



Votre mobile est-il bien protégé ?

Jean Marie Herbaux

Table des matières

I.	BÂTISSEZ UNE PREMIÈRE LIGNE DE DÉFENSE.....	2
II.	PASSEZ AU VERROUILLAGE BIOMÉTRIQUE.....	2
III.	PASSEZ À SMARTLOCK.....	2
IV.	ACTIVEZ LE CHIFFREMENT DU TÉLÉPHONE.....	2
V.	PROFITEZ DU BOUCLIER INTÉGRÉ.....	2
VI.	FAITES APPEL À UN VPN.....	2

Assurer la sécurité d'un smartphone consiste à préserver l'intégrité des contenus et des données personnelles qu'il abrite. Voici comment transformer un mobile Android en une citadelle imprenable!

I. BÂTISSEZ UNE PREMIÈRE LIGNE DE DÉFENSE

Un *code PIN* ou un *schéma* de verrouillage constitue une barrière efficace contre les accès non autorisés. Évitez évidemment les combinaisons évidentes pour privilégier les mots de passe combinant minuscules, majuscules, chiffres et symboles.

Allez dans les paramètres du téléphone, recherchez la section *Sécurité* ou *Verrouillage de l'écran*, choisissez *Type de verrouillage de l'écran* et *Code PIN ou Schéma*. Suivez les instructions pour créer le code et confirmez-le.

II. PASSEZ AU VERROUILLAGE BIOMÉTRIQUE

La reconnaissance du *visage* ou des *empreintes digitales* procure une meilleure sécurité tout en facilitant le déverrouillage.

Pour activer ces dispositifs, rendez-vous dans les *paramètres* d'Android et sélectionnez le mode souhaité.

Dans le cas d'un capteur d'empreintes, touchez *Ajouter un doigt* et procédez à l'enregistrement en posant et soulevant le doigt sur la zone d'identification jusqu'à validation.

Pour la *reconnaissance faciale*, cadrez votre visage et tournez la tête comme vous le demande l'assistant.

III. PASSEZ À SMARTLOCK

Smart Lock propose de lier le verrouillage à la proximité d'un appareil de référence ou à des lieux que vous avez définis. Il est possible, par exemple, de demander à ne pas verrouiller votre téléphone lorsque vous vous trouvez chez vous ou près d'un périphérique Bluetooth comme une montre ou une voiture.

Pour activer et configurer Smart Lock, rendez-vous dans la section *Sécurité* ou *Écran de verrouillage* des paramètres d'Android. Touchez Smart Lock et sélectionnez l'une des situations disponibles.

IV. ACTIVEZ LE CHIFFREMENT DU TÉLÉPHONE

Assurez-vous que vos données demeurent inviolables en activant le chiffrement du contenu du téléphone. Cela rend les fichiers illisibles tant que vous ne vous êtes pas identifié.

Selon la marque et la version de votre mobile, vous trouverez cette option dans la section *Sécurité* ou *Confidentialité*, voire parmi les options liées à la *localisation*. Choisissez *Chiffrement* ou *Chiffrer le téléphone* et suivez les instructions pour appliquer les algorithmes de cryptage.

V. PROFITEZ DU BOUCLIER INTÉGRÉ

Google *Play Protect* est un outil de sécurité présent par défaut sur les mobiles Android. Il analyse les applications installées afin de détecter et supprimer les éventuels éléments malveillants. *Play Protect* vérifie également les nouvelles applications avant leur installation pour s'assurer qu'elles ne présentent pas de danger.

Vérifiez que dispositif est bien en place en ouvrant les *paramètres* du téléphone et en pointant sur *Google*, *Sécurité* et *Google Play Protect*. Touchez option *Analyser les applications avec Play Protect*

VI. FAITES APPEL À UN VPN

Quand vous utilisez un réseau Wifi public, soyez vigilant et portez une attention accrue à la protection de vos données. Dans la mesure du possible, installez et utilisez un réseau privé virtuel (VPN) pour chiffrer le trafic internet entrant et sortant et masquer votre adresse IP. Orientez-vous par exemple vers *Atlas VPN*, facile à utiliser et offrant un bon niveau de sécurité. Ce tunnel sécurisé traite aussi bien les échanges réalisés depuis le navigateur web et que les flux de données des applications.