GUIDE : SÉCURISER SON SMARTPHONE

15 mesures essentielles — Applicable à Android et iOS — Toutes générations

GUIDE PRATIQUE
2 PAGES

Votre smartphone = votre vie numérique. Photos, contacts, emails, paiements, réseaux sociaux, messageries chiffrées... Sa perte ou son piratage peut avoir des conséquences graves. Ces 15 mesures couvrent les risques essentiels.

Source : cybermalveillance.gouv.fr — Licence Etalab 2.0 | Adaptation : Ayi NEDJIMI Consultants — ayinedjimi-consultants.fr | Recommandations valables pour Android 13+ et iOS 16+

MESURES FONDAMENTALES

1 Code PIN 6 chiffres minimum — ESSENTIEL

Activez un code PIN de 6 chiffres au minimum. Évitez les combinaisons évidentes (000000, 123456, date de naissance). Préférez 8 chiffres pour une meilleure sécurité.

Astuce : Utilisez un code aléatoire mémorisé sous forme de motif sur le clavier

2 Biométrie (en complément) — ESSENTIEL

Activez la reconnaissance d'empreinte digitale ou faciale pour le confort au quotidien. La biométrie reste un facteur de commodité, le PIN demeure la protection principale.

La biométrie ne remplace pas le PIN — configurez toujours les deux

3 Mises à jour automatiques — ESSENTIEL

Activez les mises à jour automatiques du système et des applications. Les correctifs de sécurité colmatent les failles exploitées par les attaquants. Un téléphone non mis à jour est une cible facile.

Paramètres → Mise à jour → Activer les mises à jour automatiques

4 Applications : stores officiels uniquement — ESSENTIEL

Installez uniquement depuis Google Play Store (Android) ou l'App Store (iOS). Les fichiers APK/IPA de sources tierces sont le principal vecteur de malware sur smartphone.

Android : désactivez "Sources inconnues" dans les paramètres de sécurité

5 Révision des permissions d'applications — ESSENTIEL

Vérifiez régulièrement les accès accordés à chaque application : caméra, micro, localisation, contacts. Une application de lampe de poche n'a pas besoin d'accéder à vos contacts.

Paramètres → Confidentialité → Gestionnaire des permissions

6 Verrouillage automatique — IMPORTANT

Configurez le verrouillage automatique après 30 secondes à 1 minute d'inactivité. Ce délai réduit drastiquement les risques en cas de perte ou de vol.

Affichage → Mise en veille → 30 secondes

7 Chiffrement de l'appareil — IMPORTANT

Vérifiez que le chiffrement complet de l'appareil est activé. Tous les iPhones sont chiffrés par défaut. Sur Android, vérifiez dans Sécurité → Chiffrement.

Rend les données illisibles sans le code PIN, même en cas de vol du stockage

8 Localisation et effacement à distance — IMPORTANT

Activez "Localiser mon appareil" (iOS : Localiser / Android : Localiser mon appareil). En cas de vol, vous pouvez localiser, verrouiller ou effacer le téléphone à distance.

iOS : icloud.com/find — Android : android.com/find

MESURES AVANCÉES ET RÉSEAUX

9 VPN sur Wi-Fi public — ESSENTIEL

N'utilisez jamais un réseau Wi-Fi public (hôtel, café, gare) sans VPN. Ces réseaux permettent l'interception de vos données. Préférez votre forfait 4G/5G ou un VPN de confiance.

VPN recommandés : ProtonVPN, Mullvad. Évitez les VPN "gratuits" suspects

10 Sauvegarde automatique — IMPORTANT

Activez la sauvegarde automatique dans le cloud (iCloud, Google One) ou en local via câble. En cas de perte, de vol ou de panne, récupérez toutes vos données.

Vérifiez que la sauvegarde s'effectue bien régulièrement : Paramètres → Sauvegarde

11 Gestionnaire de mots de passe — IMPORTANT

Installez un gestionnaire de mots de passe (Bitwarden, 1Password) sur votre smartphone. Il génère et stocke des mots de passe forts pour chaque application et site web.

Activez le remplissage automatique dans les paramètres du gestionnaire

12 MFA sur tous les comptes importants — ESSENTIEL

Activez l'authentification à deux facteurs (2FA/MFA) sur tous vos comptes : email, réseaux sociaux, banque, services cloud. Utilisez une application TOTP (Aegis, Google Authenticator).

Sauvegardez vos codes de récupération dans votre gestionnaire de mots de passe

13 Désactivation du Bluetooth et NFC inutilisés — RECOMMANDÉ

Désactivez le Bluetooth et le NFC lorsqu'ils ne sont pas utilisés. Ces protocoles peuvent être exploités pour des attaques de proximité (BlueSnarfing, eavesdropping).

Raccourci : Centre de contrôle → désactiver Bluetooth et NFC

14 Méfiance des SMS / liens reçus — ESSENTIEL

Ne cliquez jamais sur un lien reçu par SMS, même si l'expéditeur semble connu (smishing). Les banques et administrations n'envoient jamais de lien demandant vos identifiants.

En cas de doute, tapez l'URL directement dans votre navigateur

15 Navigateur et DNS sécurisés — RECOMMANDÉ

Utilisez un navigateur avec protection de la vie privée (Firefox avec uBlock Origin, Brave). Activez le DNS chiffré (DNS-over-HTTPS) dans les paramètres réseau de votre téléphone.

Android : Paramètres → Réseau → DNS privé → dns.quad9.net

Source : cybermalveillance.gouv.fr — Licence Etalab 2.0 | Adaptation : Ayi NEDJIMI Consultants — ayinedjimi-consultants.fr | Recommandations valables pour Android 13+ et iOS 16+

GUIDE SMARTPHONE — CONSEILS SPÉCIFIQUES

Encadrés adolescents et seniors + tableau de vérification

CONSEILS POUR LES ADOLESCENTS (12–18 ANS)

- **Code PIN unique** : ne le partagez jamais avec vos amis, même proches. Votre téléphone vous appartient.
- **Réseaux sociaux** : mettez vos profils en "privé" sur Instagram, TikTok et Snapchat. Refusez les demandes d'inconnus.
- **Applications de rencontre** : interdites avant 18 ans légalement. Méfiez-vous des profils qui demandent des informations personnelles ou des photos.
- **Phishing "cadeaux"** : les messages "Tu as gagné un iPhone ! Clique ici" sont toujours des arnaques. Signalez-les.
- **Localisation** : ne partagez pas votre position en temps réel avec des personnes que vous ne connaissez pas en dehors du numérique.
- **Cyberharcèlement** : si vous en êtes victime ou témoin, capturez des preuves (screenshots), bloquez l'auteur et signalez à un adulte de confiance ou sur cybermalveillance.gouv.fr
- **Applications gratuites** : "gratuit" signifie souvent que vous êtes le produit (vos données sont vendues). Vérifiez les permissions demandées.
- **Wi-Fi scolaire** : n'utilisez pas de VPN ou proxy pour contourner les filtres de votre établissement — c'est interdit et souvent détecté.
- **Mots de passe** : utilisez un gestionnaire (Bitwarden est gratuit) — n'utilisez pas votre prénom ou "azerty123".
- **Numéro utile** : 3018 — numéro national contre le cyberharcèlement (gratuit, 7j/7, 9h-23h)

CONSEILS POUR LES SENIORS (65 ANS ET PLUS)

- **Arnaques au faux support technique** : personne ne vous appellera jamais pour vous dire que votre téléphone est "infecté" et demander d'installer une application. Raccrochez.
- **Arnaques bancaires** : votre banque ne vous demandera JAMAIS vos codes par SMS, email ou téléphone. En cas de doute, appelez votre agence avec le numéro figurant sur votre carte.
- **SMS d'alerte** : méfiez-vous des SMS prétendant être La Poste, Chronopost ou les impôts demandant un paiement. Allez sur le site officiel directement.
- **Mise à jour** : acceptez toujours les mises à jour proposées par votre téléphone ou vos applications. Elles corrigent des problèmes de sécurité importants.
- **Wi-Fi en déplacement** : évitez de consulter votre banque ou vos emails sur un réseau Wi-Fi public dans un café ou un hôtel.
- **Photos personnelles** : activez la sauvegarde automatique (iCloud ou Google Photos) pour ne jamais perdre vos souvenirs si votre téléphone est perdu ou cassé.
- **Demande d'aide** : si quelqu'un vous dit pouvoir "prendre la main" sur votre téléphone à distance pour vous aider et vous demande un paiement, c'est une arnaque.
- **Mots de passe** : n'inscrivez jamais vos mots de passe sur un papier accessible. Demandez à un proche de confiance de vous aider à configurer un gestionnaire sécurisé.
- **Assistance** : consultez votre mairie, un espace France Services, ou le site aidantsconnect.beta.gouv.fr pour une aide en personne.
- **Numéro utile** : 0 805 805 817 — numéro national de signalement (gratuit, accessible aux seniors)

TABLEAU DE VÉRIFICATION — AUDIT DE SÉCURITÉ DE VOTRE SMARTPHONE

MESURE DE SÉCURITÉ	ANDROID	IOS (IPHONE)	PRIORITÉ	FAIT ✓
Code PIN 6+ chiffres activé	Paramètres → Sécurité → Verrouillage	Paramètres → Face ID → Code	Essentiel	
Biométrie configurée	Paramètres → Sécurité → Empreinte	Paramètres → Face ID / Touch ID	Essentiel	
Mises à jour automatiques activées	Paramètres → MAJ logicielle → Auto	Paramètres → Général → MAJ auto	Essentiel	
Localisation et effacement distant	android.com/find activé	iCloud → Localiser → Mon iPhone	Essentiel	
Sauvegarde automatique	Google One / paramètres	iCloud → Sauvegarde iCloud	Important	
MFA activé sur les comptes email et réseaux sociaux	Paramètres de chaque application	Paramètres de chaque application	Essentiel	
Permissions d'applications vérifiées	Paramètres → Confidentialité	Paramètres → Confidentialité	Essentiel	
Gestionnaire de mots de passe installé	Play Store → Bitwarden	App Store → Bitwarden	Important	

Chiffrement de l'appareil vérifié	Paramètres → Sécurité → Chiffrement	Activé par défaut sur iPhone	**Important**	
Sources inconnues désactivées	Paramètres → Applications → Sources	Désactivé par défaut sur iOS	**Essentiel**	
VPN installé pour Wi-Fi public	Play Store → ProtonVPN / Mullvad	App Store → ProtonVPN / Mullvad	**Recommandé**	
DNS privé configuré (DNS-over-HTTPS)	Paramètres → Réseau → DNS privé	Via profil ou VPN	**Recommandé**	

Ressources utiles : cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-smartphone | ssi.gouv.fr (guides ANSSI) | Signal (messagerie chiffrée recommandée)

Besoin d'une sensibilisation à la sécurité numérique pour vos équipes, parents ou enfants ?
ayinedjimi-consultants.fr/contact