# Sécurisez votre **SMARTPHONE**

# Table des matières

# MASQUER VOS DONNÉES PERSONNELLES

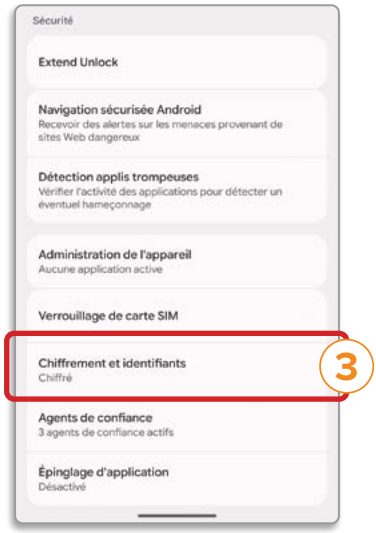
Notre smartphone contient une grande partie de notre vie. Sécuriser nos données n'est donc plus une option, mais une nécessité. Vous avez appris à sécuriser votre appareil, ici vous verrez comment protéger vos données.

## Chiffrer les données

Lorsque toutes les données à caractère personnel sont chiffrées sur un appareil, il y a peu de chances qu'un criminel parvienne à les subtiliser. Sur tous les appareils actuels, le contenu est chiffré d'office. Vérifiez que c'est bien le cas et, au besoin, activez cette option.

### Sur Android

Sur Android, un code d'accès est nécessaire pour chiffrer les données sur l'appareil. Lorsque ce code est paramétré, les données sont chiffrées automatiquement. Attention, tous les Android n'affichent pas les mêmes informations. Voici les données pour un Google Pixel sous Android 16.



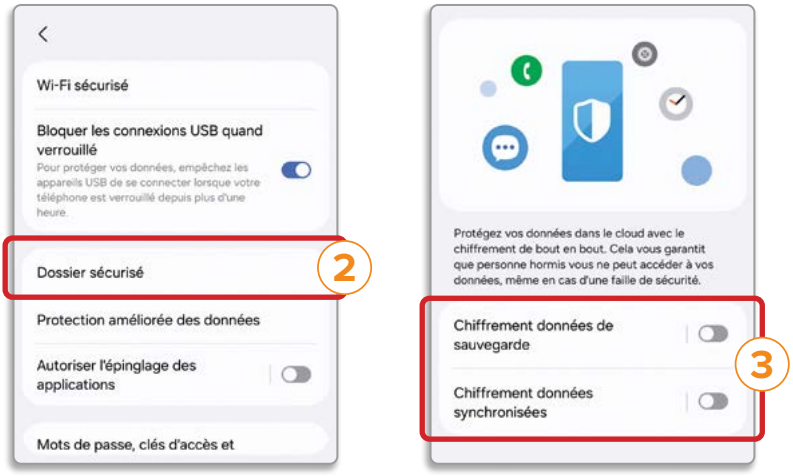

1. Allez dans **Paramètres**, puis **Sécurité et confidentialité**.
2. Tout en bas, cliquez sur **Sécurité et confidentialité renforcée**.
3. Une page s'affiche où vous pouvez constater si le contenu est chiffré.

### La protection de données sur Samsung

En plus du chiffrement d'Android, les appareils Samsung Galaxy ajoutent une couche de sécurité supplémentaire avec l'architecture Knox, préinstallée et activée par défaut. Samsung Knox s'appuie sur une sécurité renforcée liée au matériel et peut également servir pour l'administration de smartphones d'entreprise. Si le niveau de sécurité par défaut n'est pas suffisant, vous pouvez protéger encore davantage les fichiers ou applications sensibles sur

le téléphone, mais aussi dans le cloud Samsung. Vous pouvez ainsi créer un dossier sécurisé qui sera accessible uniquement via code d'accès ou donnée biométrique.

1. La protection normale est activée par défaut. Si vous voulez augmenter le niveau de sécurité en créant un dossier sécurisé, allez dans **Paramètres**, puis **Sécurité et confidentialité**.
2. Sélectionnez **Autres paramètres de sécurité** et choisissez **Dossier sécurisé**.
3. Si vous souhaitez également chiffrer la sauvegarde de données sur le cloud Google, cliquez sur **Protection améliorée des données,** et activez le **chiffrement des données**.




## Sur iOS

Si l'iPhone est protégé par un code PIN ou un mot de passe, son contenu est chiffré. Vous pouvez le vérifier dans **Réglages**. Le code d'accès est utilisé pour chiffrer les données sur l'appareil. Plus il est complexe, meilleure est la protection des données sur le téléphone.


1. Allez dans **Réglages** et choisissez **Face ID et code**.
2. Introduisez le code d'accès.
3. Vérifiez que la mention "La protection des données est activée" apparaît en dessous.

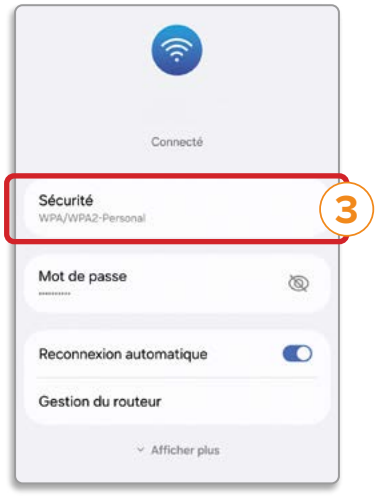
## Sécuriser votre connexion wifi

Pour éviter les regards indiscrets lorsque vous êtes connecté à internet en wifi, il importe de chiffrer la connexion. La plupart des connexions sécurisées ont recours au protocole Wi-Fi Protected Access 2 (WPA2) qui a succédé en 2006 au WPA et au WEP, devenus obsolètes. Depuis fin 2019, certains produits sur le marché utilisent le WPA3, plus sûr que le WPA2.

### Vérifier la sécurisation

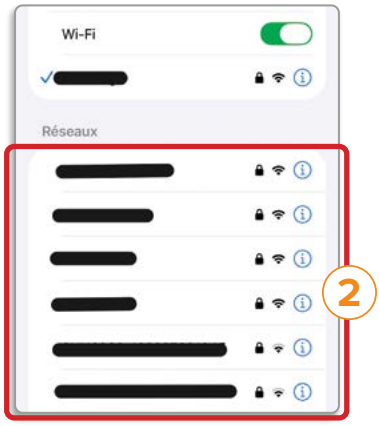
Vous pouvez vérifier, via les paramètres du wifi, que la connexion est sécurisée. Il n'y a pas toujours d'informations sur le type de sécurisation disponible.

#### Sur Android




1. Allez dans **Paramètres** et appuyez sur **Connexions**.
2. Sélectionnez **Wi-Fi**. La liste de réseaux sans fil apparaît alors.
3. Appuyez sur la roue dentée à côté du réseau auquel vous êtes connecté. Sous **Sécurité** figurent des informations sur le type de sécurisation.

#### Sur iOS




1. Allez dans **Réglages** et appuyez sur **Wi-Fi**.
2. Vous obtenez une liste des sites sur lesquels vous naviguez. Si un petit cadenas s'affiche à côté du réseau wifi auquel vous êtes connecté, cela signifie que la connexion est sécurisée.

### Faire attention aux bornes wifi

Le wifi est offert gratuitement en de nombreux endroits : gares, aéroports, hôtels et restaurants. Bien pratique, mais dangereux si vous envisagez d'effectuer des opérations sensibles à partir d'une borne wifi : vous connecter à votre compte bancaire, consulter vos e-mails… Il est assez facile pour un pirate de monter une fausse borne et c'est ensuite un jeu d'enfant pour lui de subtiliser des informations personnelles à ceux qui s'y connectent. En vous orientant vers une copie de site bancaire, il peut vous dépouiller de votre argent. Pour vous mettre en confiance, un pirate peut donner à sa borne wifi un nom d'apparence authentique, comme "WiFi Brussels Airport".
Et le danger ne vient pas seulement des fausses bornes wifi. Un pirate peut facilement épier le trafic non chiffré des autres utilisateurs sur une borne publique. Suivez ces conseils lorsque vous vous y connectez.

1. **Utilisez le protocole HTTPS.** Si un site utilise le HTTPS, toutes les données sont envoyées sous forme chiffrée et personne ne peut les intercepter. Assurez-vous que l'URL débute bien par "https". Vérifiez aussi la présence d'un petit cadenas dans la barre de navigation.

2. **Tenez compte des avertissements.** Le navigateur vous avertit qu'un certificat de sécurité n'est pas conforme ou que le site web n'est pas sûr ? Évitez de le consulter : il s'agit peut-être d'un site de phishing.

3. **Déconnectez-vous.** Faites-le immédiatement après avoir consulté un site ou une appli protégés par un mot de passe. Si quelqu'un s'immisce dans la connexion, il n'aura plus accès au site web sans s'y connecter.

4. **Désactivez la connexion automatique.** Réglez votre smartphone de manière à ce qu'il ne se connecte pas automatiquement à un réseau connu (voir p. 40). Si un pirate se fait passer pour ce réseau ultérieurement, votre smartphone ne s'y connectera pas de lui-même.

5. **Utilisez un VPN.** Si vous vous connectez via un réseau privé virtuel (VPN), la connexion ne pourra pas être interceptée (voir p. 41).

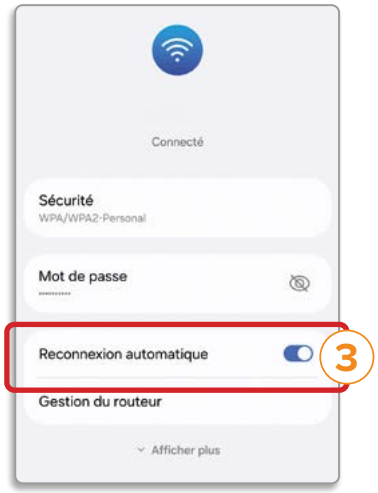

#### Préférez la 4G ou la 5G au wifi

Pour les opérations sensibles telles que la banque mobile ou la messagerie électronique, une connexion mobile (par, 4G ou 5G) est plus sûre que le wifi extérieur. Le réseau mobile étant bien sécurisé, les indiscrets seront incapables de nuire.

## Désactiver la connexion automatique

Les appareils tournant sur iOS et sur Android se connectent automatiquement aux réseaux auxquels ils se sont déjà connectés. Il existe malheureusement des failles. Si un autre réseau wifi porte le même nom, l'appareil tentera quand même de s'y connecter. Aussi est-il préférable de désactiver la connexion automatique.

### Sur Android




1. Allez dans **Paramètres** et appuyez sur **Connexions** puis sur **Wi-Fi**.
2. Appuyez sur la roue dentée à côté du réseau wifi.
3. Désactivez le curseur sur **Reconnexion automatique**.

### Sur iOS


1. Allez dans **Réglages** et appuyez sur **Wifi**.
2. Sélectionnez le réseau de wifi.
3. Désactivez le curseur sur **Connexion automatique**.

## Utiliser un VPN

L'utilisation d'un réseau privé virtuel (VPN) permet de surfer de manière plus sûre et presque anonyme. Tout le trafic internet passe par l'ordinateur du fournisseur du VPN, qui se charge du chiffrement et met à disposition une autre adresse IP. Vos activités sur internet ne permettent plus de remonter jusqu'à vous. Un criminel ne peut donc plus intercepter de données sur un réseau wifi public, par exemple lorsque vous utilisez une messagerie non chiffrée.

En outre, avec un VPN, votre vie privée est mieux protégée contre la censure des autorités publiques et les entreprises qui vous épient. Les annonceurs ne peuvent plus vous suivre aussi bien pour établir leur profil. Quant aux fournisseurs d'accès, ils ne peuvent plus enregistrer les données liées aux activités sur internet.

Il existe plusieurs applis VPN pour smartphone. À chaque utilisation, vous choisissez un pays à partir duquel vous surfez fictivement. L'inconvénient : le VPN vous oblige à faire un détour, ce qui ralentit le téléchargement des sites, musiques et vidéos. De nombreux services VPN sont disponibles, la plupart sont payants.

### Contourner les restrictions géographiques

Les chaînes de télévision interdisent parfois l'accès de leurs émissions en ligne aux internautes disposant d'une adresse IP étrangère. Avec un VPN, ceux-ci peuvent choisir un autre pays et faire croire au site web qu'ils surfent, par exemple, depuis la Belgique alors que ce n'est pas le cas. Le VPN permet aussi de se jouer des mesures de censure, comme en Chine ou en Russie, et de consulter des sites web bloqués. Mais vérifiez dans ce cas que l'utilisation d'un VPN n'est pas punissable.

### Pour choisir un fournisseur de VPN

Faites attention aux points suivants.

– **Choisissez un service compatible avec OpenVPN ou WireGuard.**

– **Cherchez à savoir s'il existe une appli mobile.** Sans appli, vous devez régler vous–même la connexion et cela peut être fastidieux.

– **Optez pour un serveur belge.** Combien de serveurs existe-t-il ? Dans quels pays sont–ils établis ? La vitesse de téléchargement dépend

de la distance qui les sépare de la Belgique. Si vous habitez dans un pays voisin, mieux vaut opter pour un serveur belge.

– **Évitez les services peu respectueux de votre vie privée, qui suivent vos activités, comme Onavo de Facebook auparavant.** Si un service vous promet "no logging", cela ne veut pas dire qu'il n'enregistre rien. Idéalement, utilisez un service VPN qui traite les données en mémoire RAM plutôt que sur un espace de stockage. Aussi, moins un service VPN vous demandera de données personnelles (adresse email, nom, adresse, numéro de téléphone) moins il sera a fortiori intrusif.

– **Payez anonymement.** Pour le paiement, Monero (bitcoin) offre le plus d'anonymat. Si vous n'avez pas de bitcoins ou de carte de crédit, choisissez un service qui utilise PayPal ou en cash via Mullvad VPN.

Les fournisseurs de VPN gratuits ont leurs limites. Comme ils disposent de peu de serveurs, la connexion est souvent lente et les données rationnées. Faites bien attention aux conditions relatives à la vie privée. Si vous regardez peu de vidéos et si vos téléchargements sont modérés, un service gratuit vous suffira.

Pour trouver le meilleur service VPN, allez sur **testachats.be/comparervpn** ou scannez ce code QR

## Effectuer les mises à jour

Pour protéger votre équipement informatique, une règle fondamentale est de mettre à jour les logiciels, et les smartphones n'y échappent pas. Les mises à jour sont là pour remédier aux erreurs qui sont régulièrement découvertes dans les logiciels. Ne reportez donc pas à plus tard leur installation.

### Quelle version est encore bonne ?

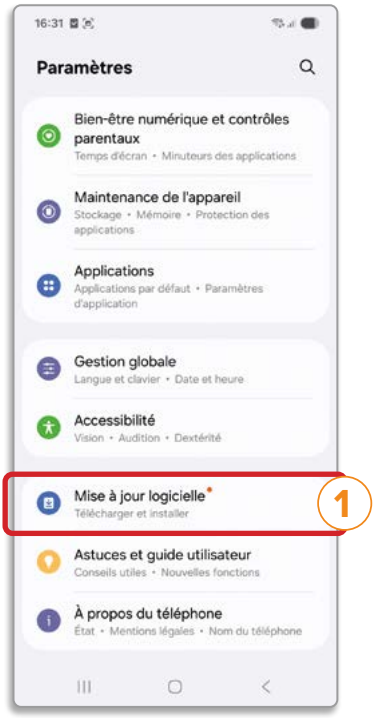
Si vous achetez un nouvel Android, veillez à ce qu'il dispose au moins de la version 15. Android 16 est sorti en juin 2025. Apple a sorti la version 26 d'iOS en septembre 2025. Il s'agit en réalité de la 19e génération de l'OS d'Apple. Le chiffre fait désormais référence à l'année pendant laquelle l'OS vivra principalement.

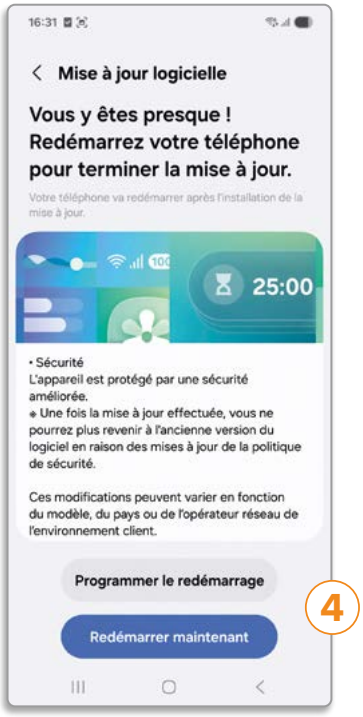
## Les mises à jour du système

Lorsqu'une mise à jour est disponible, une notification s'affiche généralement sur votre téléphone. Si vous craignez d'en avoir manqué une, vous pouvez toujours vérifier la version de votre appareil et l'existence éventuelle de mises à jour.

### Sur Android

1. Allez dans **Paramètres** et choisissez **Mise à jour logicielle**.
2. Appuyez sur **Téléchargement et installation**
3. La version actuelle et les correctifs de sécurité déjà installés vont s'afficher.
4. Si une mise à jour est disponible, appuyez sur **Télécharger et installer**. Android recherche alors les mises à jour. Appuyez sur **Installer maintenant** pour effectuer la mise à jour. Vous devrez ensuite redémarrer votre smartphone.



## Sur iOS

1. Allez dans **Réglages** et appuyez sur **Général**.
2. Sélectionnez **Mise à jour logicielle**.
3. iOS recherche alors les mises à jour. S'il y en a une, appuyez sur **Mettre à jour**.



### Mettez vos applis à jour

Les applis peuvent aussi contenir des erreurs. Vérifiez régulièrement que toutes les applis installées sont à jour (voir p. 72). Si vous négligez de le faire, votre appareil sera vulnérable aux attaques de pirates.