CSE advice:

Mobile Technologies in International Travel - Guidance for Government of Canada Business Travelers

Introduction

International travel is an essential part of Government of Canada (GC) business. Mobile technologies such as personal digital assistants (PDAs), cellular phones, smart phones, laptops, and tablets are key enablers for operational efficiency. While these devices are vital to the modern workforce, they are also susceptible to security threats and therefore must be properly managed.

Security Considerations

Government employees embarking on international travel face increased Information Technology (IT) security risks. As a business traveler, you should carefully consider the potential risks of using a mobile device during your travel. Any compromise of your device could have a negative impact on your department, its information and its reputation. A compromised device has the potential to allow unauthorized access to your departmental network, placing not only your own information at risk, but also that of the department.

Consider these key points:

- Individuals holding senior positions within government and/or those who work with valuable information may be at higher risk of being targeted through their mobile devices.
- Capabilities exist which allow threat actors to:
  - identify and target mobile devices;
  - deliver malicious code to the device;
  - use device network connections (e.g.: wireless, Bluetooth, etc.) for their own purposes;
  - leverage the device as a means of infecting other GC networks;
  - access the device as a means to track your location (e.g.: GPS);
  - activate the microphone on a device; and
  - intercept communications that are sent electronically.
- In some countries, hotel business centers and phone networks are monitored and in some locations, rooms may even be searched. As a general guideline, assume that there is no expectation of 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 and/or used for malicious purposes.

Protect Your Information

Traveling to high risk locations increases the probability of IT Security compromises. The following guidance provides steps to take **before**, **during**and **after** you travel to increase the security of the information stored on your mobile devices. Consult your IT Directorate for more information about any of the recommendations noted below.

High Risk Travel: Do not use your regular business device or personally owned devices. It is recommended that you contact your IT Directorate to request a travel inventory device. In addition:

- Keep your device in your possession at all times. If you must leave the device unattended, remove power sources (e.g.: battery) and the SIM card (when applicable) and keep them with you.
- USB sticks, camera memory cards and other storage devices can be used as a method of delivering malicious code to networks. Do not use storage devices given to you or purchased from unknown or unapproved sources and avoid using your own thumb drive in a foreign computer.
- Assume that all communication transmitted over public carrier is at risk of being intercepted.
- Assume that rented/hotel internet portals, photocopiers, etc. are monitored and therefore should only be used for non-sensitive information.
- Seek the assistance of the Canadian embassy should you encounter security issues while traveling abroad (www.voyage.gc.ca).
- When you return:
    - return your temporary travel inventory device to your IT Security Directorate (do not connect it to the network);
    - report any unusual device performance issues observed during your travel or any other associated security concerns to your IT Security Directorate or Corporate Security area; and
    - if you received removable storage devices while traveling (USB sticks, camera memory cards, etc.), do not connect these devices to computers on GC networks without consulting with your IT Security Directorate for support.
- Review and adopt the best practices noted below for before, during and after you travel.

Low Risk Travel: Use your regular business device and follow the best practices noted below.

Best Practices - Before You Travel

In conjunction with the policies established by your department:

- Disable features such as Bluetooth and wireless headset capabilities for the duration of your trip.
- Minimize the information contained on your devices.
- Remove unnecessary data. Data stored on personal devices provides a source of information to assist in targeting you (e.g.: photos/messages from friends and family, schedules, financial information, etc.).
- Only take devices which are necessary to do the job to minimize the number of devices you travel with.
- Change your passwords before you leave. Employ strong passwords on all of your devices using a combination of numbers, upper and lower case letters and/or special characters – at least 8 characters in length. Never store passwords, phone numbers, or sign-on sequences.
- Back-up your important data. If your device is compromised, you may not have the ability to recover the data.

Best Practices - While You Travel

- Keep your device in your possession at all times, not only to prevent theft and loss, but also to protect the confidentiality of information stored on the device (e.g.: avoid leaving devices in checked baggage).
- Change your password(s) at regular intervals for Government of Canada devices as well as for personally-owned 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 / keyboard especially in public areas (e.g.: shield passwords from view) and terminate connections when you are not using them
- Remain cautious when browsing the web for personal use as this could expose your personal information and or financial information to risk of compromise (e.g.: online banking) and do not use the*‘remember me’* feature on websites (e.g. re-type your password every time).
- Do not use public Wi-Fi networks. If you must use a Wi-Fi connection, select the *‘public network’* designation instead of *‘work’* or *‘home’* to prevent unintended file sharing (for Microsoft Windows).
- Do not store or communicate information above the approved classification of the device. This includes talking about sensitive information and/or sending sensitive information via email.
- 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 Directorate as soon as possible for assistance if your device is stolen, misplaced or if you suspect a security concern.

Best Practices - When You Return

Before you connect your device back to the Government network:

- 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 Directorate.
- Change the passwords on your device(s).

Interactive Galleries:

Cyber Security and Wireless Networks

https://www.cse-cst.gc.ca/en/interactive-media-medias-interactifs/cyber-security-and-wireless-technologies

Cyber Security and Social Media

https://www.cse-cst.gc.ca/en/interactive-media-medias-interactifs/cyber-security-and-social-media