

Recommended Cybersecurity Practices for International Travel

Updated: March 2025

Purpose

In an era where digital threats are increasingly prevalent, safeguarding sensitive information and personal data becomes paramount, especially in unfamiliar and potentially less secure environments abroad. The purpose of this document is to offer practical recommendations and best practices to individuals and organizations to protect their digital assets against unauthorized access, data theft, and other cyber threats while travelling. These guidelines cover a range of topics including securing devices and communications, understanding and mitigating risks associated with public Wi-Fi networks, managing passwords and encryption, and being aware of different cybersecurity laws and regulations in foreign countries. The document aims to be a valuable resource for travelers seeking to balance the convenience of digital connectivity with the necessity of cybersecurity vigilance.

Scope

This guidance is intended for all York University staff, faculty, and researchers who travel internationally.

Key Points

When traveling internationally, particularly to higher-risk destinations, key risks include:

- Devices and data being lost or stolen.
- Devices and data being seized or confiscated.
- Insecure or monitored networks intercepting data or credentials.
- Hacking attempts facilitated by physical access to devices.

Key considerations to mitigate these risks include:

- Take only the minimum number of devices with you.
- Take only the minimum amount of data/files you need with you and no highly sensitive data.
- Review the detailed guidelines below for more information and services to assist.

Guidelines

1. Consider the risk factors for your travel to help determine the risk of your travel:
 - a. Sensitivity of data or research
 - b. Destination
 - c. Local laws and legal context
2. Be aware that expectations of privacy in many foreign countries are different than Canada and also are generally reduced in border/customs areas. For example, arbitrary search or seizure of electronic devices and their content may be legal. Consider taking the following cautionary steps to avoid compromise or loss of data:
 - a. Bring only the minimum amount of data and devices you need to have with you. It is preferable to bring no data and instead access it remotely via secure network connections as much as possible.
 - b. High sensitivity data should not be stored on or routinely accessed over the network by devices you are travelling with.
 - c. Consider using a “clean” loaner device instead of your normal phone/tablet and laptop, if available.

3. While using cloud services to access your data via your device is acceptable, keep the following in mind:
 - a. Only login to such services with your own devices, not by using any third-party devices or services.
 - b. To increase protection against interception of data, make use of York's VPN service when using any third-party network.
 - c. Connect only using a web browser on your devices, rather than using dedicated apps for services, to avoid cached/persistent connections.
4. Ensure all devices are encrypted.
5. Ensure all devices are hardened to York University endpoint security standards, including:
 - a. Use a strong password for device access.
 - b. Automatic security updates are enabled for software on the device.
 - c. Enterprise anti-malware software is in use and updated.
6. Consider suspending highly privileged access while travelling, such as IT or application administrator access that can provide a very high level of access to systems and data and should not be used remotely.
7. Avoid bringing portable data storage, such as USB drives, other sensitive hard copy documents, or equipment which can be easily stolen, lost, or seized by authorities.
8. Avoid connecting to free/open wi-fi services or unsecured networks; when in doubt use [York's VPN services](#)ⁱ to secure your connection.
9. Keep in mind that some online services (e.g. Google services, search engines, social media services, etc.) may be unavailable in some countries; use of York's VPN service may be a work-around to gain access in some cases.
10. Note that York's Duo 2FA service may be unavailable in certain restricted regions for regulatory reasons.ⁱⁱ (these currently include Cuba, Iran, North Korea, Sudan, Syria)
11. Consider using a 2FA hardware token while travelling instead of using your phone.
12. Avoid use of public USB charging stations as these can be maliciously used to compromise connected devices.
13. Do not attach a USB device provided to you by a third party with your equipment/laptop, as these can be used maliciously to compromise connected devices.
14. Consider forwarding your voicemail to email, to avoid the need to dial into your voicemail account and potentially revealing your passcode.
15. When returning after travel, change your passwords as a precaution, including your Passport York password.
16. Notify your IT support if any loss or theft of York devices occurs while traveling to ensure devices are disabled/deactivated remotely.
17. In the event there's been any suspicious activity or concern relating to devices or data while traveling, including inspection of devices or data by authorities, inform your IT support and Information Security for investigation.

ⁱ <https://vpn.yorku.ca>

ⁱⁱ Duo and OFAC restriction <https://help.duo.com/s/article/7544>

Additional References:

<https://www.canada.ca/content/dam/csis-scrs/documents/publications/Far From Home 2020.PDF>

<https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/how-can-you-protect-your-research-during-travel>

<https://www.cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088>