Liste de vérification pour voyager en toute cybersécurité

Faire sa valise pour partir en voyage peut être stressant, mais voyager en toute cybersécurité ne devrait pas l'être. La sécurisation de vos appareils avant, pendant et même après votre voyage est un élément important. Celle-ci permet d'empêcher les cyberattaques, comme les maliciels, de compromettre vos renseignements personnels ou financiers.

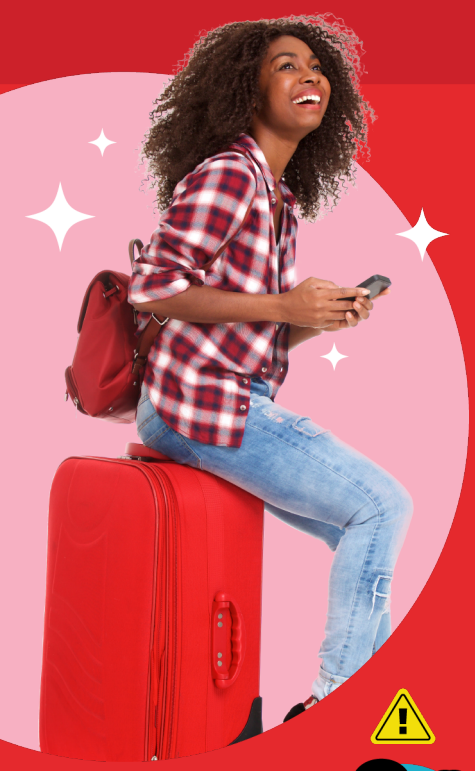
Sécuriser vos appareils lors de vos voyages

Utilisez cette liste de vérification pour que votre cybersécurité soit l'élément le moins stressant de votre voyage. Voici quelques conseils et astuces pour sécuriser vos appareils :

Avant votre voyage

- [ ] **Verrouillez vos appareils à l'aide d'un mot de passe, d'un NIP ou d'un code biométrique** pour les rendre plus difficiles d'accès en cas de perte ou de vol.
- [ ] **Activez l'authentification multifactorielle (MFA)** sur tous vos appareils et comptes pour ajouter une couche de protection supplémentaire.
- [ ] **Utilisez un réseau privé virtuel (RPV)** sur vos appareils pour vous connecter en toute sécurité au réseau Wi-Fi public si nécessaire.
- [ ] **Téléchargez du contenu sur vos appareils** à partir de votre réseau domestique sécurisé pour éviter d'utiliser des comptes personnels sur des réseaux non sécurisés pendant votre voyage.
- [ ] **Mettez en place un pare-feu** sur vos appareils pour empêcher les personnes malveillantes qui pourraient tenter de s'y connecter.
- [ ] **Activez un logiciel antivirus** pour surveiller l'activité suspecte sur vos appareils.
- [ ] **Mettez à jour les paramètres d'authentification de votre boutique d'applications** si vous voyagez avec de jeunes enfants afin qu'ils ne puissent pas faire d'achats surprises sur vos comptes, s'ils empruntent vos appareils.
- [ ] **Sauvegardez vos données** sur un disque dur ou sur un espace de stockage en nuage pour éviter de perdre vos renseignements personnels à cause de cybermenaces comme les rançongiciels.

Pendant votre voyage



- [ ] **Désactivez le réseau Wi-Fi de vos appareils** lorsque vous n'avez pas besoin de vous connecter à Internet pour éviter de vous connecter accidentellement à des réseaux non sécurisés.
- [ ] **Désactivez la technologie Bluetooth** lorsqu'elle n'est pas utilisée afin que les cybercriminels ne puissent pas se connecter à vos appareils.
- [ ] **Gardez vos appareils sur vous en permanence** ou rangez-les dans un coffre-fort, s'ils ne sont pas utilisés.
- [ ] **Soyez conscient de votre environnement** et faites attention aux personnes malveillantes qui essaient de voir votre écran.

- [ ] **N'utilisez pas de réseau Wi-Fi inconnu, non sécurisé ou public** lorsque vous accédez à des informations sensibles (utilisez vos données cellulaires si possible, sinon utilisez un réseau privé virtuel (RPV) pour une protection renforcée).
- [ ] **N'utilisez pas les bornes de recharge publiques**, mais uniquement votre chargeur personnel, vos écouteurs et d'autres accessoires que vous avez apportés de chez vous.

Après votre voyage

- [ ] **Utilisez un logiciel antivirus** pour détecter les activités suspectes sur vos appareils avant de les connecter à votre réseau domestique.
- [ ] **Supprimez les applications** que vous utilisiez en voyage et dont vous n'avez plus besoin.
- [ ] **Vérifiez vos comptes financiers** pour toute activité suspecte et signalez toute anomalie à vos institutions financières, à la police de votre région et au Centre antifraude du Canada.

Visitez le site de Pensez cybersécurité pour en savoir plus sur la façon de gérer la cybersécurité, de sorte qu'elle soit l'élément le moins stressant de votre voyage.

PENSEZCYBERSECURITE.CA

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Catalogue number: D96-103/2023F-PDF | ISBN: 978-0-660-49349-7