Safeguarding your data while travelling

We all share in the responsibility of protecting the University of Toronto's (U of T's) data, and we are all responsible for our devices and the safety of the data they contain. When travelling outside of Canada, cyber security threats are very real: malicious attacks can intercept calls and internet traffic, or demand direct access to our devices. This tip sheet offers good practices for any U of T staff, student or faculty member who travels on behalf of the University.

BEFORE YOU TRAVEL

1. **Make sure the software on all your travel devices is up to date.** Updates to your computer software and mobile device applications will work to fix known security gaps.

2. **Empty the devices you will take with you.** You should not travel with confidential data on your mobile phone and computer. Create temporary online data stores with only the data you need for the trip.

3. **Use a "burner" device.** Burners are inexpensive devices that can be used on a temporary basis when travelling. If you choose to bring your own personal devices, back up your information with a cloud service or a secure device you leave at home.

4. **Before you depart, turn off "remember me" and wipe stored passwords from all travel device applications and browsers.** Change your existing device and online account passwords to temporary travel passwords. To keep secure records of your new passwords, use a password manager such as Password Safe or KeePass.

5. **If you need to bring a portable hard drive or USB drive with you, ensure the devices are trusted and encrypted.** Never use an unfamiliar or untrusted device for this purpose.

6. **Make sure all devices and accounts are protected by strong passwords.** Where possible, set up multi-factor authentication (also known as MFA, 2FA, two-factor authentication and two-step authentication). This will ensure that the only person with access to your accounts is you.

7. **Ensure you have the departmental authorization to take data off-site.** Always check with your departmental contact first.

Safeguarding your data while travelling

AS YOU TRAVEL

1. **Keep your devices with you at all times.** Pay extra attention at airport screening and other security checkpoints, and never leave your belongings unattended at conferences.

2. **Turn off auto-connect for Bluetooth and Wi-Fi.** This will prevent your devices from connecting to unsecured and potentially malicious wireless networks.

3. **Avoid using untrusted wireless networks such as those at hotels, airports and coffee shops to conduct University-related business.**

4. **Use a virtual private network (VPN) such as UTORvpn before connecting to any University or personal online service.** Check with your department when creating your travel security plan as not all VPNs will work in all countries.

5. **When travelling, access your confidential files via O365's web interface.** The system is designed to maintain the University's data security.

6. **Do not use unfamiliar devices.** Avoid publicly accessible computers, and do not plug in unknown and untrusted devices such as USB drives and power chargers.

7. **In case of loss, make sure you know how to remotely wipe your personal devices.** Travel with a copy of your cellular provider's toll-free phone number so you can quickly have service suspended or blocked. You can also set your mobile lock screen to a photo of your emergency contact information to facilitate retrieval in the case of a lost device.

8. **Practice the same caution you would at home.** Do not download or click links from untrusted sources, and delete emails that seem suspicious.

9. **When you return, use a trusted device to change all the passwords you used while travelling.**

ADDITIONAL RESOURCES

If you require user assistance while travelling please contact your local **campus IT desk**.

If you are experiencing a known or suspected information security incident please email **security.response@utoronto.ca**.

To learn more about securing your data, visit **securitymatters.utoronto.ca**.