

10 conseils pour garder vos appareils protégés pendant les vacances | Denis JACOPINI

 10 conseils pour garder vos appareils protégés pendant les vacances

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, voici un mini-guide conçu par les experts ESET pour voyager et surfer en toute tranquillité.

Brosse à dents ? ok.

Serviette de bain ? ok.

Ordinateur, téléphone, tablette ? ok.

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails. Pas de panique ! Stephen Cobb et d'autres professionnels ESET ont créé un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

Conseils



1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.

2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.

3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.

4. Mettez un mot de passe fort et activez la fonction « délai d'inactivité » sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous nos conseils pour un mot de passe efficace en cliquant ici.

5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.

6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.

7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.

8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).

9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.

10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants

Article original de ESET



Réagissez à cet article

Original de l'article mis en page : ESET – Actualités