domaine est déterminant : l'apparence générale et le cadenas ne suffisent pas.

IMPORTANT Le visuel comporte un exemple fictif. Dans la réalité, examinez toujours l'adresse complète.

Lire une adresse web

Dans une adresse, le domaine principal se trouve juste avant l'extension comme .fr ou .com. Les fraudeurs ajoutent souvent des mots rassurants avant ou après un nom imité.

ADRESSE FICTIVE	ANALYSE
https://compte.exemple.fr	Le domaine principal est exemple.fr
https://exemple.securite-client.net	Le domaine principal est securite-client.net
https://exemp1e.fr	Le chiffre 1 imite la lettre l
https://exemple-fr.com	Le nom ressemble au service, sans être son domaine habituel

NOTE HTTPS chiffre la connexion, mais ne garantit pas que le propriétaire du site est honnête.

Vérifier par un autre chemin

Pour un compte en ligne

- Fermez le message ;
- Ouvrez l'application officielle ;
- Ou saisissez vous-même l'adresse habituelle ;
- Consultez les notifications dans votre espace personnel.

Pour une personne

- Utilisez un numéro déjà connu ;
- Posez une question dont vous connaissez la réponse ;
- En entreprise, appliquez la procédure de validation.

PRINCIPE Ne vérifiez jamais une demande suspecte avec les coordonnées qu'elle contient.

Les demandes de paiement

Un changement de coordonnées bancaires, un virement urgent ou l'achat de cartes cadeaux doivent suivre une procédure de contrôle renforcée.

Double contrôle

☐ comparez avec les informations habituelles ;
☐ contactez le demandeur par un canal indépendant ;
☐ faites valider selon les règles de l'organisation ;
☐ conservez une trace de la vérification.

ALERTE : Une voix, une photo ou une vidéo peuvent être imitées. La procédure reste indispensable.

Si vous avez cliqué

Sans avoir saisi d'information

- Fermez la page ;
- Ne téléchargez rien ;
- Signalez le message ;
- Lancez un contrôle de sécurité si un fichier a été ouvert.
-

Après avoir saisi un mot de passe

- Changez-le immédiatement depuis un appareil sain ;
- Changez aussi les comptes où il était réutilisé ;
- Activez la double authentification ;
- Déconnectez les sessions inconnues ;
- Prévenez le support concerné.

Si vous avez payé ou transmis des données

Réagir sans attendre

- Contactez votre banque par son numéro officiel ;
- Faites opposition si cela est conseillé ;
- Conservez messages, numéros, adresses et preuves ;
- Signalez les faits aux services compétents ;
- Surveillez les comptes et les tentatives d'usurpation.

URGENCE Plus la réaction est rapide, plus les possibilités de protection sont importantes.

Mémo des douze réflexes

☐ Je ralentis face à l'urgence.
☐ Je vérifie le contexte.
☐ J'affiche l'adresse complète de l'expéditeur.
☐ Je survole les liens sur ordinateur.
☐ Je n'ouvre pas une pièce jointe inattendue.
☐ Je n'utilise pas le lien d'un SMS.
☐ Je contrôle le support d'un QR code.
☐ Je lis le domaine du site.
☐ Je ne communique aucun code.
☐ Je vérifie par un autre canal.
☐ Je signale les messages frauduleux.
☐ Après une erreur, je réagis immédiatement.

Ressources publiques

cybermalveillance.gouv.fr • cyber.gouv.fr • cnil.fr • signal-spam.fr

Comprendre le rançongiciel

Écran bloqué : l'utilisateur s'arrête et prévient au lieu d'essayer seul plusieurs manipulations.

Un rançongiciel chiffre ou bloque les fichiers, puis réclame de l'argent. Il peut aussi voler des données avant de les rendre inaccessibles.

OBJECTIF : Limiter la propagation, protéger les sauvegardes et permettre au support d'analyser l'incident.

Réagir à un rançongiciel

Immédiatement

- Déconnectez le câble réseau et coupez le Wi-Fi ;
- Débranchez les supports de sauvegarde reliés ;
- Laissez l'appareil allumé si la procédure interne le demande ;
- Photographiez le message avec un autre appareil ;
- Prévenez le support ou le responsable ;
- N'essayez pas de payer ni de négocier seul.

Ensuite

L'organisation identifie les appareils touchés, sécurise les comptes, restaure depuis des sauvegardes saines et réalise les signalements nécessaires.

À NE PAS FAIRE : Ne branchez pas le disque de sauvegarde sur un appareil possiblement infecté.

Comprendre un rançongiciel

Un rançongiciel est un logiciel malveillant qui bloque ou chiffre des données et réclame une rançon. Une attaque peut aussi comporter un vol d'informations et une menace de publication.

SIGNE	EXEMPLE
Fichiers impossibles à ouvrir	Extension inhabituelle ou contenu illisible
Message de rançon	Demande de paiement ou compte à rebours
Activité anormale	Ordinateur très lent ou fenêtres inattendues
Plusieurs postes touchés	Partages réseau soudainement inaccessibles
Comptes perturbés	Mot de passe refusé ou connexion inconnue

Reconnaître les signaux faibles

☐ alerte antivirus inhabituelle ;
☐ fichiers renommés sans action ;
☐ applications qui se ferment seules ;
☐ ventilateur ou disque très actif ;
☐ message d'un collègue signalant le même problème ;
☐ connexion ou demande MFA non initiée ;
☐ courriel envoyé depuis votre compte sans vous.

NE PAS ATTENDRE : Un doute signalé tôt coûte moins cher qu'un incident caché.

Fiche réflexe rançongiciel

IMMÉDIATEMENT	ENSUITE
Arrêter l'action	Alerter le contact prévu
Débrancher réseau et couper Wi-Fi	Noter heure et symptômes
Ne pas éteindre sauf consigne	Préserver messages et écran
Ne pas payer ni répondre	Attendre les instructions
Ne pas connecter de sauvegarde	Rester joignable

Mémo des douze réflexes

☐ Je connais le contact sécurité.
☐ Je verrouille ma session.
☐ Je protège mes comptes avec la double authentification.
☐ Je n'installe rien sans autorisation.
☐ Je vérifie liens, pièces jointes et destinataires.
☐ Je refuse toute demande MFA inattendue.
☐ J'utilise uniquement les outils approuvés.
☐ J'isole rapidement un poste suspect.
☐ J'alerte sans cacher l'erreur.
☐ Je préserve les éléments utiles.
☐ Je n'improvise pas une réparation.
☐ Je suis le plan de réaction et les consignes internes.

Ressources officielles

cyber.gouv.fr • cybermalveillance.gouv.fr • cnil.fr

Virus informatiques et logiciels malveillants

Virus, vers, chevaux de Troie, logiciels espions, publiciels, botnets et menaces mobiles

Le terme logiciel malveillant désigne tout programme conçu pour nuire, espionner, voler, bloquer ou détourner un appareil. Un virus est une catégorie particulière : il s'attache à un fichier ou à un programme et se reproduit lorsque celui-ci est exécuté.

TERME	DÉFINITION SIMPLE
Logiciel malveillant	Nom général de toutes les menaces logicielles
Virus	Infecte un fichier ou un programme hôte
Infection	Présence et activité du programme malveillant
Charge utile	Action réalisée : vol, destruction, espionnage ou blocage

Comment un logiciel malveillant entre

- Pièce jointe ou lien frauduleux ;
- Logiciel piraté ou faux installateur ;
- Fausse mise à jour ;
- Site compromis ;
- Clé usb inconnue ;
- Appareil ou application non mis à jour ;
- Mot de passe volé donnant accès au système.

RÉFLEXE : Un fichier peut paraître normal tout en contenant un programme malveillant.

Le cycle d’une infection

ÉTAPE	CE QUI SE PASSE
Entrée	Le fichier ou l’application atteint l’appareil
Exécution	L’utilisateur ou le système lance le code
Installation	Le programme se cache ou crée un démarrage automatique
Action	Il espionne, chiffre, détruit ou détourne
Propagation	Il tente parfois d’atteindre d’autres appareils
Persistance	Il cherche à rester actif après un redémarrage

Les objectifs des attaquants

- Voler des identifiants et mots de passe ;
- Récupérer des données personnelles ou professionnelles ;
- Obtenir une rançon ;
- Utiliser la puissance de calcul ;
- Envoyer du spam ;
- Espionner l′activité ;
- Perturber ou arrêter un service ;
- Ouvrir une porte pour une attaque ultérieure.

À RETENIR : Le même programme peut cumuler plusieurs objectifs.

Vue d’ensemble des familles

Virus, ver, cheval de Troie et logiciel espion utilisent des mécanismes différents et nécessitent une analyse adaptée.

VOCABULAIRE : Tous sont des logiciels malveillants, mais tous ne sont pas des virus au sens strict.

Le virus informatique

Le virus se fixe à un fichier, un document à macro ou un programme. Il devient actif lorsque l’élément infecté est ouvert et peut contaminer d’autres fichiers.

CARACTÉRISTIQUE	EXEMPLE
Besoin d’un hôte	Document ou programme infecté
Déclenchement	Ouverture ou exécution
Propagation	Copie vers d’autres fichiers
Conséquence	Altération, suppression ou ajout de code

PRÉVENTION : N’activez pas les macros d’un document reçu sans raison vérifiée.

Le ver informatique

Le ver se propage automatiquement entre des appareils ou des réseaux en exploitant une faiblesse. Il n'a pas toujours besoin qu'un utilisateur ouvre un fichier.

- Se copie sur plusieurs machines ;
- Peut saturer le réseau ;
- Profite souvent d'un système non mis à jour ;
- Peut transporter une autre charge malveillante.

PROTECTION : Appliquez rapidement les mises à jour et limitez les communications inutiles entre équipements.

Le cheval de Troie

Le cheval de Troie se présente comme un programme utile ou légitime, mais exécute une action cachée. Il peut installer une porte dérobée, voler des données ou télécharger d'autres menaces.

APPARENCE	ACTION CACHÉE
Jeu ou utilitaire gratuit	Installe un accès distant
Fausse mise à jour	Télécharge un logiciel espion
Pièce jointe de facture	Vole des identifiants
Application piratée	Modifie les réglages de sécurité

Le logiciel espion

Un logiciel espion collecte discrètement des informations : navigation, identifiants, messages, localisation ou activité du clavier.

- Enregistre les habitudes ;
- Capture parfois l'écran ;
- Surveille les communications ;
- Transmet des données à distance ;
- Peut rester discret longtemps.

SIGNE POSSIBLE : Demandes d'autorisation excessives, consommation réseau inhabituelle ou compte utilisé à votre insu.

L'enregistreur de frappes

Un enregistreur de frappes, ou keylogger, mémorise ce qui est saisi au clavier. Il peut viser les mots de passe, les coordonnées bancaires et les messages.

- Utiliser la double authentification ;
- Eviter les appareils inconnus ou publics ;
- Maintenir le système et l'antivirus à jour ;
- Changer les mots de passe depuis un appareil sain après une infection.

ATTENTION : Changer un mot de passe depuis l'appareil infecté peut permettre de le voler à nouveau.

Le publiciel

Le publiciel affiche des publicités imposées, modifie parfois le navigateur ou collecte des habitudes. Tous les logiciels publicitaires ne sont pas malveillants, mais un comportement intrusif doit être traité.

- Fenêtres publicitaires nombreuses ;
- Page d′accueil modifiée ;
- Extension inconnue ;
- Redirections vers d′autres sites ;
- Ralentissements.

NE CLIQUEZ PAS : Une fausse alerte demandant d'appeler un support peut être une arnaque.

La porte dérobée

Une porte dérobée permet à un attaquant de revenir dans le système en contournant les accès habituels. Elle peut être installée par un cheval de Troie ou après le vol d'un compte administrateur.

RISQUE	MESURE
Accès persistant	Réinstallation ou remédiation contrôlée
Commandes à distance	Isolement réseau
Vol de données	Analyse des comptes et journaux
Nouvelle infection	Correction de la cause initiale

Le rootkit

Un rootkit cherche à cacher la présence d'un attaquant ou d'autres programmes malveillants en modifiant profondément le système. Sa détection et sa suppression exigent souvent une intervention spécialisée.

ENTREPRISE : Ne lancez pas plusieurs outils de nettoyage au hasard. Préservez le poste et suivez la procédure du support.

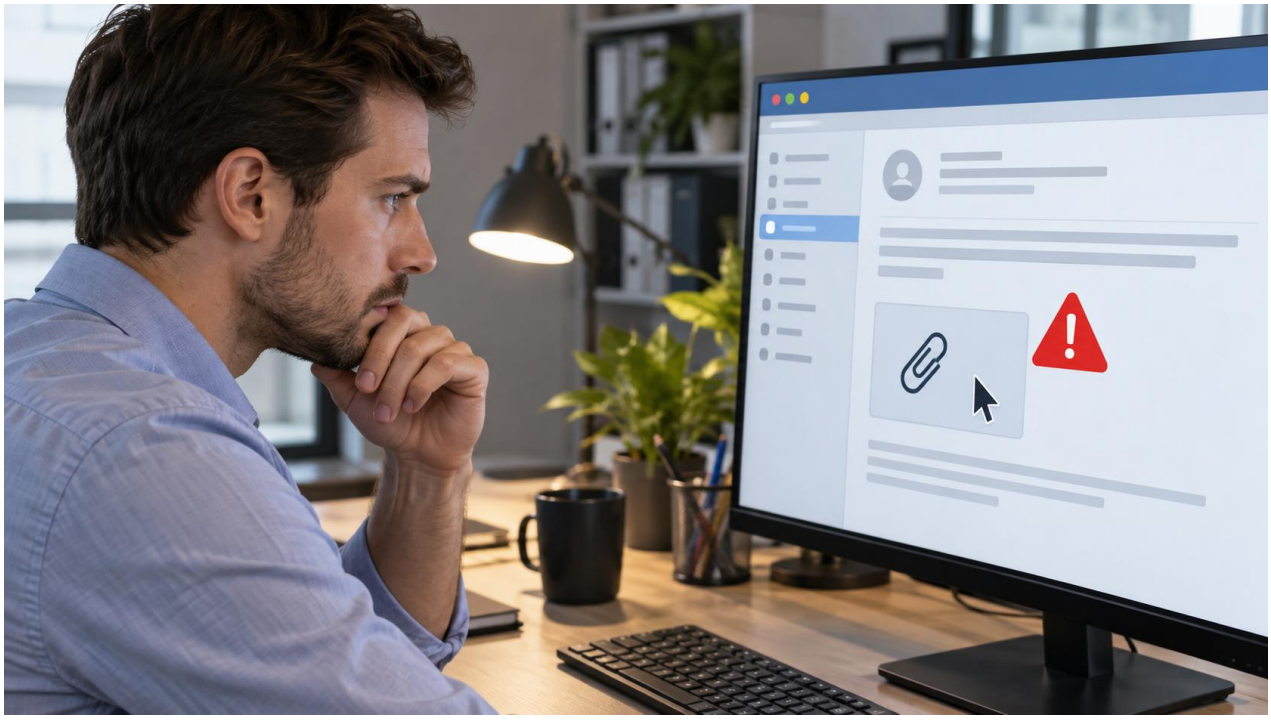
Le bot et le botnet

Un appareil transformé en bot reçoit des ordres à distance. Un ensemble d'appareils compromis forme un botnet.

UTILISATION DU BOTNET	CONSÉQUENCE
Envoi de spam	Réputation et messagerie bloquées
Attaque par déni de service	Sites rendus indisponibles
Diffusion de logiciels malveillants	Nouvelles victimes
Fraude publicitaire	Trafic artificiel
Vol automatisé	Comptes et données exposés

Les menaces par document

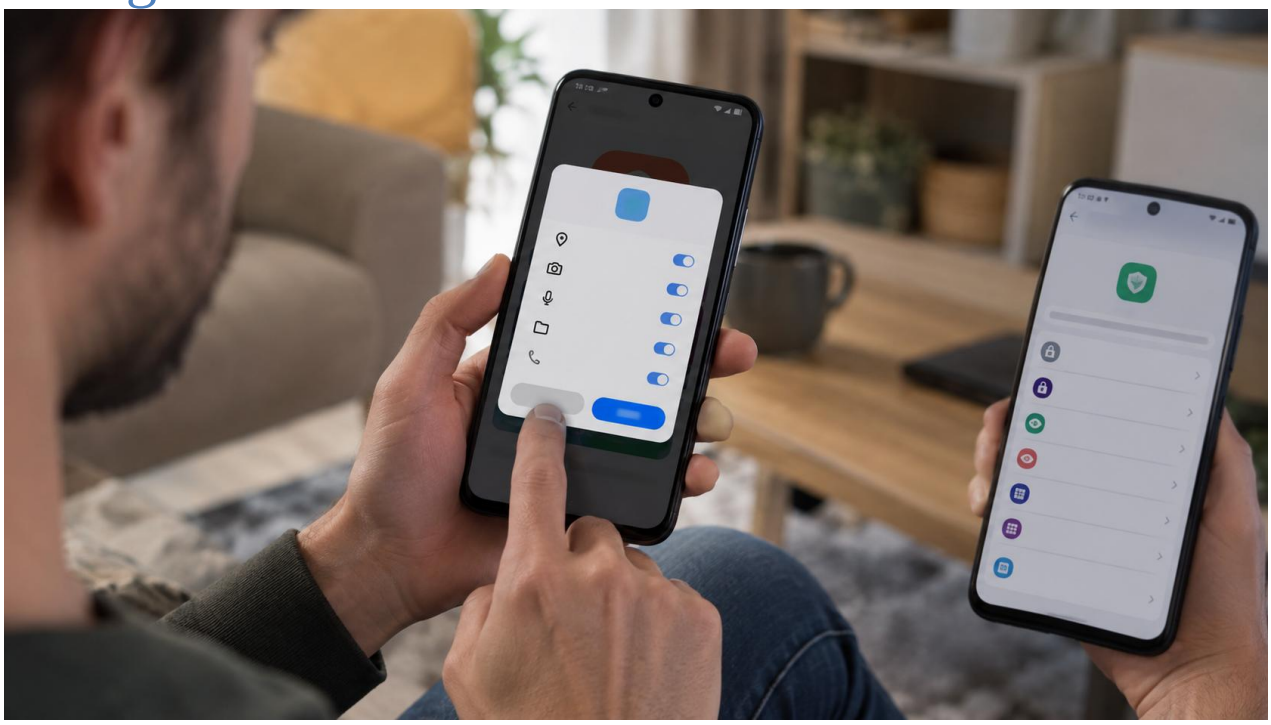
Un document bureautique peut contenir une macro, un lien ou un objet intégré capable de lancer une action malveillante.



Une pièce jointe inattendue doit être vérifiée par un autre canal avant toute ouverture.

MACROS : N'activez jamais le contenu parce qu'un document affiche simplement « Activez la modification ».

Les logiciels malveillants mobiles



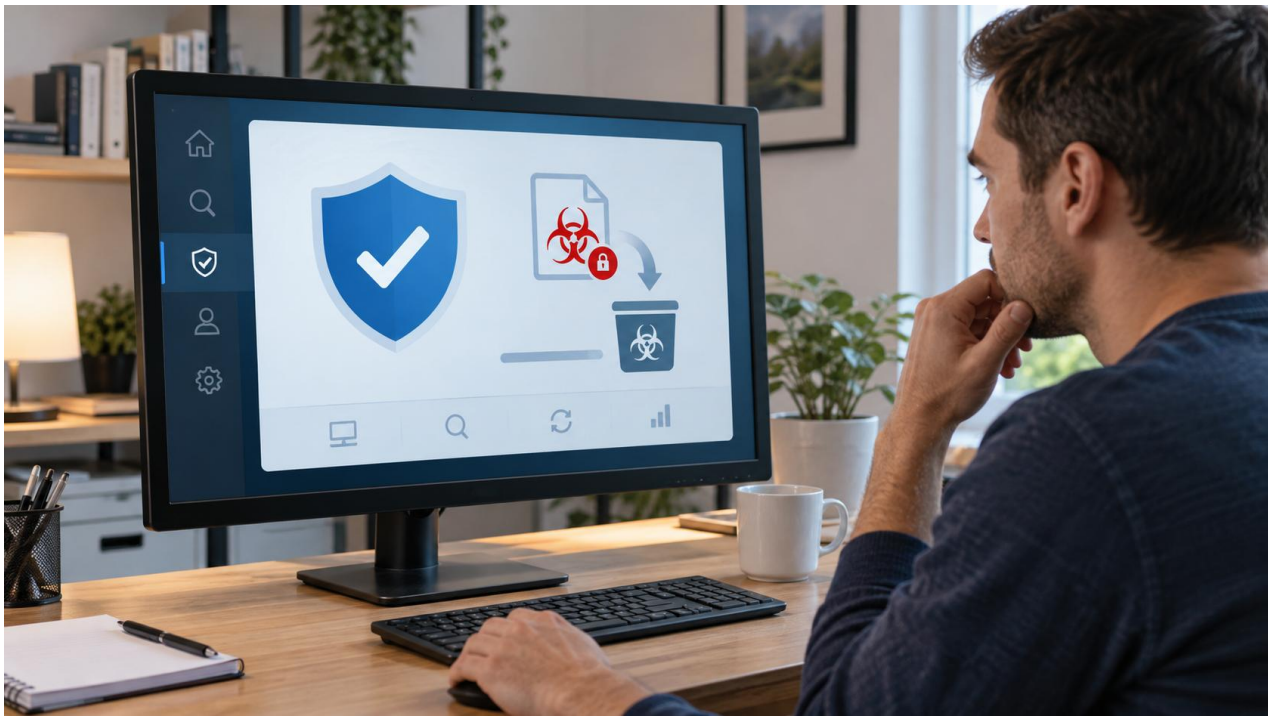
Une application demandant la localisation, le micro, les contacts et les fichiers sans nécessité doit être refusée ou supprimée.

INSTALLATION : Téléchargez depuis la boutique officielle et contrôlez l'éditeur, les avis et les autorisations.

Les signes d'une infection

SIGNE	INTERPRÉTATION POSSIBLE
Lenteur soudaine	Processus malveillant ou autre panne
Fenêtres inconnues	Publiciel ou faux support
Antivirus désactivé	Tentative de contournement
Fichiers modifiés	Virus ou rançongiciel
Comptes utilisés	Vol d'identifiants
Trafic réseau élevé	Bot, espion ou téléchargement caché

Une alerte antivirus



La quarantaine empêche le fichier détecté de s'exécuter pendant que l'utilisateur suit les consignes de sécurité.

Vrai virus ou fausse alerte

ALERTE LÉGITIME	FAUSSE ALERTE POSSIBLE
Provient de l'antivirus installé	Apparaît dans une page Web
Ouvre l'application de sécurité	Demande d'appeler un numéro
Propose analyse ou quarantaine	Exige un paiement immédiat
Donne un emplacement de fichier	Bloque la page avec un message anxiogène

RÉFLEXE : Fermez le navigateur sans appeler le numéro et contactez le support en cas de doute.

Les fichiers à risque

TYPE	VIGILANCE
Programmes exécutables	Peuvent lancer directement du code
Archives ZIP ou RAR	Peuvent masquer plusieurs fichiers
Documents à macros	Peuvent exécuter des instructions
Scripts	Automatisent des commandes
Fausses images ou factures	Extension réelle parfois masquée
Applications mobiles	Autorisations parfois excessives

Réduire le risque

☐ installer les mises à jour rapidement ;
☐ garder l'antivirus et le pare-feu actifs ;
☐ télécharger uniquement depuis une source officielle ;
☐ refuser les logiciels piratés ;
☐ désactiver les macros non nécessaires ;
☐ utiliser un compte sans droits administrateur ;
☐ sauvegarder régulièrement hors ligne ;
☐ former les utilisateurs.

Vérifier avant d'ouvrir

☐ attendiez-vous ce message ?
☐ connaissez-vous réellement l'expéditeur ?
☐ le nom du fichier correspond-il au contenu annoncé ?
☐ l'extension est-elle normale ?
☐ le message crée-t-il une urgence ?
☐ pouvez-vous confirmer par téléphone ou un autre canal ?

DOUTE : N'ouvrez pas, ne transférez pas et signalez le message.

Protéger son smartphone

☐ mettre à jour le système et les applications ;
☐ utiliser la boutique officielle ;
☐ contrôler les autorisations ;
☐ supprimer les applications inutilisées ;
☐ activer le verrouillage et la localisation ;
☐ éviter le débridage de l'appareil ;
☐ sauvegarder les données importantes.

Procédure pour un utilisateur

ORDRE	ACTION
1	Cesser d'utiliser l'appareil
2	Débrancher Ethernet et couper Wi-Fi ou données mobiles
3	Ne pas éteindre sauf consigne
4	Alerter le contact prévu depuis un autre appareil
5	Noter l'heure, les signes et les dernières actions
6	Ne pas reconnecter ni nettoyer seul

Mémo des douze réflexes

☐ Je mets mes appareils à jour.
☐ Je garde antivirus et pare-feu actifs.
☐ Je télécharge depuis les sources officielles.
☐ Je refuse les logiciels piratés.
☐ Je vérifie les pièces jointes.
☐ Je n'active pas une macro inconnue.
☐ Je contrôle les autorisations mobiles.
☐ Je sauvegarde hors ligne.
☐ Je reconnais une fausse alerte.
☐ J'isole un appareil suspect.
☐ J'alerte sans attendre.
☐ Je ne restaure pas seul un fichier en quarantaine.

Ressources officielles

cybermalveillance.gouv.fr • cyber.gouv.fr

Procédure pour un utilisateur

ORDRE	ACTION
1	Cesser d'utiliser l'appareil
2	Débrancher Ethernet et couper Wi-Fi ou données mobiles
3	Ne pas éteindre sauf consigne
4	Alerter le contact prévu depuis un autre appareil
5	Noter l'heure, les signes et les dernières actions
6	Ne pas reconnecter ni nettoyer seul

Mémo des douze réflexes

☐ Je mets mes appareils à jour.
☐ Je garde antivirus et pare-feu actifs.
☐ Je télécharge depuis les sources officielles.
☐ Je refuse les logiciels piratés.
☐ Je vérifie les pièces jointes.
☐ Je n'active pas une macro inconnue.
☐ Je contrôle les autorisations mobiles.
☐ Je sauvegarde hors ligne.
☐ Je reconnais une fausse alerte.
☐ J'isole un appareil suspect.
☐ J'alerte sans attendre.
☐ Je ne restaure pas seul un fichier en quarantaine.

Ressources officielles

cybermalveillance.gouv.fr • cyber.gouv.fr

Cybersécurité en entreprise

Rançongiciels, gestion des incidents, charte informatique, télétravail et plan de réaction

Une réponse efficace repose sur des rôles connus, des décisions tracées et une communication coordonnée.

La cybersécurité concerne toute l'entreprise

La sécurité ne dépend pas uniquement du service informatique. Une erreur de destinataire, un accès laissé ouvert ou un signal faible ignoré peut toucher les clients, les salariés et la continuité de l'activité.

ACTEUR	RESPONSABILITÉ
Direction	Fixer les priorités et les moyens
Responsable informatique ou prestataire	Protéger, surveiller et restaurer
Managers	Faire appliquer les règles et organiser la continuité
Salariés	Respecter les consignes et signaler rapidement
DPO ou référent données	Évaluer les conséquences sur les données personnelles

Ce que l'entreprise protège

ACTIF	EXEMPLES	CONSÉQUENCE
Données	Clients, paie, contrats	Fuite, altération ou indisponibilité
Comptes	Messagerie, cloud, administration	Usurpation et fraude
Équipements	Postes, serveurs, téléphones	Arrêt de travail
Services	Site, production, facturation	Interruption d'activité
Réputation	Confiance des partenaires	Perte de clients

RÉFLEXE : Protéger les données, mais aussi les accès, les outils et la capacité à travailler.

Les portes d'entrée fréquentes

- Pièce jointe ou lien d'hameçonnage ;
- Mot de passe volé ou réutilisé ;
- Accès à distance mal protégé ;
- Logiciel non mis à jour ;
- Clé usb ou matériel inconnu ;
- Faux support technique ;
- Prestataire ou compte partenaire compromis.

PRÉVENTION: Mises à jour, double authentification, sauvegardes hors ligne et sensibilisation réduisent fortement le risque.

Définir et qualifier un incident

Un incident de sécurité est un événement qui porte ou peut porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des systèmes et des données.

NIVEAU	EXEMPLE	RÉACTION
Faible	Message suspect non ouvert	Signaler et supprimer selon consigne
Modéré	Compte possiblement compromis	Bloquer l'accès et vérifier
Élevé	Poste infecté ou données exposées	Isoler et mobiliser l'équipe
Critique	Plusieurs services arrêtés	Activer la gestion de crise

Les étapes de gestion d’un incident

ÉTAPE	QUESTION
Détection	Que s’est-il passé et quand ?
Qualification	Quels systèmes, données et métiers sont touchés ?
Confinement	Comment empêcher l’extension ?
Investigation	Quelle origine et quelle portée ?
Remédiation	Comment retirer la cause et corriger ?
Reprise	Quels services redémarrer et dans quel ordre ?
Retour d’expérience	Quelles améliorations décider ?

Isoler immédiatement le poste

Débrancher le câble réseau ou désactiver les connexions limite la propagation vers les autres équipements.

ACTION : Suivez la procédure interne : isolez du réseau, laissez l’appareil disponible pour l’équipe technique et alertez.

Procédure en cinq gestes

ORDRE	GESTE	BUT
1	Arrêter l'action en cours	Éviter d'aggraver la situation
2	Débrancher Ethernet ou couper Wi-Fi et Bluetooth	Limiter la propagation
3	Ne pas éteindre sauf consigne interne	Préserver des éléments utiles
4	Alerter par un autre moyen fiable	Déclencher la réponse
5	Noter heure, écran et dernières actions	Aider au diagnostic

ATTENTION : Ne reconnectez jamais l'appareil de votre propre initiative.

Alerter le bon interlocuteur

L'alerte utile précise les faits observés, l'heure et les dernières actions sans interprétation hâtive.

CANAL : Utilisez le numéro, la messagerie ou la fiche d'urgence prévus par l'entreprise.

Donner une alerte utile

Informations à transmettre

☐ votre nom, service et moyen de rappel ;
☐ nom ou numéro du poste ;
☐ lieu et mode de connexion ;
☐ heure approximative du premier signe ;
☐ message observé ;
☐ dernière action effectuée ;
☐ présence éventuelle d'autres postes touchés.

EXEMPLE : « À 10 h 15, après ouverture d'une pièce jointe, mes fichiers ne s'ouvrent plus. J'ai débranché le câble réseau et appelé depuis un autre téléphone. »

Préserver les éléments utiles

- Photographier l'écran si cela est autorisé ;
- Conserver le courriel et sa pièce jointe sans les rouvrir ;
- Noter les url, numéros appelants et noms affichés ;
- Ne pas modifier les fichiers concernés ;
- Tenir une chronologie simple ;
- Remettre les éléments uniquement aux personnes habilitées.

CONFIDENTIALITÉ : Ne partagez pas les preuves dans une discussion collective ou sur un compte personnel.

Organiser la cellule de crise

La cellule de crise sépare les décisions, les actions techniques et la communication tout en partageant la même chronologie.

DISCIPLINE : Un responsable coordonne, chaque décision est datée et les informations sont vérifiées avant diffusion.

Répartir les rôles

RÔLE	MISSION
Pilote de crise	Arbitrer et fixer les priorités
Équipe technique	Contenir, analyser, corriger et restaurer
Métiers	Définir les activités prioritaires
Communication	Préparer des messages validés
Juridique et DPO	Évaluer obligations, contrats et données
Ressources humaines	Informer et accompagner les salariés

REMPLACEMENT : Chaque rôle critique doit avoir un suppléant joignable.

Communiquer pendant la crise

- Utiliser un canal de secours si la messagerie est compromise ;
- Communiquer uniquement des faits confirmés ;
- Indiquer ce que les salariés doivent faire ;
- Eviter de nommer une personne comme responsable ;
- Coordonner les messages aux clients et partenaires ;
- Conserver les versions et heures de diffusion.

MESSAGE COURT : Situation connue • action demandée • canal de contact • prochaine mise à jour

Données personnelles et notifications

L'organisation doit déterminer si l'incident constitue une violation de données personnelles. Elle documente les violations et évalue les risques pour les personnes. Une notification à la CNIL peut être nécessaire dans les 72 heures après en avoir pris connaissance lorsque la violation présente un risque.

SALARIÉ : Votre rôle est de signaler immédiatement. La qualification et les notifications relèvent des responsables désignés.

Le retour d'expérience

☐ reconstituer la chronologie ;

☐ identifier les causes techniques et organisationnelles ;

☐ mesurer ce qui a bien ou mal fonctionné ;

☐ corriger les failles et procédures ;

☐ mettre à jour les contacts et fiches réflexes ;

☐ former les équipes ;

☐ tester les actions décidées.

OBJECTIF : Apprendre sans rechercher un coupable : améliorer la capacité collective à réagir.

À quoi sert la charte informatique

La charte informatique fixe les règles d'utilisation des équipements, comptes, réseaux et données. Elle précise les droits, les devoirs, les contrôles possibles et les personnes à contacter.

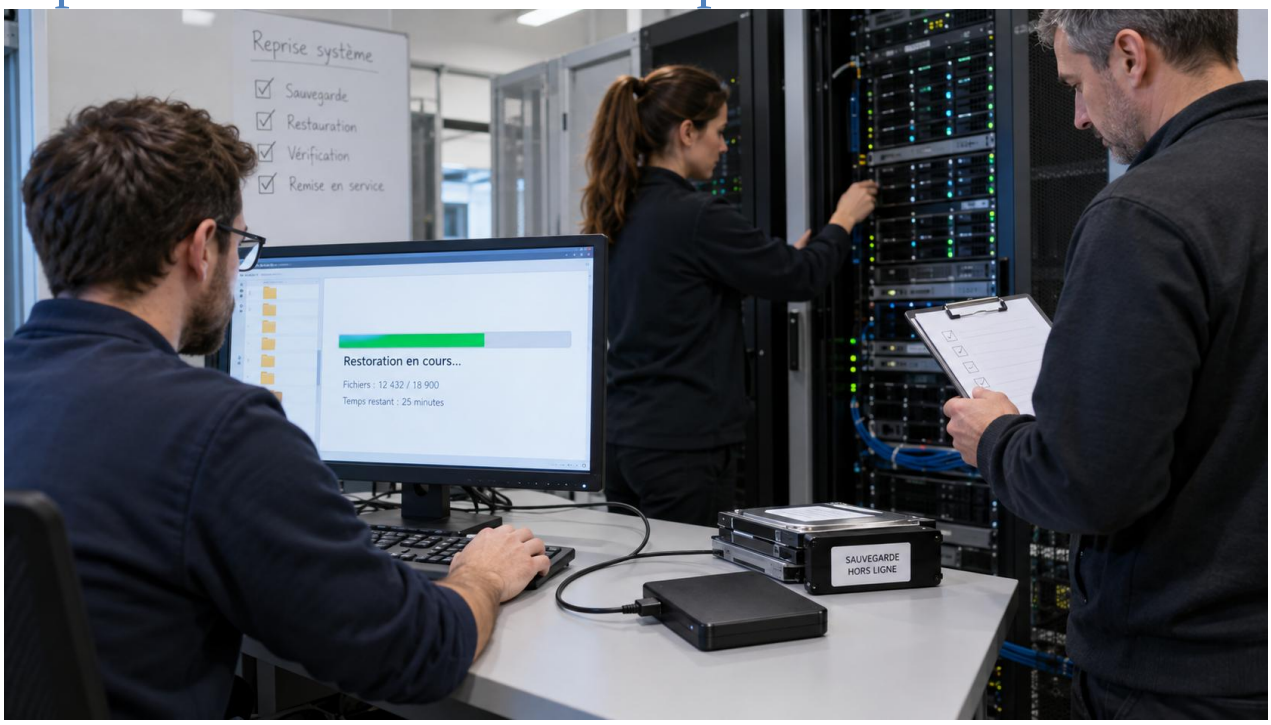
La charte est expliquée, comprise et accessible ; une signature seule ne remplace pas la sensibilisation.

BON RÉFLEXE : Demandez une explication lorsqu'une règle n'est pas claire.

Les règles essentielles de la charte

THÈME	RÈGLE SIMPLE
Comptes	Usage nominatif et secret
Matériel	Ne pas prêter ni modifier sans autorisation
Logiciels	Installer uniquement les applications approuvées
Données	Utiliser les espaces et canaux autorisés
Internet	Respecter l'usage professionnel défini
Incidents	Signaler immédiatement tout événement suspect

Préparer la continuité et la reprise



La restauration se fait depuis une sauvegarde vérifiée, dans un environnement maîtrisé et selon un ordre de priorité.

PRINCIPE : Restaurer trop vite sans éliminer la cause peut réintroduire l'attaque.

Construire le plan de réaction

QUESTION	À PRÉPARER
Qui décide ?	Titulaire et suppléant
Qui alerter ?	Liste hors ligne et numéros directs
Comment communiquer ?	Canal principal et canal de secours
Quoi isoler ?	Réseaux, postes et services prioritaires
Quoi restaurer ?	Ordre des activités essentielles
Où sont les preuves ?	Emplacement protégé et responsables

TEST : Le plan doit être exercé, corrigé et accessible même lorsque le système informatique est indisponible.

Courriel cloud et outils collaboratifs

☐ vérifier les destinataires et les pièces jointes ;

☐ ne pas transférer un message professionnel vers une adresse personnelle ;

☐ utiliser le cloud approuvé par l'entreprise ;

☐ limiter les droits de partage ;

☐ retirer les personnes qui n'ont plus besoin d'accès ;

☐ ne jamais transmettre un secret dans une discussion non autorisée.

RÉFLEXE : Le canal pratique n'est pas toujours le canal autorisé.

Poste de travail et départ du bureau

☐ verrouiller la session à chaque absence ;

☐ ranger les documents sensibles ;

☐ récupérer les impressions ;

☐ ne pas laisser de badge ou support amovible ;

☐ fermer les applications métier ;

☐ signaler immédiatement la perte d'un appareil ;

☐ respecter la procédure de fin de contrat ou de mission.

RACCOURCI WINDOWS : Windows plus L verrouille immédiatement la session.

Les risques du télétravail

RISQUE	EXEMPLE	MESURE
Réseau non maîtrisé	Wi-Fi public	Connexion approuvée et VPN
Regards indiscrets	Écran visible	Orientation et filtre
Mélange des usages	Ordinateur familial	Matériel professionnel dédié
Fuite de documents	Impression à domicile	Éviter ou détruire sûrement
Faux support	Appel urgent	Rappeler par le canal officiel

Installer un poste de télétravail sûr

Un appareil professionnel, une connexion protégée et une double authentification réduisent les risques à domicile.

AVANT DE COMMENCER : Mettez à jour l'appareil, vérifiez le **VPN** et gardez le téléphone de validation sous votre contrôle.

Télétravail pas à pas

Connexion

- Utilisez l'équipement fourni ;
- Connectez-vous au réseau prévu ;
- Activez le **VPN** si la procédure l'exige ;
- Validez uniquement une demande **MFA** initiée par vous.

Pendant et après

☐ protégez l'écran et les conversations ;
☐ enregistrez dans l'espace professionnel ;
☐ verrouillez à chaque pause ;
☐ déconnectez les accès en fin de journée.

Déplacements et lieux publics

- Évitez les Wi-Fi ouverts ;
- Ne discutez pas d'informations sensibles ;
- Gardez l'appareil avec vous ;
- Désactivez Bluetooth et partage inutiles ;
- Utilisez un filtre de confidentialité si nécessaire ;
- Ne branchez pas de chargeur ou de clé inconnue ;
- Signalez immédiatement perte ou vol.

HÔTEL ET TRAIN : Un écran visible et une conversation entendue peuvent suffire à créer une fuite.

Mes 10 réflexes de cybersécurité

Une fiche à conserver près de son ordinateur ou à partager avec ses proches.

1. **Je mets à jour mes appareils et mes applications.** Les mises à jour corrigent des failles de sécurité.
2. **Je verrouille mon écran dès que je m'éloigne.** Même pour une courte absence.
3. **J'utilise un mot de passe long et différent pour chaque compte.** Un gestionnaire de mots de passe peut m'aider à les conserver.
4. **J'active la double authentification.** Je commence par ma messagerie et mes comptes importants.
5. **Je ne communique jamais un code de connexion.** Ni par téléphone, ni par courriel, ni par message.
6. **Je vérifie avant de cliquer.** Un message urgent, une adresse inhabituelle ou une pièce jointe inattendue doivent m'alerter.
7. **Je télécharge depuis les sources officielles.** Je me méfie des fausses alertes qui proposent d'installer un logiciel.
8. **Je sauvegarde régulièrement mes fichiers importants.** Je vérifie que je peux les récupérer si mon appareil tombe en panne ou est attaqué.
9. **Je protège mes connexions et mes données.** Sur un réseau public ou en déplacement, je suis les consignes de sécurité de mon organisation.
10. **Je signale rapidement tout incident ou doute.** Un message suspect, un appareil perdu ou une connexion inconnue doivent être pris en charge sans attendre.

Le réflexe essentiel : en cas de doute, je m'arrête, je vérifie par un autre moyen et je demande conseil.