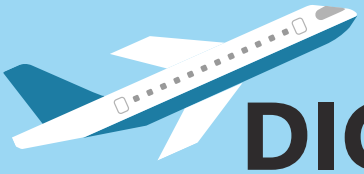

UNIVERSITY OF WATERLOO'S GUIDE TO

DIGITAL TRAVEL SAFETY

How to keep your data safe and secure while travelling

THINGS TO CONSIDER BEFORE YOU LEAVE:

BACKUP AND ENCRYPT
Ensure your devices are backed up completely to multiple safe locations before you leave. In addition, encrypt all data on your devices.

BE WARY OF THE BORDER
You may want to travel without any sensitive data. Border agents in some countries have been known to seize devices and duplicate the data on them.

USE TRACKING SOFTWARE
Install device tracking software to locate missing or stolen devices, or to remotely wipe its memory and storage in the case that it becomes irretrievable.

USE ANTI-VIRUS SOFTWARE
Use anti-virus and firewall software on your devices to prevent security attacks. Make sure your operating system and applications are up-to-date.

TWO-FACTOR AUTHENTICATION
Investigate whether your 2FA method will work at your destination. Text message 2FA might not work in places with spotty cell service.

USE A CHARGING BLOCK
Use a charging block rather than a USB port at a charging kiosk. Charging cables can be used to transfer data, leaving your data vulnerable.

AVOID EXTERNAL STORAGE
Avoid using unknown USB drives, CDs, DVDs, or other media storage with your devices. These can harbour malicious software (malware).

LIMIT WHAT YOU PACK
Use company phones and computers that can be wiped clean upon your return, or buy a cheap burner phone to use just for the trip.

PROTECT YOUR CREDENTIALS
Use strong, temporary passwords during your trip and revert to your original passwords later on. Use different passwords for each of your different accounts.

THINGS TO CONSIDER DURING YOUR TRIP:

GET SECURE ACCESS
Securely access data from your destination. This may be hard to do if you are somewhere without reliable Internet or if your location blocks VPN.

NO SECURE ACCESS?
If there is no VPN available, avoid sending confidential data. You may even want to set up a disposable email account to use during your trip.

AVOID UNSECURED WI-FI
Many public venues offer unsecured Wi-Fi. Never transmit sensitive data using unsecured networks unless you take other steps to prevent digital snooping.

BEWARE OF PUBLIC DEVICES
Public or shared devices may be insecure or contain malware that can capture passwords and communications. Using these devices can be risky.

YOU MAY BE MONITORED
Be aware that your web activity (e.g. webmail, web browsing, Skype, Wikipedia, Google Apps) may be monitored by the government or other entities.

WATCH YOUR DEVICES
Pay close attention to your devices and keep them nearby at all times. Turn off auto-connect for Bluetooth and Wi-Fi connections.