Travel Safely With Your Electronics

As a member of the University of Regina community, your electronic devices may contain sensitive information about the university, its students, its employees, and/or its research. This data is a target for hackers and identity thieves, which is why every traveller has a responsibility to keep this data safe and secure. Protecting your electronic devices and the information they contain – both personal and University-related – is critical when travelling. Follow these security steps before, during, and after your trip for a safer experience.

BEFORE YOU TRAVEL

ACCESS RISK

When travelling abroad, review the Government of Canada's Travel Advice and Advisories for your destination(s). Note the risk level and associated recommendations. Health and Safety may also be contacted for risk advisory services (health.safety@uregina.ca).

COMPLETE THE TRAVEL AUTHORIZATION WORKFLOW

This will direct you to additional travel safety planning resources, if applicable.

SECURE ACCESS TO YOUR ELECTRONIC DEVICE(S)

Use strong PINs, passphrases, or passwords.

MINIMIZE DATA

Remove sensitive and non-essential data, applications, and stored payment methods.

ENCRYPT STORAGE

Ensure your device's storage is encrypted. Encryption is a process that turns the information stored on your device into unintelligible text characters that only be read with a decryption key. **NOTE:** Some countries restrict or ban encrypted devices; verify regulations for your destination. If encryption is not allowed, access UofR data via web browser only.

MULTI-FACTOR AUTHENTICATION (MFA)

The University of Regina requires Duo MFA for employees (faculty and staff) to access certain university applications. The Duo mobile app will function offline (via passcodes) or when connected to the internet. Logins that require the Duo MFA will not be successful if these originate from countries under US/Canadian sanctions as Duo does not permit the MFA application or its use in these countries. Microsoft Authenticator, which is currently used for M365 authentication, may also be used for communication while traveling.

WHILE YOU ARE TRAVELLING

CONNECT SAFELY AND USE NETWORKS WISELY

Turn off automatic Wi-Fi/Bluetooth connection features. Disable wireless peripherals when not in use. Be aware that networks without encryption are vulnerable to man in the middle attacks and are commonly employed in travel specific areas (e.g. such as near airports). Avoid public Wi-Fi and unencrypted networks for sensitive tasks (e.g., banking, accessing university data). Use a trusted Virtual Private Network (VPN) when on public or unencrypted networks (see Tech Note #569 for VPN configuration instructions).

MONITOR YOUR DEVICE(S)

Check regularly for unusual behaviour or signs of tampering (e.g., abnormal battery usage, unknown apps installed, camera or microphone activation). It is also wise to occasionally reboot your mobile devices. If you must leave your device unattended, use secure storage (e.g. a hotel safe).

BE AWARE AT BORDERS

Border officials may inspect devices. Before traveling, review your rights and limitations at a border crossing and follow applicable laws. If asked for access, wherever possible, unlock the device yourself rather than providing your password to others.

REVIEW GUIDANCE

Consult the Government of Canada's guidance:
Remaining cyber safe while travelling; security recommendations

Device security for travel and telework abroad

Mobile devices and business travellers - Canadian Centre for Cyber Security

How can you protect your research during travel?

AFTER TRAVELLING

UPDATE CREDENTIALS AND STAY VIGILIANT

Change passwords and PINs used during travel. Be alert for increased phishing/fraud attempts. Monitor credit card statements for unauthorized charges.

REPORT ANY ISSUES OR INCIDENTS

Immediately report any suspected theft or security incidents involving University devices or data to the IS Service Desk and Protective Services at 306-585-4999 or Online and In-person Reporting.