MOBILE **SECURITY**

INTERNET USE ABROAD

Be cautious when connecting to the internet abroad, as it can be vulnerable and exposed.

When in foreign countries, try to avoid conducting sensitive work. Assume that all network connections are being monitored. Do not use public Wi-Fi networks.

PROTECT YOUR DEVICE

Mobile devices are a prime target for theft. Keep your device in your possession at all times, use password protection and minimize the amount of information you store on them. If stolen, the information contained within may be accessed and/or used for malicious purposes. Using your device, malicious actors can...

- Track your location
- Activate the microphone
- Intercept electronic communications

UNSECURED DATA IS VULNERABLE

When possible, use a Virtual Private Network (VPN) to increase the security of your connection.

Without encryption, others can access your unsecured public network and access data travelling through it. Use Virtual Private Networks (VPNs) to increase the security of your connection.

$ PAY-PER-USE NETWORKS DO NOT CERTIFY SECURITY

Always use caution when using unknown networks.

Paying for a network doesn't mean it is safe. Many paid networks are unencrypted and are accessed by multiple people. Keep your device secure by avoiding untrusted network connections.

CAN YOU TRUST YOUR CONNECTION

Encryption protects the confidentiality of data. If you are using an unencrypted connection, your information is open for all to see.

Whenever possible, ensure you use a trusted and encrypted connection to secure your internet access.

CYBER CRIME IS A REAL THREAT

Cyber Crime is on the rise and has shown double-digit growth year after year. Every second, 18 adults become victims of a cyber crime incident.

Protect your information and understand that important tasks, such as online banking, should not be conducted on unsecured and untrusted Wi-Fi connections.

BEST PRACTICES

- Use a PIN or strong password to access the device
- Disable features not in use such as GPS, Bluetooth or Wi-Fi
- Avoid joining unknown or unsecured Wi-Fi networks, and if you must connect to a Hot Spot, set the network location to "Public"
- Do not use "Remember Me" features on websites and mobile applications – always type in your password
- Avoid opening files, clicking links or calling numbers contained in unsolicited text messages or e-mails
- Maintain up-to-date software, including operating systems and applications
- Encrypt personal or sensitive data and messages
- Do important tasks, like online banking, on a private or known trusted network

SÉCURITÉ DES DISPOSITIFS MOBILES

UTILISATION D'INTERNET À L'ÉTRANGER

Soyez vigilant lorsque vous vous connectez à Internet dans un pays étranger, car la connexion peut présenter des vulnérabilités.

Évitez d'accomplir des tâches de nature sensible à l'étranger. Tenez pour acquis que toutes les connexions réseau font l'objet de surveillance. N'utilisez pas de réseaux Wi-Fi publics.

PROTECTION DE VOS DISPOSITIFS

Les dispositifs mobiles représentent des cibles de choix pour les voleurs. Gardez-les toujours sur vous et minimisez la quantité d'information qu'ils contiennent. Protégez toujours vos dispositifs par un mot de passe. S'ils sont volés, l'information qu'ils contiennent pourrait être accessible et utilisée à des fins malveillantes. Des acteurs malveillants pourraient...

- Découvrir votre emplacement
- Activer votre microphone
- Intercepter vos communications électroniques

LES DONNÉES NON SÉCURISÉES SONT VULNÉRABLES

Dans la mesure du possible, utilisez un réseau privé virtuel (RPV) pour accroître la sécurité de votre connexion.

Tout le monde peut accéder aux réseaux publics non chiffrés et donc non sécurisés, et obtenir les données qui y transitent. Utilisez les RPV pour sécuriser vos sessions de navigation.

PRATIQUES EXEMPLAIRES

- Utilisez un NIP ou un mot de passe fort pour accéder au dispositif.
- Désactivez les fonctions non utilisées comme les capacités GPS, Bluetooth ou Wi-Fi.
- Évitez de vous connecter à des réseaux Wi-Fi inconnus ou non sécurisés. Si vous devez absolument vous connecter à un point d'accès, sélectionnez la configuration d'un réseau public.
- N'utilisez pas la fonction « se souvenir de moi » des sites Web et des applications mobiles – entrez toujours votre mot de passe.
- Évitez d'ouvrir des fichiers, de cliquer sur des liens ou de composer des numéros contenus dans des messages texte ou des courriels non sollicités.
- Gardez les logiciels à jour, y compris les systèmes d'exploitation et les applications.
- Chiffrez les données et les messages personnels ou sensibles.
- Réalisez les tâches importantes, comme les transactions bancaires en ligne, sur un réseau privé ou fiable.

$ LES RÉSEAUX FACTURÉS À L'UTILISATION NE GARANTISSENT PAS LA SÉCURITÉ

Soyez toujours vigilant lorsque vous utilisez des réseaux inconnus.

Les réseaux pour lesquels il faut payer ne sont pas synonymes de sécurité. De nombreux réseaux payants ne sont pas chiffrés et plusieurs personnes peuvent y accéder. Gardez votre dispositif en sécurité en évitant les connexions aux réseaux inconnus.

VOTRE CONNEXION EST-ELLE FIABLE?

Les fonctions de chiffrement protègent la confidentialité des données. Si vous utilisez une connexion non chiffrée, tout le monde peut accéder à votre information.

Dans la mesure du possible, utilisez une connexion fiable et chiffrée.

DES RISQUES SONT ASSOCIÉS AU CYBERCRIME

Le cybercrime est à la hausse. Il affiche une croissance à deux chiffres année après année. Chaque seconde, 18 adultes sont victimes d'une cyberintrusion.

Protégez votre information et sachez qu'il ne faut pas effectuer de transactions bancaires ou toute autre tâche importante en ligne sur un réseau Wi-Fi non sécurisé et non fiable.