Get Cyber Safe travel checklist

Keep your devices secure while travelling
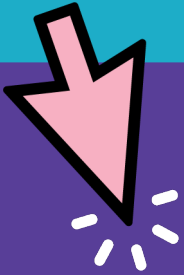
Packing for a vacation can feel stressful but being cyber safe for your trip shouldn't be. Securing your devices before, during and even after your trip is an important part of travelling to prevent cyber attacks, like malware, from compromising your personal or financial information.

Use this checklist to make cyber security the least stressful part of your vacation. Here are some tips and tricks that you can use to secure your devices:

Before you travel

- [ ] **Lock your devices with a password, PIN or biometric** to make them more difficult to access if they get lost or stolen

- [ ] Enable **multi-factor authentication (MFA)** on all your devices and accounts to add an extra layer of protection

- [ ] Use a **virtual private network (VPN)** on your device to safely connect to public Wi-Fi if necessary

- [ ] **Download streaming content** to your device from your secure home network to avoid using personal accounts on unsecure networks while you're away

- [ ] **Set up a firewall** on your device to restrict malicious activity trying to connect to your device

- [ ] **Enable anti-virus software** to monitor your device for suspicious activity

- [ ] **Update your app store authentication settings** if you're travelling with young children so they can't make surprise purchases on your accounts if they borrow your devices

- [ ] **Back up your data** to a hard drive or cloud storage to avoid losing your personal information to cyber threats like ransomware
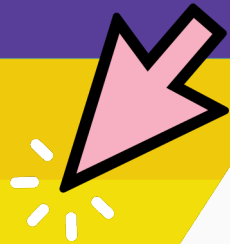
During your travel

☐ **Disable your device's Wi-Fi** when you don't need to connect to the internet to avoid accidentally connecting to unsecured networks

☐ **Disable your Bluetooth** when it isn't in use so cyber criminals can't connect to your device

☐ **Keep your device with you at all times** or lock devices in a safe if they aren't being used

☐ **Be aware of your surroundings** and watch out for shoulder surfers trying to view your screen

☐ **Do not use unknown, unsecured, or public Wi-Fi** when accessing sensitive information (use your cellular data if possible, if not use a VPN for enhanced protection.)

☐ **Do not use public charging kiosks**, only use personal chargers, headphones, and other device accessories that you brought from home
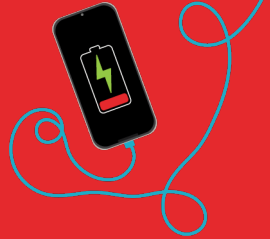
After you travel

☐ **Use anti-virus software** to scan devices for malicious activity before connecting to your home network

☐ **Delete apps** that you used while travelling that you no longer need

☐ **Check your financial accounts** for any suspicious activities and report anything amiss to your financial institutions, local police, and the Canadian Anti-Fraud Centre

Visit the Get Cyber Safe website to learn more about how to make cyber security the least stressful part of travelling.

GETCYBERSAFE.CA

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada