CYBER TIPS WHILE TRAVELLING INTERNATIONALLY

Created: April 26, 2019

When you are travelling outside of Canada, there are different laws and requirements related to the use of technological devices and information. The expectation of privacy also varies dependent upon the country you are visiting.

Every country has its own expectations with respect to importing and exporting technology, information protection and privacy, legal and illegal content and freedom of speech. It is highly recommended that you make yourself aware of the local laws with respect to devices and data for the countries to which you are travelling.

Travelers should expect their devices (phones, laptops, IPads, etc.) to be openly examined and scrutinized by immigration officials and perhaps local law enforcement. You may be expected to give officials your password to unlock your devices or decrypt your data and failure to do so could result in your device being confiscated and possible detention or expulsion from the country.

BEFORE YOU GO

1) **No device can be protected at all times**. Your data or device may be lost, stolen or hacked while you are travelling, or it could be subject to seizure by authorities. Some suggestions to protect your data include:
    i) **Consider the data that is on your device** - Data and devices that are legal in Canada may be illegal in other countries. Check the Global Affairs Canada Travel Advice and Advisories for the country you will be travelling to (https://travel.gc.ca/destinations/). Choose the Laws and Culture tab. It will usually include a section on Imports/Exports that may indicate if a particular type of technology is illegal for import.
    ii) **Limit the amount of sensitive data that is stored on or accessible from your devices** and only take the data you need to access while travelling. Consider previously deleted information, as it is not automatically removed from a hard disk or storage environment. If you have questions regarding how to do this, please contact the IT Service Desk for assistance (email: itsupport@ucalgary.ca or phone 403-220-5555).
    iii) **If you are carrying departmental data on your device**, ensure that you have authorization to take the data off-site.
    iv) **Obtain a temporary email account**, where possible, to avoid your UCalgary or personal email history and content being copied or monitored.
    v) **Use unique passwords for accounts you will use during your travel**. When returning from travel, change the password as soon as possible after you return. Be aware that all of your passwords are at risk of being detected and recorded.
    vi) **Keep your data** on an encrypted/password protected USB device instead of your computer.
    vii) **Do not carry materials or information perceived to be linked to sensitive topics** in that country.
2) **Remove all apps that you don't need as you cross a border**. For example, remove your GMAIL account from your device (with all your email and contacts) prior to going through immigration and security. Once you have passed through those points, you can add it back on to your device. This will allow you to comply with any immigration or security requests to view your device information. You may also consider doing this with any banking information that you have on your device.
3) **Encrypt** sensitive information at all times and ensure that you understand the classification of data that you are carrying when you travel. If you are carrying University owned or research data, please see the Information Security Classification Standard at https://www.ucalgary.ca/policies/files/policies/im010-03-

security-standard_0.pdf If your data includes Level 3 (Confidential) or Level 4 (Restricted) information, please contact your IT partner prior to travelling with this information.

4) **If possible, travel with clean formatted loaner technology** rather than your day-to-day working devices. If you are a UCalgary employee using a University owned device, contact the IT Support Centre (email: itsupport@ucalgary.ca or phone 403-220-5555) for more information about loaner technology.
5) **Consider setting up additional security measures if it is necessary to connect to the University's network.** For example, you may want to move data you need while travelling to One Drive so you can access it securely on-line and avoid syncing data on any mobile device you may be carrying with you, or you could set up multi-factor authentication to increase webmail security. The IT Support Centre (email: itsupport@ucalgary.ca or phone 403-220-5555) can help you with additional security measures.
6) **Ensure your anti-malware software is running and up to date prior to the travel**.

WHILE ABROAD

1. **If you are asked by an immigration or other law enforcement official** to unlock or decrypt your device for their perusal, accede to their request in accordance with local legal requirements.
2. **Lock** all unattended technology to prevent unauthorized access.
3. **Do not leave your device** in an unattended area or vehicle.
4. **Exercise caution** before sending documents or information abroad that would fall under the coverage of that country's secrets laws.
5. **Be aware that public wireless networks are untrusted** and avoid using them if possible.
6. **Do not allow anyone else to use or access** your device.
7. **Avoid using public computer workstations and charging stations.** Public infrastructure is easily modified to detect and record anything that is typed to them including account identifiers and credentials.
8. **Do not connect unknown USB flash drives** to your device. They may contain malicious software.
9. **Do not install software that is from an unknown source** or software that is delivered through an unknown channel.
10. **Be extra careful when presented with unknown links or attachments**. Be aware of websites that may push inappropriate content or malware without your authorization.
11. **Do not connect to the University's network** unless absolutely necessary. Consider that all network connections, including encrypted connections, are being monitored.
12. **Electronic data has the same legal status as paper based information assets.** The content, not the medium, determines the treatment of the data. Protect notebooks and paper documents with the same diligence as electronic information.
13. **If your device or data is stolen while you are abroad** and it is University owned equipment or University data, report it to the University's IT Security Department as well as Campus Security.
14. **If your device has been compromised unknowingly during travel**, it is a risk to all systems that the device connects to. If it is University owned equipment, do not use the technology upon return without it being wiped and refreshed by the IT Support Centre.

Further information on Cyber Security while travelling is available on the Government of Canada's websites at:

Cyber Security while travelling
https://travel.gc.ca/travelling/health-safety/cyber-safe and

Remaining cyber safe while travelling: security recommendations
https://travel.gc.ca/travelling/health-safety/cyber-safe/recommendations

If you have questions about Cyber Security please contact the University's IT Support Centre
Email: itsupport@ucalgary.ca or phone 403-220-5555