Communications Security Establishment | Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

MOBILE DEVICES AND BUSINESS TRAVELLERS

OCTOBER 2018

ITSAP.00.087

What are the threats and risks?

As a business traveller, you should carefully consider the potential risks of using a mobile device during your travel. A compromised device has the potential to allow unauthorized access to your organization's network, placing not only your own information at risk, but also that of the organization. Please consider these key points:

- Individuals holding senior positions or those who work with valuable information may have a higher risk of being targeted through their mobile devices
- Commercial technologies (e.g., International Mobile Subscriber Identity (IMSI)catchers) exist which allow threat actors 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)
  - Use the device as a means of infecting other networks in your organization
  - Access the device to track your location
  - Activate the microphone or camera on the device
  - Intercept communications that are sent electronically
- In some countries, hotel business centers 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.
- Mobile devices are a prime target for theft. If stolen, the information contained within may be accessed or used for malicious purposes.

Best Practices—Before you Travel

- Disable features such as Bluetooth and wireless headset capabilities.
- Remove unnecessary data.
- Only take the devices that are necessary to do the job.
- Change your passwords before you leave.
- Back-up your important data.

Want to Learn more?

Read our following documents:

- Mobile Device Security—Securing the GC (ITSE.80.001)
- Using your Mobile Device Securely (ITSAP.00.001)
- Securing the Enterprise for Mobility (ITSM.80.001)
- Mobile Technologies in International Travel - Guidance for Government of Canada IT Security Managers (ITSB-88)

AWARENESS SERIES

Best Practices—While you Travel

- Keep your device in your possession 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 inspections points.
- Change your passwords at regular intervals on mobile devices and frequently used applications and Web sites.
- 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 who might be able to view your screen or keyboard.
- Do not use the *remember me* feature on websites, retype your password every time.
- Do not use public Wi-Fi networks.
- Do not store or communicate information above the approved classification of the device.
- PIN-to-PIN messaging is not suitable for exchanging sensitive information and is not protected by security settings.
- Do not open e-mails, attachments or click on links from unknown sources.
- Contact your IT Security department as soon as possible for assistance if your device is stolen, misplaced or if you suspect a security concern.

Best Practices – After you Travel

- If your device was not in your possession for any reason or if you suspect a security concern, report this information to your IT Security department.
- Change the passwords on your devices and on any online services you accessed while abroad.

High Risk Travel

Travel can be considered high risk when there is a combination of the following factors: Identity of the traveller (e.g. Chief executive officer), special event (e.g. The World Economic Forum) or high risk locations as defined by Global Affairs Canada (GAC). If 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 your organization has an inventory of devices for travel, contact your IT department to request one for the duration of your trip. If you must use a personal device, keep Bluetooth, Wi-Fi and location sharing off and for extra security use a VPN.
- Assume that all communications transmitted over public carriers are at risk of being intercepted and Encrypt all sensitive information on your mobile devices before beginning your trip.
- Assume that hotel internet connections, photocopiers, or fax machines are monitored and, therefore, should only be used for non-sensitive information.
- Report any unusual device performance issues observed during your travel or any other associated security concerns to your IT Security department.

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 (CCCS) **cyber.gc.ca**