Travel security guide for university researchers and staff

Table of Contents

The current environment

International travel for research is frequent and beneficial – not only to individual researchers but to the broader pursuit of knowledge through academic research and collaboration. Canada's researchers and universities are a strategic resource to Canada and advance our place in the world economically, politically and socially.

In an era of changing geopolitical realities, Canadian researchers travelling abroad may be targeted for their access to certain sources of information as foreign governments and businesses place a high priority on acquiring information related to research and innovation. This guide is not meant to cover general travel safety, but rather focuses on risks created due to the intersection of geopolitical dynamics and research areas. **This guide describes the nature of economic and geopolitically motivated threats to you or your research, provides basic steps you can take to mitigate risk and suggests actions you can take in case of incidents.**

It cannot be understated: international travel for research is a good thing! The information provided in this guide is meant to ensure rl.jn6 (esear)30.2(cher)9.410.mhkou a (.u

1. Five reasons Canadian researchers may be of interest and at risk

For researchers, the pursuit of knowledge and academic excellence drive them to collaborate across Canada and across borders. While travel is an integral part of collaboration, there are five factors that may put a Canadian researcher more at risk of being a target for theft and espionage while abroad.

1. **Your research:** While all research could be of interest to malicious actors, your research may be of more interest if it relates to:
   a. Canadian or foreign security practices, like military practices or law enforcement.
   b. Canadian or foreign commercial activities or intellectual property development.
   c. STEM and emerging technology fields.
   d. Health or other personal data (e.g. human genomics, interviews with key figures, etc.).
   e. Politically sensitive contexts (either domestic or international).
2. **Your access to indirect partners:** Information about fellow research partners, your institution, private industry partners and the Canadian government[1] can be used by malicious actors to target them.
3. **Your access to the United States:** Given the close relationship between Canada and the United States and the mobility that many researchers enjoy between Canadian and U.S. institutions, Canadian researchers occupy a unique strategic position. In some cases, Canadian researchers have privileged access to advanced U.S. technologies, which few others can legitimately procure. As a result, when travelling abroad, Canadian researchers may be seen as soft targets for access to U.S. institutions or research data.
4. **Where you travel to:** As a Canadian researcher, you have the privilege of being able to travel to many places around the world. While many of these countries are safe, some countries are riskier and the level of risk can change as global dynamics evolve.
5. **Who you travel with:** Researchers often have the opportunity to travel as part of delegations made up of other researchers, university senior leadership, business leaders or government officials. As part of a high-profile group, you may be more at risk of drawing attention from foreign governments or other actors.

Mitigation tips

Assess the level of risk associated with your travel due to: your area of research, indirect partners or access to U.S. research, particularly in sensitive areas.

Discuss any concerns with appropriate resource people within your university (supervisor, IT department, travel office).

Consult the Government of Canada's travel advisory website and take relevant precautions associated with

1 Additionally, any relationship that you or your research has with organizations such 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 Organization for Economic Cooperation and Development (OECD), the United Nations (UN) and the World Trade Organisation (WTO) may be of value.

Mitigation tips

Mitigation tips

Be vigilant and monitor the progress of associations, particularly new relationships and connections with foreign nationals. Always be heedful of discussions regarding your work, even if seemingly benign.

Refrain from talking about sensitive parts of your research in public places or with contacts you have just met.

Refrain from offers of companionship while travelling and be aware of risks associated with sexual activity (eg. age of consent and sexual orientation) in the country where you are travelling.

If you are a victim of elicitation, cultivation or entrapment or suspect that someone is trying to victimize you, notify the Canadian consulate in your area immediately and file a report with the appropriate person at your institution, either immediately or upon return. In case of emergency when abroad, contact the Government of Canada collect at: 1-613-996-8885 or sos@international.gc.ca.

Mitigation tips

Consult with your IT department before you travel. Make sure all electronics have the latest anti-virus, encryption, firewall and program patches. Use burner or travel specific devices. Follow guidance for use of Virtual Private Networks and other safeguards for accessing the Internet while away.

Before you travel, carefully consider what data you need. Bring the minimum.

Encrypt and transfer data onto a separate external storage device and keep it with you at all times while travelling. Keep data passwords separate from the media.

If your devices are out of your sight at any time during travel, assume that the equipment has been compromised.

Appendix A – Travel security checklist for university researchers

Before you travel:

Cyber intrusion

Do not let your devices out of your sight at any time during your travel. If this happens, assume that the equipment has been compromised.

Do not plug an unknown device, including USB keys, cameras or digital picture frames, into any of your equipment.

- Should you find it necessary to plug an external device into your equipment for presentation purposes at a conference, you should consider that your device has been compromised.

If possible, do not access cloud data storage sources while travelling.

- If access to cloud storage is necessary, be sure to only do so on personal and secure devices.

If your device is lost or stolen, notify your IT department immediately.

When you get back:

Upon your return home, take appropriate steps to clean your hard drive or other devices especially if your think your device may have been compromised. Have all external devices scanned for viruses, including gifts or conference swag.