***Avertissements de sécurité***

1. Mettez un code d'accès sur votre téléphone

La chose la plus simple à faire est de mettre un code d'accès sur votre téléphone. Avoir un code d'accès rendra plus difficile pour quelqu'un de prendre votre téléphone et de faire défiler, d'accéder à vos comptes ou d'installer quelque chose de malveillant. Dans le cas où votre téléphone est volé ou que vous le perdez, il sera un peu plus difficile pour d'autres d'accéder à votre téléphone. La plupart des téléphones demandent simplement un code d'accès à 4 chiffres, mais certains téléphones vous permettront d'utiliser un code d'accès plus complexe ou même une empreinte digitale.

2. Désactiver le partage de localisation

La plupart des téléphones ont un GPS et d'autres indicateurs de localisation qui peuvent déterminer votre position générale ou exacte. Grâce à cette capacité, de nombreuses applications peuvent collecter et partager vos informations de localisation. Cependant, de nombreux smartphones vous offrent la possibilité de gérer le partage de votre position dans les « paramètres ». Vous pouvez choisir les applications qui peuvent accéder à votre position ou vous pouvez choisir de désactiver complètement le paramètre de localisation. Réduire l'accès à la localisation peut également aider à augmenter l'autonomie de la batterie de votre téléphone. Si votre téléphone ne propose pas de paramètres de partage de localisation spécifiques, choisissez soigneusement vos applications lorsque vous téléchargez afin de ne pas partager votre localisation sans le savoir.

3. Désactivez le Bluetooth lorsque vous ne l'utilisez pas

Le Bluetooth permet à votre téléphone de communiquer avec d'autres appareils, comme l'option mains libres de votre voiture ou votre imprimante. Cependant, si quelqu'un d'autre y accède, il pourrait l'utiliser à mauvais escient pour accéder à vos informations ou intercepter vos appels. Désactivez le Bluetooth sur votre téléphone et activez-le uniquement lorsque vous devez vous connecter à d'autres appareils. De nombreux téléphones permettent également aux utilisateurs de définir des codes d'accès ou des niveaux de sécurité supplémentaires sur leur Bluetooth. Utilisez toutes les options disponibles pour améliorer votre confidentialité.

4. Vérifiez vos paramètres de confidentialité et de sécurité

La plupart des smartphones disposent de paramètres qui vous aideront à gérer votre confidentialité et votre sécurité. Vous pouvez trouver ces commandes dans les paramètres de votre téléphone ou dans les paramètres d'une application spécifique. Ces paramètres peuvent vous permettre de limiter l'accès d'une application aux données de votre téléphone, notamment l'accès à votre localisation, vos photos, vos contacts, vos notes, etc. Vous pouvez même bloquer les cookies et limiter les données collectées par votre navigateur mobile.

5. À quels comptes en ligne êtes-vous automatiquement connecté ?

L'une des fonctionnalités pratiques d'un smartphone est d'accéder rapidement à vos comptes de messagerie ou de réseaux sociaux d'un simple toucher du doigt. Cependant, cela signifie également que vous êtes toujours connecté à des comptes qui peuvent contenir des informations sensibles. Pensez à vous déconnecter de certains comptes si vous le pouvez, afin que d'autres personnes ne puissent pas y accéder si elles utilisent votre téléphone. Gardez à l'esprit que, selon le type de téléphone que vous possédez, vous ne pourrez peut-être pas vous déconnecter de certains comptes, tels que les comptes de messagerie, mais devrez peut-être supprimer l'intégralité du compte de votre téléphone. Dans ce cas, prenez votre décision en fonction de votre propre risque en matière de confidentialité et de sécurité. Bien qu'il puisse être gênant d'accéder au compte via le navigateur, cela peut être plus sûr.

6. Vérifiez les applications que vous téléchargez

Reconnaissez les applications qui se trouvent sur votre téléphone et si vous avez une application inconnue, supprimez-la. Les applications sont faciles à télécharger et à oublier, mais selon l'application, elle peut accéder à des informations privées ou être un programme de surveillance que quelqu'un a installé à votre insu ou sans votre consentement.

7. Mettez un mot de passe sur votre compte mobile pour empêcher les autres d'accéder à votre compte

Si vous craignez que quelqu'un contacte votre opérateur de téléphonie mobile pour obtenir des informations sur vous et votre compte, vous pouvez demander à votre opérateur de téléphonie mobile de mettre en place une sécurité supplémentaire sur votre compte, comme un mot de passe. Seule une personne disposant de ce mot de passe sera autorisée à apporter des modifications à votre compte.

8. Verrouillez votre compte téléphonique en ligne

Gardez à l'esprit que même si quelqu'un n'a pas accès à votre téléphone, il peut être possible pour lui d'accéder à votre compte en ligne. Les comptes en ligne peuvent inclure votre compte de téléphone mobile, vos journaux d'appels, vos comptes de messagerie ou de réseaux sociaux, votre compte Google Play/Apple AppStore ou iCloud. Mettez à jour les mots de passe et les questions de sécurité de ces comptes pour vous assurer que personne d'autre ne puisse y accéder.

9. Utilisez des numéros de téléphone virtuels (tels que Skype ou Viber) pour préserver la confidentialité de votre numéro

Pour optimiser davantage votre confidentialité, envisagez d'utiliser un numéro virtuel, tel que Skype ou Viber, ou un numéro jetable, afin de ne pas avoir à communiquer votre véritable numéro de téléphone. Un numéro de téléphone virtuel vous permettra également de filtrer les appels et de passer des appels/envoyer des SMS à partir du numéro virtuel.

10. Essayez de ne pas stocker d'informations sensibles sur votre téléphone

Bien qu'il puisse être tentant de stocker des informations telles que des mots de passe, des numéros de compte ou des informations personnelles sur votre téléphone, moins vous avez d'informations sensibles, moins quelqu'un d'autre risque d'y accéder. Vous pouvez même envisager de supprimer les SMS ou les messages vocaux sensibles afin qu'ils ne soient pas stockés sur votre téléphone.

11. Utilisez un logiciel anti-virus et anti-logiciel espion sur votre téléphone

Après des années d'avertissements, nous sommes assez habitués à nous assurer que nous avons des programmes anti-logiciel espion, anti-logiciel malveillant et anti-virus sur nos ordinateurs. Ces logiciels devraient également être utilisés sur nos smartphones. Recherchez des programmes dans les magasins d'applications et discutez-en avec votre fournisseur de services sans fil. Certains téléphones sont livrés avec un logiciel intégré que vous ne voudrez pas contourner.

12. Soyez prudent lorsque vous utilisez des applications de sécurité

Il existe de nombreuses « applications de sécurité personnelle » disponibles au téléchargement qui proposent d'accroître la sécurité personnelle des utilisateurs en les connectant immédiatement à des personnes de confiance sélectionnées. Plusieurs de ces applications sont conçues et commercialisées spécifiquement pour les

survivants de violences. Avant de faire confiance à une application de sécurité en cas d'urgence, assurez-vous de la tester avec vos amis et votre famille pour vous assurer qu'elle fonctionne correctement pour vous. Votre ami de confiance peut ne pas recevoir votre position avec votre appel d'urgence ou ne pas recevoir du tout votre appel à l'aide. Sachez toujours quel est le moyen le plus rapide d'accéder au 000 sur votre téléphone en cas d'urgence. De nombreux téléphones disposent d'un bouton d'appel d'urgence rapide que vous pouvez même composer sans saisir le code d'accès du téléphone.