
Canadian Security Intelligence Service
Service canadien du renseignement de sécurité
FAR
FROM
HOME
A travel security guide
A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.
DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.
Canada

TABLE OF CONTENTS

THE THREAT ENVIRONMENT

In a world that increasingly measures national power and security in economic as well as military terms, Canadian citizens travelling abroad may be the target of foreign intelligence collection activities. Many foreign governments and businesses place a high priority on acquiring classified government-protected information as well as sensitive proprietary information related to research and innovation from Canadian businesses, industries and academic institutions. The threat you face as a Canadian traveller is real.

This guide describes the nature of the foreign intelligence, terrorism and economic threats, provides basic steps you can take to mitigate the associated risk, and actions you should take to report suspicious incidents.

SECURITY IS A STATE OF MIND

You are responsible for your own safety. The majority of safety issues can be managed appropriately through good planning, preparation, and sound security practices.

Your best security tool is your situational awareness, which means being aware of what is going on in your environment and understanding what impact that might have on your personal safety. This could change on a daily or even hourly basis. Always remain aware of the environment and keep up to date on the potential threats in the area within which you are travelling.

The security assumptions we make about overseas travel being easy and safe are often wrong. For many of us, overseas travel has become so routine that we incorrectly assume it to be low-risk. You need to take special precautions when traveling in an official capacity, especially to countries with safety and security concerns. If you are travelling on behalf of a government organization, you should receive a country-specific briefing from a designated security officer before your departure.

Similarly, if you are travelling on behalf of your company or industry group or an academic institution, you should consult country-specific security information from a trusted source such as **travel.gc.ca**. Never make assumptions when travelling overseas. Always research your destination and prepare yourself for your own travel. You are always in charge of your own security.

Your vigilance should be heightened while overseas. When you travel abroad, you may be vulnerable due to the limited control you exercise over your immediate surroundings. Foreign governments and their agents act with greater impunity on their own soil, to say nothing of local extremists and criminals.

Familiarize yourself with the law. It is very important that you familiarize yourself with the laws, customs and culture of the country or countries you are about to visit. You are subject to the laws and regulations of the country you are visiting for which your Canadian citizenship will offer you little immunity. Note that even a diplomatic passport does not prevent you from being targeted during your stay in a host country. Before departing you should consult **travel.gc.ca** for country-specific information, as well as keep copies of the contact information for the nearest Canadian Embassy, High Commission or Consulate.

Canada and Canadians are targets for many hostile actors. Canada and Canadians have been, and will continue to be, targeted by foreign intelligence agencies seeking state, industrial and academic secrets; by extremists who see you, as a representative of a Western government, company or academic institution, as an enemy; and by criminals who are simply looking for a quick score. In short, you are not safe simply because you are Canadian. In the eyes of those who wish Canada harm, you are a legitimate target. Try to be a hard target by avoiding being predictable and accessible. Maintain good situational awareness.

You ARE worthy of targeting. As Canadians, we often assume our citizenship makes us less of a target. Similarly, by booking hotel accommodations in a 'safe' area, we assume we are less likely to be the victim of crime. These determinations are up to the threat actors, not the traveller. Always try to maintain a low profile when travelling. Do not wear clothing or other items with logos openly identifying you as a foreign representative. Your dress, discipline and body language are very important when travelling. Do not display wealth or anything that may increase your value as a target.

Do not overlook the threat posed by thieves. At the very least, briefcases, laptops, smartphones and the like are attractive to common criminals, as they are to foreign intelligence agencies. The result is the same: a security breach - one that could potentially harm you, the Canadian government, your company, academic institution and by extension Canada as a whole. Be suspicious of unsolicited offers of assistance and be aware of distractions or diversions that allow unknown individuals to control or funnel your movements.

VISA APPLICATIONS AND PREPARING FOR THE TRIP

The gathering of information by foreign entities may begin before you even book your flights and hotels. In some countries, information gathering on you begins well before you arrive. The information you provide on your visa application form could be used to assess your "worthiness" as a target, drawing a detailed initial profile of who you are as a person. If you are part of a high-level industry, academic or government delegation, assume you will receive consideration as a potential target.

In order to be successful on your trip, planning and preparation are key. A worthwhile practice is to complete at least 70% of your planning and preparation in Canada. Before you go anywhere, inform yourself about the general security and political situation in the country you are visiting. When you arrive in-country you will be ready to put your plan into action. The remaining 30% of your effort can be spent updating and verifying your situational awareness and familiarizing yourself with the country on arrival.

Visa applications have become more comprehensive with more questions than ever before. When filling out such applications, be truthful but do not volunteer more information than needed. Given the intrusive nature of the questions, all visa requirements should be explored prior to booking travel. For example, some countries will request passport numbers of family members, even if they are not travelling with you. Moreover, questions on the nature of your employment can be geared to acquiring very specific details. Be aware of the publicly available

information about you. Conduct an Internet search of your name and position in advance of your visa application to find out what can be found out about you on the Internet.

Be prepared to answer questions at the border. Before departure, ensure that you will be comfortable answering questions from the host country's customs officials about the reasons for your travel. This is especially important if you are travelling in a group, as any divergence between rationales could be used as a pretext for some kind of action on the part of local authorities.

What should you leave Canada with? Consider alternative means for transferring information you will need while travelling, especially that of a more sensitive nature, before you leave Canada.

Consult a designated security officer before leaving. In consultation with your company or department security officer, you may want to use a "disposable" telecommunication device while on travel. By disposable, we do not mean that the device is thrown away but rather that it contains no information when you leave and that, upon your return, it is completely wiped clean and the operating system is re-installed. You do not want to take abroad a device packed with e-mails, contacts and documents.

Contact lists. Leave behind any address books or lists of names and contact numbers not necessary for the trip.

Communications. Keep others informed of your whereabouts for your own personal safety and security. Leave emergency contact information with your supervisor and arrange regularly scheduled check-in calls or messages at home. **Registration of Canadians Abroad** is a free service that allows the Government of Canada to notify travellers in the event of an emergency abroad (for example, natural disasters or civil unrest) or a personal emergency at home.

Travel light. Do not saddle yourself with excess baggage. It will attract attention, curtail your mobility and mean you have more to protect.

AT THE AIRPORT

What to do at any airport. Apart from following normal security procedures at airports, be vigilant and in a position to observe or watch for any type of suspicious activity – from fellow passengers, flight crews, etc.

Airline or border control agents. Assume that any detail given to airline or border control agents will be collected by the host country. **It may also be shared with other countries**. Keep your passport in your bag or pocket until you arrive at the border control.

Do not advertise your identity. Always conceal your bag tags. In fact, you may want to put the identifying bag tags in your checked bags and use some other type of identifier, such as a ribbon, on the handle.

Luggage. Do not leave belongings unattended. Assume your checked luggage will be searched in transit. Do not agree to carry items for other parties unless you are certain of their nature or contents. No one should get control of your suitcases or bags. Maintain physical or visual control of your luggage at all times while in the airport. Baggage claim areas are often where criminals will target their victims. Be especially vigilant in these areas.

POINTS OF ENTRY AND BIOMETRICS

Covert and overt means of targeting. Should you be identified as a potential target through the visa application process, the host intelligence agency may undertake covert or overt actions against you to further their information collection efforts.

Surveillance. Assume that in many countries, you will be subject to physical surveillance. A country-specific briefing and conducting your own research prior to departure will assist in broadening awareness on this issue. Always maintain a healthy level of awareness.

A secondary search could be used as a pretext to seize or copy your files. One of these overt methods can occur right at the Point of Entry – usually an airport – where you can be selected for a secondary inspection by the local Customs Service. During this inspection, your belongings may be subject to scrutiny, copied and/or seized, including whatever documents you may be carrying on your person, in your laptop, your tablet, and your smartphone.

A secondary search could indicate hostile interest. It could also simply mean that you triggered one of the many tripwires used to select passengers for secondary inspections. In either case, you should always be ready to handle a secondary inspection with prepared responses to explain purpose of your visit as well as being able to account for your belongings and so on. You should let your superior or delegation head know you have been selected for a secondary inspection.

Be prepared to invoke your right to a consular visit. Should the questioning during a secondary search become inappropriate or lead to your detention, call the Canadian Embassy, High Commission or Consulate, as you are entitled to Consular Access. When communicating with consular officials, keep your description of events to a minimum as somebody may be listening. In countries that are party to the Vienna Convention on Consular Relations, the arresting authorities are obliged to advise you of your right to access consular representation and to arrange for this access. They are not required to inform a Canadian government office of your detention or arrest unless you specifically ask them to do so.

If you are a dual citizen and travelling in the other country where you hold citizenship, local authorities may refuse to grant your access to Canadian consular services, thereby preventing Canada consular officers from providing you with those services.

Biometrics are increasingly being used at points of entry, the purpose of which is to catch criminals and terrorists who often travel using a multitude of identities and documents. At the same time, extensive information is being collected – information that could be used by a hostile intelligence service. This is especially true for individuals who travel to a given country, at different times, for both business and personal reasons. In these instances, the host country already knows who you are and what you do. Again, this can be very problematic if you occupy a sensitive position. Some biometric techniques include face recognition, iris scan and fingerprinting. In some countries, biometrics are taken covertly via closed

circuit television and cameras (CCTV). Also, a number of countries **share the biometric information they collect with neighbouring countries.** It is possible that this information is readily available in a country where you have never travelled.

ELICITATION, CULTIVATION AND OTHER TRAPS

Why would someone be interested in you? Foreign governments try to collect intelligence to advance their own foreign policy, security and economic interests. As someone representing a government organization, Canadian business or academic institution, your access to classified government or privileged private sector information and academic research makes you an attractive target for foreign intelligence services and other threat actors.

Contacts. Assume that any meetings you have abroad with personal contacts will come to the attention of the foreign government, even if they occur before or after the period of official meetings. Also assume that,depending on the relationship between your contact and the government, your contacts abroad will be interviewed before your arrival or after your visit.

Criminals may be interested in your information, especially if it relates to law enforcement. If your work is law enforcement-related, the information you hold or have potential access to could be of great value to criminal organizations interested in knowing if there are any investigations targeting them and if there are any "leaks" within their organizations.

Secrets can appear mundane. Those foreign intelligence agencies and other threat actors targeting Canada and Canadians are not solely after prized information – such as a blueprint to a new fighter jet or sensitive industry research about a new product or service – but information that, to the Canadian person or institution holding this information or knowledge,

appears unremarkable. Items such as an organizational chart may not appear to be of value but could be considered a key requirement for a hostile intelligence service.

They may be interested in gaining indirect access to an allied country or non-Canadian business. Foreign intelligence agencies may also be interested in the information and access they could obtain via Canada's membership in organizations as diverse as the North Atlantic Treaty Organization (NATO), the G7 and G20, the Commonwealth, la Francophonie, the Organization of American States (OAS), the Asia-Pacific Economic Cooperation (APEC), the Organisation for Economic Cooperation and Development (OECD), the United Nations (UN), the World Trade Organization (WTO) as well as any one of hundreds of business or professional organizations.

Gaining access to advanced American technologies. Canada occupies a unique strategic position as a trusted ally of the United States, which gives privileged access to advanced American technologies few others can legitimately procure. When travelling abroad, Canadian researchers or government officials may be seen as potential targets for access to American institutions or research data.

Canada: a source of technological advances and intellectual property. Canada also participates in a system of military and strategic partnerships, and possesses a wealth of natural resources and human talent which continue to generate technological advances. These technologies

are coveted by countries interested in developing their own technological and commercial opportunities while avoiding the associated research and development costs. The loss of such information diminishes Canada's competitive advantage and amounts to a transfer of wealth from Canada to another country.

How does the gathering of information happen?

Below are some of the most common methods foreign intelligence agencies employ to collect information.

Elicitation. This is a technique used by foreign agents whereby they engage you in what appears to be harmless or random conversation but the aim is subtly to extract information about yourself, your work and colleagues. Warning signs are when someone:

- **Appeals to your ego by flattering you;**
- **Emphasizes mutual interests and suggests "getting together" at a future date to pursue the mutual interest;**
- **Uses false statements to get you to correct them with the information you have access to;**
- **Volunteers information – the "give to get" principle at work. They share some form of sensitive information with you in the hopes you will return the favour;**

- **Leads you to believe they are very knowledgeable about your area of expertise. If they are an intelligence officer, that knowledge is likely limited and cursory, but just enough to bluff their way through a conversation.**

Cultivation. Well-orchestrated approaches by hostile intelligence services begin with a period of "cultivation". A relationship is established between the representative of an intelligence service (whose true identity is unknown) and the unsuspecting person being recruited. You should be vigilant and monitor the progress of associations, particularly new relationships and those with foreign nationals. Always be mindful of discussions regarding your work, even if seemingly benign.

Unwittingly volunteering information. Never talk shop or volunteer information in front of taxi drivers, waiters and bartenders, who could be intelligence officers or informants. Every little bit of information can be useful to a competitor.

The "Mosaic Effect". Some intelligence agencies will obtain one piece of information from you and build on that with other pieces of information acquired from your colleagues or that you unwittingly offered to other sources who are working together. You may not think that you have offered any desired information, though when pieced together the result can be quite valuable (thus creating the "mosaic effect").

Entrapment and blackmail. Sexual entrapment, colloquially known as the "honey trap", refers to the use of an attractive individual – informed

by your sexual identity and preferences – to seduce you and get you in a compromising position or one where you could be blackmailed. Honey traps often involve the clandestine recording of an intimate encounter. These recordings are either used to blackmail or publicly embarrass the victim. Foreign governments are known to employ this tactic, and travellers should be aware of the potential hazards of accepting offers of companionship while travelling. There are also reports of individuals who have suspected they were drugged and who awoke to find that their hotel room had been searched, smartphone stolen and secret business documents missing. It is also important to know the laws regarding sexual activity in the country or countries you are visiting, specifically regarding the age of consent and sexual orientation.

Covert methods including intrusions. Hostile actors may decide to conduct an intrusion operation against you. This would entail breaking into your hotel room in order to steal or copy sensitive documents in either hard or digital form. Though you may not notice that someone has surreptitiously entered your room, some travellers have returned to their rooms to find individuals searching their belongings or conducting unnecessary maintenance activities. Others have reported laptop computers showing signs of unauthorized usage or actual damage, packages having been opened and resealed or left open, locks on briefcases and suitcases missing or showing signs of forced entry.

≥ **Intrusions may be conducted by the host government, a foreign intelligence service of another country or foreign business operatives.**

- **Intrusions are frequently accomplished with the cooperation of the hotel staff.**
- **Several countries, and possibly foreign companies, have the ability to overcome commercial computer intrusion-protection software and hardware.**
- **If you report evidence of intrusion to the hotel management or local authorities, they may deliberately want to mislead you by passing off the operation as a criminal activity.**

Even if there are no obvious signs of intrusion, it does not mean that an event has not occurred in a discreet fashion.

Eavesdropping. Assume that conversations can be monitored in public places and in public transport. Eavesdropping activities can range from the strategic positioning of an unobtrusive bystander, to the use of concealed sophisticated audio and visual devices.

- **Use discretion at all times.**
- **Beware of eavesdropping at social settings where attendees feel secure and are more likely to talk about themselves and their work.**
- **Vulnerable venues include public and host-provided transportation, restaurants, bars, meeting facility restrooms, hotel rooms and telephones.**
- **Concealed devices are cost efficient, low risk, and can be used in conjunction with overt devices such as traffic, security, and pedestrian-monitoring cameras.**

Information gathering through open sources. Open source research goes beyond simply conducting an internet search of your name and address. It entails scouring every possible source of publicly available information – such as trade publications, academic journals, websites, social media profiles, public registrars, etc. – that exists on you, your family and work. You would be surprised how much open source information is accessible to someone who knows how and where to look. Even if you think you have a low profile and have not left a digital trace behind, some information related to you, your family and friends is freely available. The gathering of such information serves to build a profile of who you are, and where you might be most easily approached either overtly or covertly. A personal, financial and professional profile of you or your business can be constructed by someone willing to invest the effort. *Remember, information about you on the Internet is almost certainly there forever.*

Social networks are great, except that now everybody knows your name and possibly what you look like. You might not have an account on social networks such as Facebook, Twitter and LinkedIn but a member of your family, a friend or a co-worker might, and they may have inadvertently posted information related to you. Remind your family and friends to exercise discretion when posting information about you. Even if you use enhanced security and privacy settings on your social media, all information posted online should be considered publicly available.

Even garbage is information. All types of information can be gathered by rummaging through your trash. Be cognizant of what you throw out, especially material of a sensitive nature. Do not throw away business or personal notes in the garbage of your hotel room or meeting rooms.

Be cautious of accepting gifts. Be wary of gifts, especially electronic ones that can plug into your computer – USB keys, cameras, digital picture frames, etc. These items could be infected with malware and other viruses that could give someone remote access to your computer and network. Never plug in a device of unknown origin without proper virus scanning. Consult with your IT resource team or company security procedures prior to using any digital gifts.

The private sector is involved in this type of activity as well. There are private companies that are in the business of packaging open source information on people and companies for a price. These companies may also use more intrusive methods to gather information.

INTERCEPTION OF COMMUNICATIONS

Intercepting your communications. Wireless communications can be monitored in any country. Your institution may have guidance regarding the use of wireless services when travelling, such as the use of VPNs. It is also important to check **travel.gc.ca** to be aware of the level of security recommended for the geographic region you are travelling to. Local authorities will have the ability to access telecommunication networks, which means that they can access information on your devices such as call logs, contact lists, documents, messages and can even listen to and record phone calls. Consider travelling with a phone that only has necessary information for your trip.

Wireless vulnerabilities. The devices you carry for the most part can connect to the Internet or be accessed wirelessly. This makes them vulnerable to cyber-attacks and hacking. Attackers can access your hard drive and everything on it; can activate your microphone or camera without your knowing; can log every key you hit and every number you enter, etc. These vulnerabilities can persist along after you return home – be vigilant and report suspicious activities.

Use good electronic hygiene: Do not let anyone plug an external device into any of your equipment.

There should be no reason for authorities to remove your equipment out of sight at airports, security checks and hotels. Should this happen, even for a very brief period of time, assume that the equipment has been compromised.

All types of electronic communication are vulnerable. Any type of communications (e.g. voice calls, SMS, instant messaging, web browsing, social media use, etc.) can be intercepted. It is worth noting that a landline, although by no means secure, is normally more difficult to intercept than a mobile phone. The use of public pay phones is a good alternative but should not be considered secure communication.

Voice intercepts via the Telephone Service Provider (TSP). Authorities can monitor your telephone conversations. Not only can they gain information directly from your conversation, but also from the numbers you dial (telephone tolls). Looking at call patterns not only helps build a personal profile of someone, but a larger organizational one as well.

Data intercepts via the Internet Service Provider (ISP). Data can be intercepted via technical means by the Internet Service Provider. Be it a smartphone, a tablet, desktop or laptop, these communications can all be intercepted and eventually "taken over".

Your car as a listening device. People often feel they can carry on work-related conversations in cars they rent while on business without giving any thought to the potential for eavesdropping or tracking through devices paired to the vehicle or through manipulation of technologies embedded in the vehicles by the manufacturer.

Identity fraud and phishing. Another reason to safeguard your information while travelling is that it could be used by an attacker to impersonate you and send targeted emails loaded with malicious software to employees in your organization, or further afield, in the hopes of tricking recipients into opening the e-mail and attachments. This would then automatically infect their computers or networks with the malicious software. When attending conferences or training abroad, be aware that attackers can use attendance lists to specifically target you with well-crafted emails – think before you click!

Storage. Do not hand in mobile devices or smartphones at reception or security desks. Leave them secured at the Embassy, High Commission or Consulate if travelling for government purposes or any other means if travelling for business.

Post travel. If you brought any corporate hardware or software with you while travelling, be sure to have it examined upon your return by your IT department or technical officer for any signs of intrusion or compromise before using it at your work site.

MOBILE AND SMARTPHONES

Voice Communications Interception

Eavesdropping on wireless communications is always a concern. There is inherently very little protection afforded to the wireless voice call unless expensive third party products are used for encryption. Again, authorities in the host country have access to these cellular networks.

Data Transmission Interception

There is a particular concern that some foreign government infrastructures can isolate, decrypt and store certain data communications which are often assumed to be protected with proprietary encryption software. Assume your data transmissions are being intercepted.

Live Microphones in Secure Areas – Mobile phones

Bringing mobile phones into security zones presents the risk of (unintentional) live microphone transmissions. All mobile phones should be kept outside of secure areas.

Tracking

Surreptitious tracking of the whereabouts and movements of the user is a particular concern. Smartphones provide a dedicated adversary the means to track the movements of the targeted device and its users by intercepting or acquiring GPS information transmitted or stored on the phone. Your phone has a unique signature that, once brought to the attention of an attacker, can be followed anywhere in the world.

Bluetooth and Wi-Fi Wireless

Other wireless networks available with most smartphones such as Bluetooth and Wi-Fi introduce additional interception and data loss vulnerabilities that can be exploited by an attacker. Public Wi-Fi is by its very name not private!

Lost or Stolen Smartphones and/or laptops

More so than the replacement cost, the greatest concern of a lost or stolen device is unauthorized access to the data it contains. Passwords, encryption, time lock-out and remote wipe can be used to counter this risk.

Never leave a smartphone or laptop unattended; compromise takes mere seconds.

LAPTOPS AND TABLETS

Personal information. Do not keep any personally identifiable information on your laptop. Certain software can find files on your hard drive that may contain personally identifiable information. Consider leaving personal devices at home as they are as vulnerable as corporate devices and not as easily replaced.

Sensitive files. Remove them from the hard drive and put them on a USB flash drive if necessary. To ensure that the files are actually deleted from the laptop's hard drive, use a proven media sanitizing software tool. Keep the USB flash drive on your person. Encrypt the files on the removable media and keep the password separate from the media.

Cloud storage. Be aware that certain web browsers and applications store passwords. Should these passwords be compromised, the shared nature of cloud computing makes all stored information unprotected and accessible. This also means that other accounts or databases that can be accessed with those passwords are now vulnerable. If possible, limit your interaction with cloud drives while travelling by transferring necessary documents and research to a secure and clean device. If access to cloud storage is necessary, be sure to only do so on personal and secure devices.

Battery. Make sure the laptop battery is charged before you go to the airport; expect to prove that the laptop is functioning correctly. Ensure an innocuous start-up screen is in place.

Airport security. Do not send your laptop through the airport X-ray conveyor belt until it is your turn to walk through the metal detector. This will ensure you will be able to pick it up promptly when it comes out the other end and prevent anyone from walking away with it. Never check laptop computers as checked luggage. **Keep your laptop in sight at all times. It is a high target item.**

USB FLASH DRIVES (thumb drives)

These devices can be very small and therefore more easily lost, stolen or hidden.

Popularity. The popularity of thumb drives makes them a vehicle for cyber criminals to spread malware. They have even been targeted at the production phase, while they are being created, so a brand new product could potentially be already infected. You may wish to exercise caution when considering their use.

Running software code. A computer can run software code from a USB the moment it is plugged in. Software has been released that can make a USB thumb drive auto-execute when inserted into an operating system, tricking the operating system into treating it as a CD, and then dropping malicious software into it. Issues with data loss, bandwidth consumption, network performance, software licensing and productivity are likely signs that devices have been manipulated.

Other risks. Getting individuals to divulge confidential and personal information as part of a larger fraud, information gathering or system access scheme is made easy when a perpetrator, for example, drops several flash drives somewhere close to the intended target (e.g. a hotel), and waits for an unsuspecting victim to insert it into their system, giving the perpetrator access for further manipulation.

AT YOUR DESTINATION

Hotels

Hotel staff. Only provide the information necessary to conduct your transactions. Use only the most generic information possible as your employer/institution if asked; there is no need to volunteer information. Have copies of your passport ready instead of relinquishing your passport. Always try to keep positive control of your passport.

Hotel phones and computers. Beware of the use of hotel phones and computers as authorities have access to these networks.

Answer with hello. You should answer the room telephone with a simple "hello." Again, do not volunteer information; this call could be used by someone to confirm that you are indeed in a given room.

Hotel safes and securing classified documents. Do not use the hotel safe for classified or sensitive material. Do not leave classified or sensitive documents or equipment unattended in hotel rooms. Classified government material is best kept in secure storage at the Embassy, High Commission or Consulate.

Use encryption and Virtual Private Networks if you must work using non-secure networks. When on official travel, never use an open (i.e. hotel, coffee shop, etc.) network to conduct work as these are easily intercepted. Prior to your departure, engage a designated security or IT

officer at your department, company or institution to discuss various VPN and or encryption methods available to you.

Never use an open or hotel network for work. Avoid using a "free" and or unknown Wi-Fi connection as you may be accessing a network that is controlled by an intelligence agency or, more likely, a criminal. Wi-Fi is available in many locations such as airports, coffee shops and train stations. These systems are very vulnerable to abuse by hackers, competitors or foreign intelligence services. As such, it is best to avoid such systems for discussions or exchanges of sensitive or proprietary information. Ensure encryption software or features of your wireless local area network (WLAN) are installed to avoid compromise. Factory installed encryption should be changed.

Do not advertise where you are staying. If someone has your room number, it makes it easier for them to target you whether they are an intelligence officer or a criminal. This is especially important for women. Please consult **travel.gc.ca** for more specific information related to maintaining your personal safety. Always meet guests in the lobby and never in your room for security reasons.

Pretend that someone is always in your room. Leaving on a TV or radio, along with the lights, can give the impression that someone is in the room. Criminals are opportunists, and will not likely take a chance on your room if they believe someone is in there. Closing the curtains keeps prying eyes out. Leave the "Do Not Disturb" sign on your door.

Never open your door to anyone without first verifying the identity of the person with the front lobby at all times. Always confirm unannounced or uninvited guests with the front desk.

Alternate exit routes. Always look for alternative exits in case of an emergency. In some emergencies, getting out quickly is essential - you may not have time to wait. Ensure that your room is **not** accessible at street level (below the third floor) and **is** accessible to first responders §(below the seventh floor where fire ladders can reach). Always have an emergency bag ready containing items such as: flashlight, passport, money, credit cards, medications, glasses, water and power bars etc.)

Do not relinquish control over your key(s). This is a simple safety and security precaution.

General

Travel with disposable devices if possible. Consider traveling with clean or "disposable" devices. Even if they aren't hacked into or otherwise tampered with, they could be stolen. Laptops, smartphones, and USB sticks – these are all mobile devices that are essential for your communications with your colleagues but they also involve risk.

- **They should not be used by anyone other than the employee.**
- **They should not be used to connect to unprotected wireless devices.**
- **They should not have unauthorized software installed on them.**

Physical access to these devices allows for the extraction of data and / or the compromise of systems in support of information gathering efforts.

Consult with your IT Branch. Make sure that whatever media device you take has the latest anti-virus, encryption, firewall and program patches installed. Remember, your computer and smartphone can be used as a gateway into your corporate network and from there to your most priceless information.

The threat of kidnapping is real. The terrorist threat of kidnapping in some countries is significant, as many groups are dependent on this type of criminal activity in order to fund their operations. In order to make yourself less of a target, you should look for signs of hostile reconnaissance, vary your daily routines and change the routes you take to and from your hotel and place of work. Terrorists use the same methods as intelligence officers in order to obtain information. They will elicit information as well as gather it through other types of collection means. Situational awareness is your best defense. Routine and complacency are the two most common causes of safety and security issues.

Do not talk shop in unsecure locations. Assume your hotel room is bugged and that the list of telephone calls made from your hotel will be collected by the host country. Do not "talk shop" in taxis, public transportation and in public. Moreover the taxi may be outfitted with a camera and other audio-visual equipment. This equipment may be found in all taxis for driver safety reasons, but this kind of technology can have dual-uses.

Taxis. Try to arrange transportation in advance. Have a trusted person pick you up. If this is not possible, use hotel courtesy shuttles when available or research the name of reputable taxi companies. Always negotiate the taxi fare prior to departing, never share a taxi with a stranger, do not travel in taxis that are unmarked or do not have an official license prominently displayed. Always sit in the rear diagonally opposite the taxi driver. This allows you to see the hands of the taxi driver and is the most direct and safe route out of the taxi in an emergency (on the sidewalk instead of into traffic.)

Your personal data is stored on many devices. Electronics primarily refer to your phone, and laptop, however even key fobs and smart watches can be a target as they have personal data such as pictures, schedules and health information on them. These can prove to be treasure troves for intelligence agencies, business competitors, academic institutions as well as profit generators for criminals. Avoid being distracted by your devices. Continue to pay attention to your environment while using them.

Avoid high crime areas. High crime areas are not places you should normally visit. Should you need to enter those areas, appropriate measures should be taken – such as timed physical or telephone check-ins. Note that locals will immediately detect that you are from outside the area. In case of a robbery, have a "throw away wallet or purse" ready to give away. A wallet with fake credit cards and local or American money are enough to satisfy a thief and allow you to walk away from potential harm.

Criminals also seek to profit from available information. Criminals are opportunistic. They wait for you to make a mistake so they can exploit it. Their task is made easier if you volunteer information about yourself, your comings and goings, or your possessions to people you do not know. For instance, do not talk about how to use a hotel safe to store your laptop and other valuables in a taxi and then pay for it with a credit card or make mention of your name. This type of information can prove very useful to criminals, and they too are known to pay for information.

Do not attract notice. Be discreet about who you are, what you do and what type of valuables you are carrying.

Do not travel alone if you can. Traveling in a group is usually more safe. Criminals, like other types of predators, are less likely to target a group than a lone individual. However, the group should also seek to be discreet to avoid attracting unwanted attention.

Medication and Medical facilities. Always travel with enough prescribed medication (in their original containers) to last you for the time you are away and with a reserve supply in case your return is delayed. Make sure that you verify the legality of this medication in the country you are travelling. Additionally, you should be aware of what type of medical facilities, local emergency care, means of payment, standard of case and capabilities that are available in the country where you are travelling.

Money. Always arrive with enough local currency or enough money that will work in the country within which you are travelling to get you through the first 24 hours.

Threat Response. Stay calm when confronted, assess your options, and disengage or remove yourself from the situation if possible. Attract attention to yourself by yelling, screaming, or making any kind of noise. Try to create distance between you and your aggressor using furniture or vehicles. When travelling, having a whistle handy can help you attract attention in almost any environment.

Remember – Have a plan and a back-up plan.

Travel Smart

Get Travel insurance
Register at Travel.gc.ca
In case of emergency abroad – collect call 1-613-996-8886
sos@international.gc.ca