6 conseils pour améliorer la sécurité de votre téléphone intelligent

Devolutions

LES TÉLÉPHONES INTELLIGENTS ONT CHANGÉ… NOTRE VIE AU GRAND COMPLET!

Les téléphones intelligents ont changé… notre vie au grand complet! Ils ont changé notre façon de travailler, nos interactions avec les autres, la façon dont on commande notre pizza (*miam… pizza!*), la manière dont nous achetons nos billets d'avion, nos habitudes de jeu – et j'en passe.

Grâce à leur capacité de traitement, leur connectivité et leurs innombrables applications, les téléphones intelligents sont comme des mini-ordinateurs qui peuvent être trainés partout et avec lesquels vous pouvez appeler vos amis. Ceci étant dit, pensez à toutes les informations qui se trouvent sur votre téléphone : courriels, messages texte, contacts, images, etc. Votre portable contient une tonne d'informations personnelles confidentielles.

Cependant, comme ils sont si pratiques et que nous les utilisons toute la journée (et parfois même la nuit!), nous avons tendance à négliger la sécurité de ces appareils. Ça expose nos informations privées et sensibles au risque de tomber entre de mauvaises mains. La bonne nouvelle, c'est qu'on peut adopter certaines mesures d'hygiène en matière de sécurité pour éviter d'être la cible des pirates et des fouineurs. Voici quelques conseils de base que vous devriez adopter :

1. Évitez d'avoir des conversations confidentielles en public

Je ne sais pas combien de fois je me suis assis dans un aéroport, un café, un restaurant ou un autre lieu public et j'ai entendu (pas volontairement bien sûr!) quelqu'un dire quelque chose d'incroyablement personnel et confidentiel en parlant sur son téléphone intelligent. N'oubliez jamais que quelqu'un pourrait écouter votre conversation!

Notre premier conseil d'hygiène de sécurité est donc bien simple : ne discutez jamais de quelque chose de confidentiel en public. Ça n'inclut pas seulement des sujets évidents comme les mots de passe. Ça inclut aussi vos plans de vacances ou même le partage de votre achat récent sur Amazon (parce que quelqu'un pourrait se précipiter chez vous et le saisir sur le pas de votre porte avant que vous n'ayez le temps de rentrer chez vous!). Ne tombez pas dans la paranoïa et ne pensez pas que « Big Brother » (ou Big Hacker dans ce cas-ci) vous écoute, mais servez-vous du gros bon sens et soyez prudents.

2. Méfiez-vous des faux messages texte

Les pirates informatiques sont connus pour envoyer de faux messages texte qui vous dirigent vers un site Web ou qui vous demandent d'ouvrir un document. Oui, la plupart de ces textes sont ridicules et vous les envoyez directement à la poubelle. Certains d'entre eux ont toutefois l'air vrais et semblent provenir de personnes et (en particulier) d'entreprises que vous connaissez et en qui vous avez confiance.

Le conseil ici est : en cas de doute, supprimez le texte ou (si vous le souhaitez) confirmez l'authenticité en appelant ou en envoyant un courriel à l'expéditeur. N'utilisez pas le numéro fourni dans le texte, parce qu'il peut également être faux.

3. Méfiez-vous des faux courriels

Les pirates informatiques sont étonnamment doués pour créer des objets qui attirent l'attention et qui obligent les gens à ouvrir des courriels (par exemple, « confirmer notre réunion de 15 h » ou « votre colis est retardé - détails à l'intérieur »). Vous devez faire preuve de la même prudence et de la même diligence que lorsque vous utilisez votre ordinateur de bureau ou votre ordinateur portable. La meilleure option est de supprimer les courriels suspects. Si vous les ouvrez, au moins ne cliquez sur aucun lien ou ne téléchargez aucune pièce jointe.

4. Téléchargez des applications uniquement à partir de sources fiables

Qui n'a pas 35 applications ou plus sur son téléphone intelligent?! De nos jours, nous avons des applications pour tout : jeux, réseaux sociaux, météo - et bien plus encore. La mauvaise nouvelle, c'est que les pirates utilisent des applications pour propager des logiciels malveillants. Pour éviter d'en être victime, installez les dernières mises à jour logicielles et contrôles de sécurité sur votre téléphone et téléchargez uniquement des applications provenant de sources fiables (par exemple, App Store, Google Play, etc.).

5. Rangez votre téléphone dans des endroits appropriés

Si vous êtes dans un lieu public, ne laissez jamais votre téléphone dans un sac ou une sacoche sur le sol, car il est très facile de le voler - il suffit de quelques secondes. Ce n'est pas non plus une bonne idée de garder votre appareil dans votre poche arrière.

En plus de le ranger dans un endroit approprié, n'oubliez pas de configurer votre téléphone pour qu'il se verrouille ou s'éteigne automatiquement après une période d'inactivité (choisissez une période courte!), et exigez un mot de passe, un code NIP ou une séquence pour le déverrouiller. Chiffrer vos données est également une sage décision, et vous devriez avoir la possibilité de localiser un appareil perdu et de supprimer des données à distance.

6. Utilisez des connexions Wi-Fi sécurisées

Connectez-vous à Internet à partir de réseaux Wi-Fi sécurisés uniquement. Si ce n'est pas possible, utilisez un VPN réputé pour chiffrer vos données et garder votre activité cachée.

La conclusion?

Les téléphones intelligents sont devenus essentiels. Sérieusement, je peux à peine respirer si je n'ai pas le mien! Nous devons cependant faire attention aux choses (et aux personnes) que nous aimons. Le contrôle de l'accès avec un mot de passe, l'installation d'applications légitimes et l'utilisation d'un accès à distance sécurisé peuvent empêcher vos informations privées de tomber entre de mauvaises mains. Comme je le dis toujours, mieux vaut prévenir que guérir!