Destination: Anywhere Outside Canada

General Advice

Government of Canada's Travel Advice and Advisories page

Read the full guidance for the country you plan to visit: Ensure you have the information to make an informed decision about additional steps you may need to take before – or while – traveling.

Ensure your devices are encrypted, unless travelling to a country where encryption is restricted, then seek additional guidance from your local IT HelpDesk.

Store documents: Use OneDrive (web version) to store any travel documents you need or create while you're away.

Keep devices secure: Keep devices in sight and never leave them unattended.

Phone plan: Check with your phone provider to ensure your plan works in the countries you're visiting.

Password: If border officials ask for your password to unlock your device, then unlock it yourself if allowed. If they insist that you share your password, then provide it, but change your password immediately and inform UBC cybersecurity ASAP (security@ubc.ca).

Local laws: Be aware of local laws and regulations regarding content, use of VPNs or other apps on your devices.

Public Wi-Fi: Avoid using public Wi-Fi networks (e.g., transit hubs, restaurants, etc). Use UBC VPN if you must connect to public Wi-Fi.

Smartphone Considerations

Consider whether to borrow a loaner smartphone:
Check with your local IT HelpDesk

Disable biometric login: Use a passcode instead.

Wipe sensitive data: Remove any personal or confidential UBC-related files, photos or messages stored locally on your device.

Remove or sign-out of UBC apps: Uninstall or log out of FASMail, MS Teams, OneDrive, and Zoom before leaving. You can access these through a browser during travel if needed.

Avoid third-party messaging: Do not use unapproved apps for UBC business.

Use Eduroam: a secure, worldwide Wi-Fi service for the academic and research community, where permissible at partner institutions.

AutoConnect

Finder

Scan QR code for fast access to web-based applications

FASmail **MS Teams** **OneDrive** **Zoom**

Go Further

Take these steps to protect your non-UBC information:

Payment: Choose one credit card as your main payment method and monitor transactions closely. Report any fraud to your provider immediately. Have a backup card just in case.

Install a mobile payment platform if needed.

Remove or sign-out of personal apps: If concerned, remove apps including banking, social media, archived files, messages and photos. You can access these through a browser during travel if needed.

UBC Loaner Laptop (if needed)

Consider whether to borrow a loaner laptop:
Check with your local IT HelpDesk

Loaner laptops provided based on availability

Sign-in: Local account (no CWL login)

Do not keep any Personal Information on the laptop.

Software:

- *Microsoft Office:* Use web versions of Outlook, OneDrive, and Teams only (shortcuts on desktop).
- *Adobe Acrobat Reader* (pre-installed).
- *Acrobat Pro:* Available upon request.
- *Cisco AnyConnect:* Always use VPN whenever connected to Wi-Fi.
- *Web Browsers:* Firefox, Edge, and Chrome are available. Avoid logging in for syncing.

Additional Resources

Duo Mobile: Use a Duo token or the Duo app on your phone for secure UBC logins (even without internet). Scan QR code for help.

Privacy Matters @ UBC

UBC Finance Travel

SRS Int'l Travel Resources