Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

MOBILE DEVICES AND BUSINESS TRAVELLERS

MAY 2021

ITSAP.00.087 V2

As a business traveller, you should carefully consider the potential risks of using mobile devices during your travel. A compromised device can allow unauthorized access to your organization's network, placing not only your information at risk, but also that of your organization. This document offers information on the threats and risks to mobile devices during travel and how to best prevent these risks from becoming a reality.

THREATS AND RISKS

Mobile devices are a prime target for theft. If stolen, a threat actor may be able to access the information contained on your device and use the device or the information for malicious purposes. Everyone should take precautions to protect their mobile devices when travelling. However, individuals who hold senior positions or work with valuable information may have a higher risk of being targeted by threat actors.

Threat actors can use commercial eavesdropping devices (e.g. International Mobile Subscriber Identity [IMSI] catchers) to do the following:

- Identify and target mobile devices
- Deliver malicious code to the device
- Use the device's network connections (e.g. Wi-Fi, Bluetooth)
- Access the device and track your location
- Activate the microphone or camera on the device
- Intercept communications

In some countries, hotel business centres and phone networks are monitored, and rooms may be searched. Users should assume that there is no privacy in offices, hotels, Internet cafes, or other public areas.

BEFORE YOU TRAVEL

Before you travel, take the following actions:

- Disable features such as Bluetooth and wireless headset capabilities
- Remove unnecessary data
- Take only the devices that you need to do the job
- Change your passphrases and passwords before you leave
- Back up your data

AWARENESS SERIES

Cat. No. D97-1/00-087-2021E-PDF
ISBN 978-0-660-38741-3

WHILE YOU TRAVEL

While you travel, you can take the following actions to protect yourself:

- Keep possession of your phone at all times. If you must leave the device unattended, remove the battery, if possible, and the SIM card and keep them with you.
- Power off devices while going through customs or other inspection points.
- Empty your Trash and **Recent** folders after every use. Clear your browser after each use (delete history files, caches, cookies, URL, and temporary internet files).
- Be aware of your surroundings and be mindful of shoulder surfers trying to view your screen or keyboard.
- **Do not use** the Remember Me feature on websites. Enter your log-in credentials every time.
- **Do not use** unknown, unsecured, or public Wi-Fi networks and charging kiosks.
- **Do not** store or communicate information above the approved classification of the device.
- Keep an eye on your cables, chargers and peripherals. Modern cables can be programmed to compromise your device since they can contain microcontroller components.
- **Do not** open emails, attachments, or click on links sent from unknown sources.
- Do not accept chargers
- Contact your IT Security department right away if your device is stolen or misplaced, or if you have a security concern.

AFTER YOU TRAVEL

When you return from your trip, take the following actions:

- Report suspected security concerns to your IT security department.
- Change the passphrases, passwords, or PINs on your devices or accounts that you accessed while abroad.

HIGH-RISK TRAVEL

Travel can be considered high risk if the traveller's identity is well known or is high-profile (e.g. Chief Executive Officer), if the event or conference is widely known about (e.g. The World Economic Forum), or if the destination is high-risk (as defined by Global Affairs Canada). If you are unsure of the risk, contact your IT Security department.

High-risk travel requires the following special considerations:

- Do not use your regular business or personally owned devices. If you must use a personal device, turn off Bluetooth, Wi-Fi and location sharing and use a VPN.
- Ask your IT department if they have an inventory of devices for travel or "burner devices" and "burner accounts" for high-risk, high-threat environments.
- 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.
- Assume that hotel Internet connections, photocopiers, or fax machines are monitored. Only use them for non-sensitive information.
- Report any unusual device performance issues or any other associated security concerns to your IT Security department.

ADDITIONAL PUBLICATIONS

The Cyber Centre has created additional publications that provide guidance to business travellers using their mobile devices. These publications include:

- *ITSAP.00.001 Using your Mobile Device Securely*
- *ITSM.80.001 Securing the Enterprise for Mobility*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.30.030 Secure Your Accounts and Devices With Multi-Factor Authentication*
- *ITSAP.30.025 Password Managers-Security*
- *ITSAP.70.015 Security Tips for Peripheral Devices*

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