Cyber Security and Travel Considerations

Check List

- Consider using loaner devices
- Backup your devices
- Update and secure your devices
- Decide what data is absolutely necessary
- Avoid use of “Free” or public wireless
- Avoid use of public workstations
- Be aware of your surroundings when logging into any device
- Avoid leaving your devices unattended
- Use the Western ROAMS VPN where possible
- Notify Western immediately if a device is lost or stolen
- When you return, change any passwords used while travelling
Your Responsibilities

University-related travel includes within it the responsibility to safeguard yourself as an employee, student, or researcher, but also the information on your person, on your digital devices, or within the access of application platforms you may access while away.

Implications related to cyber security and travel include digitally securing devices such as phones and laptops, being mindful of connecting to unknown access networks, physical theft or loss, and the threat of having digital traffic intercepted.

Before Traveling

UPDATE AND BACK UP YOUR DATA BEFORE YOU GO
A good practice is to backup all of the data on your device prior to your travels; ensure documents, pictures, videos, etc. are part of the backup process; also, apply all relevant security and application patches recommended by your vendor.

CLEAN YOUR DEVICE BEFORE YOU TRAVEL
A good practice, combined with the above BACK UP recommendation, is to clear your device of sensitive information (personal or professional) before copying back to your device upon your return a recommended action is to have your device scanned for malicious code.

ENSURE A PIN IS IN USE FOR YOUR MOBILE DEVICE AND ENABLE REMOTE Wipe FUNCTIONALITY
Where available and appropriate, enable the functionality for remote wiping your device should it be lost and ensure that the PIN functionality is enabled and working (the numerical access code you use to access your device).

While Traveling

KEEP YOUR DEVICES WITH YOU AT ALL TIMES
Remain diligent about where your devices are, where they are stored, and do not leave your technology unattended at conferences, hotels, or transportation venues.

BE AWARE OF "OTHER" NETWORK CONNECTIONS
Ensure your devices do not automatically connect to active Bluetooth or wireless networks; enter into "airplane" mode when you are able.

UNTRUSTED NETWORKS
When conducting university-related business, try to use official conference-provided or host-provided (universities, etc.) networks; try to avoid the free wireless hotspots provided by transportation venues, coffee shops, and other consumer-oriented locations.

USE WESTERN ROAMS (VPN) WHEN CONNECTING TO WESTERN RESOURCES
By using the Western ROAMs VPN solution, you are establishing an encrypted channel between your device and any resources you might access; this connection makes your device look as though it is on the Western network.

BE CAUTIOUS ABOUT EXTERNAL STORAGE DEVICES
If you absolutely need to bring a mobile storage device (hard drive, USB stick, SD card, etc.), please exercise diligence in terms of where the device is at all times; if the device contains particularly sensitive information, it is a good practice to encrypt the drive.

After You Travel

CHANGE YOUR PASSWORD(S)
If you are able, a good practice is to change your password before going and then changing again upon your return; your password (or passcode) may take different forms: PIN for your mobile device, local password for your own laptop, or your Western credentials if it is a laptop provided by the university; finally, some jurisdictions may demand your password upon entry to their nation—please follow up with Western Legal Counsel or the Privacy Officer for further information on what you are able to do to protect yourself.

USE WESTERN’S WEB-BASED OFFICE 365 FOR DOCUMENTS AND COMMUNICATIONS
It is a good idea to utilize the Office 365 platform (myoffice.uwo.ca) when abroad as it maintains the messages and documents in a secure location; further, there will be no cached or downloaded versions of these items on your local device.

BE AWARE OF YOUR SURROUNDINGS
Watch for possible shoulder surfers, and be discrete when entering your ID and passwords into any device. Be aware of pickpocket scenarios. Avoid having your devices out and visible in public spaces.

AVOID TAKING THIS TYPE OF DATA WITH YOU, UNLESS ABSOLUTELY NECESSARY TO CONDUCT WESTERN BUSINESS

- If you must travel with this type of data, make certain your device is using full disk encryption.
- Ensure your device does not automatically login any of your accounts.

CONFIDENTIAL, SENSITIVE or PROPRIETARY DATA