CANADIAN CENTRE FOR CYBER SECURITY

Mobile devices and business travellers

October 2024

ITSAP.00.087

As an employee, you're privy to your organization's important and sensitive information. You're responsible for protecting it whether you're in the office, working from home, or travelling. As a business traveller, you should carefully consider the potential risks of using a mobile device when travelling. A compromised device may allow unauthorized access to your organization's network and its information. Before you travel, consider the following points.

- Threat actors may identify and target mobile devices to:
  - deliver malicious code to the device to access information and infect other devices on your organization's network
  - use the device's network connections, such as Wi-Fi or Bluetooth
  - activate the microphone or camera
  - track your location
  - intercept communications that are sent electronically
- In some countries, hotel business centres and phone networks are monitored, and rooms may be searched.
  - Assume there is no privacy in offices, hotels, Internet cafes, or other public areas.

High-risk travel

Travel can be considered high-risk when factoring in the following variables:

- identity of the traveller (for example, Chief Executive Officer)
- special events (for example, The World Economic Forum)
- high-risk locations, as defined by Global Affairs Canada (GAC)

If you are unsure of the risk, contact your IT security department.

High-risk travel requires the following special considerations:

- Contact your IT department to request a travel device for your trip if possible
  - If you must use a personal device, turn off Bluetooth, Wi-Fi, and location sharing and use a VPN.
- Assume that all communications transmitted over public carriers are at risk of being intercepted. Encrypt all sensitive information on your mobile devices before your trip.
- Report any unusual device performance issues or any other associated security concerns to your IT security department.

AWARENESS SERIES

© His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2024

Cat. No. D97-1/00-087-2024E-PDF
ISBN 978-0-660-72983-1

Guide for business travellers

Before you travel

- **Protect your assets.** Back up your information and update device software to improve defence capabilities.
- **Move anonymously.** Deactivate features such as location, Bluetooth, and auto-connect settings on your device.
- **Travel light.** Take only the devices that you need and remove unnecessary data.
- **Lock it down!** Update your credentials with complex passphrases and passwords and activate multi-factor authentication (MFA), if available.
- **Avoid using free password managers** that are not part of your operating system or browser.

While you travel

- **Keep your devices in your possession at all times**. If you must leave a device unattended, remove the battery and SIM card if possible, and keep them with you.
- **Be aware of your surroundings.** Be mindful of shoulder surfers trying to view your screen or keyboard. Power off devices while going through customs or other inspection points.
- **Deactivate the "Remember Me" feature on websites of business or personal value** and where MFA is not available, enter your login credentials every time so your passwords are not stored.
- **Connect safely.** Where possible, use your cellular data plan to access the Internet and avoid unknown, unsecured, or public Wi-Fi networks when accessing sensitive information.
- **Communicate securely.** Do not store or communicate information above the approved classification of the device. Do not use PIN-to-PIN messaging to exchange sensitive information as it is not protected by security settings.

After you travel

- **Report suspected security concerns** to your IT security department.
- **Switch it up!** Change passphrases, passwords, or PINs on your devices and accounts that you accessed while abroad.
- **Use anti-virus software** to scan devices for malicious activity before connecting to your home and work networks.

Learn more

- Using your mobile device securely (ITSAP.00.001)
- Mobile device guidance for high profile travelers (ITSAP.00.088)
- Device security for travel and work abroad (ITSAP.00.188)
- Securing the enterprise for mobility (ITSM.80.001)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at the Cyber Centre **cyber.gc.ca**