ONTARIO TECH

BULLETIN FOR CYBERSECURITY TIPS WHILE TRAVELLING INTERNATIONALLY

This document is intended to provide readers with cyber security information to increase awareness of cyber threats that they may face when travelling internationally. This document covers various technologies and devices that individuals may interact with while travelling such as Bluetooth, Wi-Fi, computers, and mobile devices. Adhering to this document will help mitigate and, in some cases, eliminate the cyber security risks that come with travelling internationally.

1. Before Travelling

- ***Data Backup:***
  - Back up important data files to a device that you will not travel with.
  - Devices with important data can get lost or damaged in transit or stolen.
  - Never travel with data that you are not prepared to lose or that violates your employer's policies or applicable laws.

2. While Travelling

- ***Social Media and the Public:***
  - Don't give your social media details to strangers. Consider making your accounts private.
  - Don't post information or photos online that someone could use to identify your location. Post pictures after you've left an area.
  - Take precaution if using dating apps overseas.
  - Be aware of your surroundings and be mindful of people who might be trying to view your screen or keyboard.
- ***Charging Your Devices:***
  - Use your personal computer or a direct-to-wall-socket charging port when charging your devices.
  - Avoid charging your devices on other computers or devices that you do not control, namely hotel docking stations, as malicious software on other devices can be transferred when your device is connected.
- ***Connecting Your Devices:***
  - Disable your Wi-Fi connection when you are not using your device to connect to the Internet. Use a VPN when connected to the Internet.
  - Never connect an unknown device to your tablet or laptop. Any device that connects to a USB port (external hard drives, MP3 players, etc.) can be considered a storage device and may contain malicious software.
  - Avoid using unknown storage media (CDs, DVDs, floppy disks) in your computer. They may contain malicious software that automatically reads the contents of storage media or drives. You do not need to click on a malicious file for your computer to be infected.

3. Wi-Fi

- ***Using Wi-Fi:***
  - You can connect your devices to the Internet at wireless access points, coffee shops, hotels or airports while travelling.
  - Using public Wi-Fi networks is not recommended because they are easily hacked.

- Individuals can create free Internet access points and steal the identity and personal information of other people.
- Information sent over an unknown network could be intercepted.
- As a best practice, avoid connecting to public wireless Internet and logging into sensitive accounts (i.e. Bank Account) or sending information that you would not like other people to know about.

- ***Public or Shared Devices:***
  - Facilities such as hotels and airports offer devices that can be used to connect to the Internet.
  - These devices should not be considered as trusted access points as malicious software and hardware can be installed by members of the public.
  - When using shared or public computers, don't use the "remember me" feature when logging into accounts. Log out of accounts when you're done.
    - ***Keylogger Example:***
      - A keylogger in the form of software or hardware records information typed by the user on the computer (passwords, credit card numbers).
      - Travellers are advised to not use publicly accessible devices for viewing or transmitting information that, if disclosed, could harm the traveller or the traveller's organization.

4. Portable and Mobile Devices

- ***Phones:***
  - ***Password Protection:***
    - Enable a password on your device and change the password before travelling, regularly while travelling, and after the travel is complete.
    - Ensure the password meets the complexity requirement defined by the organization's security policy.
    - Enable the setting that erases all device data after a certain number of failed login attempts.
  - ***Protecting Your Device:***
    - Enable self-locating options and anti-theft software.
    - Keep your devices in your possession at all times. If this is not possible remove the battery, memory expansion and SIM cards, and keep them with you.
  - ***Compatibility and Security:***
    - Use multi-factor authentication to add an extra layer of security.
    - Contact your service provider or your organization's IT department to ensure that the device will work in the area you are travelling to.
    - Avoid connecting the device to the USB port of an unknown or untrusted computer.
- ***Tablets/Laptops:***
  - ***Password Protection:***
    - Enable a password on your device and change the password before travelling, regularly while travelling, and after the travel is complete.
    - Ensure the password meets the complexity requirement defined by the organization's security policy.

        - Enable the setting that erases all device data after a certain number of failed login attempts.
    - ***Device Security:***
        - Update the antivirus software prior to travelling.
        - Install and enable a firewall on the device.
        - Install software updates for the device operating system.
        - Purchase or download software or hardware before travelling.
        - Set web browsers to their highest security setting.
        - Use multi-factor authentication to add an extra layer of security.
    - ***Additional Precaution and Safety:***
        - Disable wireless (Wi-Fi, Infra-Red and Bluetooth) connections when not in use.
        - Avoid connecting USB devices and storage media obtained from unknown sources.
        - Encrypt the data on the device and verify whether or not the area you are travelling to permits entry of a device with encrypted data.

5. Digital Information Laws and Regulations

- ***Intellectual Property***
    - You must obey the intellectual property, digital information and encrypted data laws in the countries you visit.
    - In some countries the government is able to view your web activity and make you give them the data on your device including corporate intellectual property.
    - Downloads on your device can cause intellectual property and digital asset problems when travelling from country to country.
    - Before travelling abroad, contact the embassy of your destination country in Canada to familiarize yourself with the intellectual property, digital information and encrypted data laws.
    - Border agents are legally entitled to search and confiscate the devices of those entering or leaving their countries. Do not take any data into another country that you are not prepared to lose.

6. Bluetooth

- ***What is Bluetooth?***
    - Bluetooth is a technology that enables a connection between two devices.
    - Users have to allow another device to connect their device before data is exchanged.
    - Once this connection is made, data can flow freely between the two devices with little or no user confirmation.
- ***Bluetooth-enabled Cars***
    - Take precaution when pairing devices to Bluetooth-enabled cars. When your device is paired with a car, your personal information is stored on the car's system.
    - As a best practice, do not pair devices with rental cars, but if you do, ensure that stored data is deleted and remove your device from the rental car's paired device list.
- ***Bluetooth Connections***
    - Some Bluetooth devices connect automatically to Bluetooth networks without authorization.

- Disable your Bluetooth networking while travelling to prevent unwanted connection attempts and remove lost or stolen devices from your paired devices list.

7. Protecting Your Equipment

- ***Securing Devices***
  - Always keep your devices with you and do not leave them unattended. Do not allow strangers to use your devices.
  - Lock up valuable or sensitive electronic equipment when not in use.
- ***Hotels and the Public***
  - Don't leave valuable or sensitive electronic equipment in your hotel room. If you do, remove the battery, if possible and the SIM card and keep them with you.
  - Don't flash expensive devices in poor or crowded areas.
- ***While Travelling***
  - Keep electronic equipment in your carry-on baggage to avoid loss or damage in transit.
  - Power off devices while going through customs or inspection points.

8. Devices From Events

- ***Conferences and Training Events***
  - During conferences and training events, software and hardware that contain malicious software may be offered to participants.
  - Do not attach or access devices received during your travels until they are properly assessed by the organization's information technology team.

9. Targeted Email Attacks

- ***Phishing Attacks***
  - Before, during and after travelling to a scheduled event, travellers may receive targeted email attacks.
  - These emails appear authentic, typically request sensitive information and may unknowingly install malicious software on your device through an attachment or web link.
  - Travellers attending international conferences on energy, environment, finance and military are commonly targets of spear phishing attacks.

If you have any inquiries regarding this document, please contact the Office of Risk Management at orm@ontariotechu.ca.