CANADIAN CENTRE FOR
CYBER SECURITY

UNCLASSIFIED
SEPTEMBER 2021 | ITSAP.00.088

Mobile Device Guidance for High-Profile Travellers

If you're someone who is in a high-profile position, such as a politician or a senior executive, you need to protect the security of your mobile devices when you travel. Mobile devices contain sensitive information and they are high-value targets for cyber threat actors. If your device or the information on it is compromised, it could be used against you or the organization you represent. Below, we cover some of the common threats and the security measures you should take before, during, and after you travel to protect your mobile devices.

THREATS

Threat actors use different techniques to gain access to devices and sensitive information. Some attack methods practiced are included in the following examples:

- **Shoulder-surfing:** Using in-person visibility to steal your sensitive information.
- **Phishing**: Sending fraudulent emails or texts that include malicious files, malicious links, or requests for personal information.
- **Network spoofing:** Masquerading as another network.
- **Signal jamming:** Interfering with, disrupting, or blocking communications signals and services.
- **In-the-middle attacks**: Exploiting vulnerabilities to intercept communications.
- **Ransomware:** Using malicious software to encrypt files or lock systems and devices until the victim pays a sum of money.

For more information on these types of threats, refer to *ITSAP.00.100 Don't Take the Bait: Recognize and Avoid Phishing Attacks*, *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi*, and *ITSAP.00.099 Ransomware: How to Prevent and Recover*.

RISKS

Travel is considered **high-risk** if a traveller's identity is well-known or high-profile. This is especially true when the high-profile traveller is going to a widely known event or conference (e.g. The World Economic Forum), or the traveller's destination is considered high risk by Global Affairs Canada.

When travelling, threat actors from foreign intelligence services, criminal groups, or competitor organizations may attempt to compromise your devices. As someone in a high-profile position, the information you deal with may be highly sensitive. Threat actors target technical, political, strategic, military, financial, and personal data. If your devices, or the information contained on them, are compromised, it could be used against you or the organization you represent.

Your organization should consider any risks introduced by international travel and determine its level of tolerance. You and your organization should implement measures to mitigate those identified risks.

Communications Security Establishment | Centre de la sécurité des télécommunications
Canada

Cat. No. D96-74/2021E-PDF ISBN 978-0-660-40283-3

BEFORE YOU GO

- Use corporately owned, temporary devices ("burner devices") if possible.
- Enforce multifactor authentication (MFA) to access devices and accounts.
- Install anti-virus and spyware protection and a firewall.
- Run updates and install patches for operating systems and applications.
- Back up devices for possible recovery when returned.
- Remove unnecessary data and applications from devices.
- Install a virtual private network (VPN) on your devices to securely transfer data.
- Configure a sandbox to securely access organizational data apart from other device applications.
- Limit administrative privileges to secure software settings and restrict downloadable applications
- Configure devices to run anti-virus software on storage devices (e.g. USB drives) upon installation.
- Implement appropriate network security settings for devices (e.g. restrict Wi-Fi connectivity to secure networks, disable hot-spot discovery).
- Configure mobile devices to disable external connection access (e.g. Wi-Fi and Bluetooth) while accessing the organization's secure network (i.e. internal network).
- Turn off devices before going through customs and security.
  - Inform IT if your device is inspected by security.

DURING YOUR TRIP

- Encrypt sensitive information.
- Avoid using personal accounts, if possible.
  - If necessary, secure with MFA, inform IT, and change passwords when returned home.
- Disable Bluetooth and Wi-Fi.
- Assume that communications transmitted over public carriers can be intercepted.
- Avoid using hotel, and public Wi-Fi and Bluetooth.
- Use your organization's network and VPN to access and send sensitive information.
- Maintain control of chargers, cables, and peripherals at all times.
- Avoid using storage media (e.g. USB) and peripherals given to you by external sources.
- Keep your devices in your possession and be aware of your surroundings at all times

WHEN YOU RETURN

Monitor your devices for unusual behaviours. Indicators such as your device acting slow or pop-ups disappearing before you can read them will need to be brought to the attention of your IT security team.

Compare the device's image with a backup for signs of malicious activity.

If your device has been compromised, forensic research is recommended and a factory reset to restore the device is recommended.

Use a secure back up to restore the device before further use.

If you notice suspicious activity on your device during or after travel, follow these security measures:

1. Disconnect your device from the Internet and any other devices.
2. Use another device to contact your service provider and your IT team to begin the appropriate incident management processes.
3. Keep the device disconnected for the rest of your trip.
4. Examine the device in your organization's secure environment once returned from travel.
5. Eliminate the threat from the device and use the latest secure backup to restore the device.
6. Replace the device's SIM card.

LEARN MORE

Visit our website (**cyber.gc.ca**) to find a catalogue of our publications, including:

- *ITSAP.00.087 Mobile Devices and Business Travellers*
- *ITSAP.70.002 Security Considerations for Mobile Device Deployments*
- *ITSAP.10.096 How Updates Secure Your Device*
- *ITSAP.40.016 Using Encryption to Keep Your Sensitive Data Secure*
- *ITSAP.80.101 Virtual Private Networks*

Cat. No. D96-74/2021E-PDF ISBN 978-0-660-40283-3