CYBER AND ESPIONAGE THREATS to GC Senior Officials and Employees TRAVELLING ABROAD

GC SENIOR OFFICIALS AND EMPLOYEES: ATTRACTIVE TARGETS

Foreign governments collect intelligence to advance their own national objectives, security and economic interests. Government of Canada (GC) senior officials and employees are attractive targets for collection activities because of their access to privileged information, GC decision makers and their contacts that could benefit other countries. Canadians travelling at the behest of the GC are particularly vulnerable because (i) they have limited control over their immediate surroundings and (ii) foreign governments and their agents act with greater impunity on home soil. Some countries may not be able to prevent threat activities by state actors from other countries operating within their borders.

Major international events may attract the attention of threat actors and could possibly increase the likelihood of malicious cyber and espionage activities targeting the event and its participants. Areas in and around locations of public international events, as well as designated spaces and services for the delegations (e.g., restaurants, hotels, meeting rooms and transportation) may be under surveillance by threat actors. As such, these areas should not be considered safe zones for sensitive discussions and no documents or electronic devices should be left unattended.

YOU COULD BE TARGETED WHEN TRAVELLING ABROAD

VIA YOUR ELECTRONIC DEVICES

Mobile phones and other wireless devices (e.g., iPads and smart watches) may be vulnerable and can be exploited by threat actors. Mobile phones can be targeted when logging onto free Wi-Fi; by clicking on a link in a phishing email; or by someone with physical access to your phone (particularly security or customs, or when left unattended). Certain countries control and manipulate the Internet infrastructure in their jurisdiction which can be used to compromise your device.

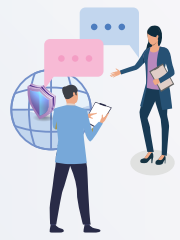
ANY MOBILE PHONE CAN BE ACCESSED COVERTLY THROUGH BYPASSING SECURITY PROTOCOLS

- Cyber threat actors can take snapshots of your screen and obtain information such as online banking, social media and Web activities.
- Telephone cameras may be covertly activated to take photos of you and your surroundings.
- Likewise, microphones may be remotely activated. Surveillance software, or spyware, such as Pegasus, can obtain GPS coordinates to track your movements, even while your mobile phone is in airplane mode.

See the Canadian Centre for Cyber Security's website for guidance on how to protect your information and IT assets.
Visit: cyber.gc.ca/en/guidance

ELICITATION

a technique used by foreign agents whereby they engage you in what appears to be harmless or random conversation, with the aim of subtly extracting information about you, your work and colleagues.



CULTIVATION

a representative of a foreign intelligence service (whose true identity is unknown) attempts to establish a relationship with you and recruit you. Be vigilant and mindful of discussions regarding your work, even if seemingly benign.

EAVESDROPPING

activities ranging from strategic positioning of unobtrusive bystanders to using concealed sophisticated audio and visual devices to surveil your sensitive or classified discussions. Be aware of your surroundings in public settings; avoid sensitive or classified discussions outside of secure areas (e.g., taxis, restaurants, elevators, hotel rooms, aircrafts and trains).

INTRUSION

a threat actor enters your hotel room to steal or copy sensitive documents in hard or digital form. Threat actors may rent rooms or floors in advance of planned delegation arrivals to install intercept devices or support intrusions while you are away. They may also recruit hotel staff to report on you and your movements.

PROTECTING YOURSELF WHEN TRAVELLING ABROAD

EXERCISE PROPER CYBER SECURITY HYGIENE

- Do not carry cell phones or smart technology near sensitive or classified discussions.
- Ensure your devices have the most recent updates and patches installed.
- Beware of phishing messages. Do not click on suspicious links from unknown senders. Verify that the sender's email is accurate.
- Ensure maximum security settings on your email accounts.
- Use up-to-date anti-virus/anti-malware on computers.
- Do not use USB sticks on distrusted computers or from unknown sources on your devices.
- Do not enter personal information, such as online banking. Only use public computers to search general websites.

ENSURE PROPER HANDLING OF ALL CLASSIFIED AND SENSITIVE INFORMATION

- Send classified information to your destination via appropriate accredited means prior to your departure.
- When required to transport information, ensure it is in an appropriate secure carrying case; never leave the case unattended.
- Only read, access and store classified information in a secure accredited environment or via a secure IT system.
- Do not discuss sensitive information over a phone or near a cell phone or other wireless device, or over open email or encrypted apps (Signal, WhatsApp, etc.).
- Do not write or store any classified information on devices that connect to the Internet.
- Assume that any information provided to airline or border control agents will be collected by the host country.
- Be discreet about your identity, your employment and your location.

Report any suspicious activities to the nearest Canadian embassy.

Canada