For the Record...

SECURITY TIPS WHEN TRAVELLING WITH MOBILE DEVICES

Overview

Travelling with smartphones, tablets and laptops? Worried about new rules that are changing frequently? Border and airline security practices are more dynamic than ever, making it truly a "traveller beware" environment. It is important to note that border and airline security agents have the authority to stop you from boarding a flight or crossing a border if you refuse to provide access to a device in your possession.

In addition to border and airline security practices, you should always be vigilant when travelling with devices that may be remotely hacked, lost or stolen. Be careful when connecting to Wi-Fi and in accepting USB devices from unknown sources. More specific guidance is outlined below.

Before you leave

- **Only take the devices you absolutely need!**
- Make sure your mobile device is password protected with a complex password.
- Back up your device(s) and have all your software updated, including virus scan software.
- Have your laptop encrypted so if it is lost or stolen your data will not be accessible. Free encryption software is available through Information Technology Services (ITS) at: http://www.mun.ca/its/dataencryption/fde.php.
- Have Memorial's virtual private network (VPN) installed on your university-managed device. This provides offsite users secure remote access to files shares and other IT resources normally only accessible from on campus and removes the need to store those files locally on your device. VPN can be requested through ITS at: http://www.mun.ca/cc/services/servicecatalogue/VPN.php
- If you have an iPhone, enable "find my phone" so you can find it if misplaced.

While you're travelling

- Only turn on your Wi-Fi when required, and be vigilant if connecting to public Wi-Fi.
- To avoid unauthorized connections to your Bluetooth, only turn it on when required.
- If your devices can't go with you (e.g., going for a swim), ensure they are stored in a secure location such as a hotel room safe.
- If you have a university-managed smartphone you can contact the ITS Service Desk (709-864-4587) to have the device wiped if it is lost or stolen.
- Minimize online transactions (i.e. online banking) while traveling to reduce the risk of exposing sensitive/confidential data.

For the Record...

- Do not use USB/storage devices that are given to you from unknown/untrusted sources during your travels. This includes USB devices given as "freebies" at conferences and meetings. These types of devices can be carriers of viruses, etc. and cause significant damage to your device(s) or network(s) to which you have access.

If you need assistance or have any questions, please contact the ITS Service Desk at 864-4587, help@mun.ca or chat support at http://www.mun.ca/its/support.php, or drop by at HH2012 or UC3000.