Traveler's Safety Handbook

September 2025

UNIVERSITY OF TORONTO

DEFY GRAVITY

Table of Contents

Introduction

International travel plays a vital role in advancing research and enabling groundbreaking collaborations. As research opportunities expand, so too does the risk of unauthorized access to research, networks and devices.

Recent attempts by foreign governments and businesses to illegally or covertly obtain innovative research make it essential for even the most seasoned travelers to take proactive measures in protecting their intellectual property and guard against digital breaches while traveling.

As the University of Toronto (U of T) strengthens its international partnerships, it must be accompanied by strong awareness and practical steps to protect the elements that make its research world-class. Beyond your typical travel guide, this handbook serves as a reference for U of T researchers to travel securely, confidently and responsibly.

Protecting Yourself

Your safety and wellbeing always come first. Being aware of how your work, data and online presence may attract attention abroad is key to protecting yourself.

To mitigate personal safety risks while traveling, it is important to be aware of your environment, limit the information shared and remain vigilant.

Pre-Travel

- Check official guidance. Review the Government of Canada's travel advisories for up-to-date health, safety and security information at your destination.
- Use your resources. If you are a student, register with International SOS through U of T for global medical, security and travel assistance.
- Know your topic. Think about whether your research area could attract special interest abroad, especially if it touches on emerging technology, security or high value intellectual property.
- Pack light. Bring only the data, files or devices you truly need. Leave unpublished or highly sensitive research at home.
- Use travel-ready devices. If you have one, use a dedicated travel laptop or phone that you can wipe before and after your trip to avoid malware transfer and research theft.
- Plan ahead. Pre-load your presentations and materials so you won't need regular cloud access abroad.
- Avoid carrying sensitive physical documents such as research notes, contracts or internal project timelines, as these may be copied or stolen.
- Check your online footprint. Take a moment to review what information about your research or affiliations is visible on social media and adjust privacy settings accordingly.
- Limit sharing on the go. Avoid posting travel plans or research updates while abroad. Consider making your social media profiles private while traveling.

During Travel

- Be intentional in conversations. Take your time when meeting new contacts, especially if they ask detailed questions about your work, partners or future plans.
- Treat all details as valuable. Even small pieces of information, meeting lists, internal emails and travel schedules, can be used nefariously by determined individuals.
- Use trusted devices. Avoid using public computers or hotel business centres for research-related communications.
- Pause before you share. A quick moment to consider whether this information needs to be shared immediately can help avoid oversharing.
- Recognize persuasion tactics. Be aware of approaches like unexpected flattery, too-good-to-be-true offers or surprise collaboration invitations as these can sometimes mask attempts to access you or your research.
- Watch for unusual opportunities. Some recruitment programs or “prestigious partnerships” are designed to gather valuable research. Take time to check the details and verify legitimacy.

Case Study

At a conference, a researcher was offered an all-expenses-paid lab exchange. After looking closer, they realized the funding came with conditions that could have transferred their ongoing research and/or intellectual property. They declined the offer. Taking time to read the fine print and conduct due diligence checks on the partner resulted in protecting their research.

Protecting Research

Your discoveries and ideas are powerful, and they can attract attention from governments or organizations looking for shortcuts to innovation. Good habits can help protect your research and make sure your work stays in the right hands.

When you're traveling, you may be subject to different rules and laws. In some places, local authorities can request access to your devices and information. Planning ahead keeps you in control.

Partnership Due Diligence

- Gather the facts. Look into partners, hosts and conferences ahead of time.
- Build smart agreements. Create clear expectations to your research contracts, presentations and engagements to safeguard your research and your team.
- Know if your research is sensitive. Topics connected to military, security, dual-use or cutting-edge technology are especially valuable to others. Be prepared to handle them with extra care.
- Share only what's published/publicly available. Keep details about unpublished research or ideas within your trusted teams.

Laws and Regulations

- Consult with U of T's Export Control and Controlled Goods Program. Some data or software may fall under Canadian export regulations. Confirm if you need to remove anything before you leave.
- Know your limits abroad. Lectures or presentations can also count as exports.
- Review Canada's Export Control List before you go.
- Respect sanctions. Be aware of any country-specific restrictions that apply to you as a Canadian researcher.
- Keep your research with you. Bring only what's essential and always ask if you really need to bring sensitive research on your trip. Some countries may inspect or copy your devices at the border, conferences or hotels.

Case Study

At an international conference, a researcher briefly left a laptop unattended while speaking with colleagues at another table. When the device went missing, it was assumed to have been stolen, only to reappear on the same table several hours later. Subtle damage to the screws revealed that the hardware had been accessed, exposing sensitive research, prototypes and future project plans. Soon after, unauthorized elements of the work appeared at another institution.

Protecting Networks

Your professional network, colleagues, students, partners and institution rely on you to handle information carefully. Good habits while traveling help keep your connections strong and protected.

Researchers play a key role in safeguarding their research but also their broader network of students, colleagues, partners and institutions.

Protecting U of T

- Share thoughtfully. Stay mindful about what you share abroad, whether in formal presentations or casual chats. Focus on what's necessary and avoid details about internal operations or strategic plans.
- Protect your connections. Remember, you're not just protecting your own research, you're also safeguarding your students, partners and collaborators who trust you with their information.
- Understand the value. Canada's leadership in advanced research makes U of T an attractive partner. Staying aware helps maintain our competitive edge.
- Report concerns quickly. If you notice someone trying to gain access to your login details or research information in ways that feel suspicious, reach out to the Information Security Team.
- Use the support available. Keep up with U of T's information security guidance on safeguarding your data while traveling.
- Encourage your students and colleagues to take similar precautions when traveling.

Case Study

While traveling abroad, a researcher struck up a casual conversation with an individual curious about their work. As they shared about colleagues and departmental projects, it felt like ordinary small talk. Weeks later that same information was used to launch targeted phishing campaigns at their colleagues and students. Being mindful of what is shared helps protect both the research and those behind it.

Protecting Devices

Your devices are your lifeline for staying connected. With some thoughtful steps, you can use them confidently without putting sensitive information at risk.

Physical and remote access to your devices can be used to gain unauthorized access to your research, network and personal information. This makes it crucial for academics to secure their devices when traveling or sharing data abroad.

Crossing Borders

- Keep devices close. Carry your devices and chargers with you, and keep them powered down at border crossings to help protect your data.
- Print boarding passes to avoid turning your device on at customs or other inspection points.
- Be prepared. Some countries may request that you unlock your device or share passwords. Knowing this in advance helps you plan. If asked, try to keep your device in sight.
- Some countries mandate registration for border control, visas, financial services or government functions. If registration is needed, use the web version rather than downloading an application on your device for these tasks to limit access to your device.

Connectivity Best Practices

- Stay one step ahead. Update all software before you go, back up your important files and use web-based tools instead of downloading applications when you can.
- Stay in control. Disable auto-connect features for Wi-Fi, Bluetooth and location services. Power your device off fully once a day. These small steps can make a big difference.
- Assume communications transmitted while traveling can be intercepted. Understand the different ways your devices can be exploited, including phishing, malware, direct access and connecting to networks.
- Use security tools smartly. Encryption, multi-factor authentication (MFA) and virtual private networks (VPNs) are good practice. Note that some countries ban / restrict their use. Check the Wassenaar Arrangement for exemptions.

Avoid High-Risk Environments

- Avoid connecting to Bluetooth or Wi-Fi networks while traveling, even on secured networks. Wi-Fi services should only be used to hotspot your laptop from your cellphone data plan.
- Keep devices separate. Don't link personal devices to U of T provided ones. This protects both from unintended risks.
- Store passwords securely. Use a reputable password manager (your IT team can recommend options) and avoid reusing old passwords or remember me features.
- Plug in safely. Use only your own chargers and USB sticks, avoid unknown devices and use an AC adaptor over USB connections for charging.
- Be cautious with unfamiliar technology and content. Limit cloud access on public devices, avoid logging into unfamiliar equipment and stay alert when encountering unexpected emails, unknown links or unverified QR codes.
- Only download applications from trusted, official sources.

Upon Return

- Refresh your passwords. Change passwords for any accounts you accessed during your trip using a trusted device.
- Run a quick check. Do an antivirus scan for peace of mind.
- Reach out if needed. If something feels off, such as suspicious activity on your device or accounts, connect with U of T's Information Security Team.

Case Study

A researcher connected to what they thought was the hotel's Wi-Fi. Unbeknownst to them, the network was a malicious copy. Within moments, their credentials were stolen, leaving their critical research and their team's data exposed.

Additional Resources

Your well-being and security are important, and there are resources in place to help you navigate challenges you may encounter while traveling. Take advantage of these additional resources to ensure you have the support you need:

U of T Resources

- U of T Research Security: Safeguarding Research
- U of T Information Security
- U of T Report a Data Incident
- U of T Safety Abroad
- U of T International SOS
- U of T Export Control & Controlled Goods

External Resources

- Government of Canada - Safeguarding Your Research Portal
- Government of Canada Travel Advisories
- Government of Canada - Guide to Export Controls
- Government of Canada - Current Sanctions Imposed by Canada
- The Wassenaar Arrangement Participating Countries

Contact

For additional information on this booklet or assistance in conducting due diligence checks for faculty traveling to high-risk environments, please contact the Research Security Team at researchsecurity@utoronto.ca.