

Cybersecurity: Some Advice for Travellers

While travelling, users may be carrying a variety of computing platforms and devices whose compromise or theft could cause harm to HEC Montréal. The present document contains advice on how to protect against cyberattacks that may affect employees, faculty and students at the School while travelling abroad or at home.

IMPORTANT



In some countries, business centres and hotel telephone networks are monitored and, in some locations, hotel rooms may even be searched. As a general rule, you should not expect your right to privacy to be respected in offices, hotels, Internet cafés or any other public place.

Before Leaving

A cyber-safe trip abroad requires good preparation. With this in mind, it is recommended that you:

- **Backup all content** on your computer and telephone. As long as you regularly save data on the School's shares (U and P drives, Sharepoint, Teams and OneDrive), you have nothing to worry about: your data will regularly be copied by the School's IT services and will be accessible remotely using a secure connection. If you use personal devices, be sure to save data in a safe and secure storage space.
- Consider the consequences for your organization of the loss or theft of information stored on your travel device. Delete data from the device that is not needed for the trip, while making sure you back up all data on the School's servers.
- Change passwords and access codes on your devices to strong but easy-to-remember combinations.
- Enable a screensaver on your cell phones that contains a name and contact point, in the event you lose the device. Avoid mentioning the School's name.
- If you don't need the Bluetooth function on your mobile device, disable it.
- Make sure you have the VPN client installed on your computer to be able to establish secure connections with the School's network. All laptop computers provided by the School have this VPN installed by default.

During Your trip

- Keep your device with you at all times. Do not leave the device with a baggage check service and avoid security lockers in trains, airports and hotels.
- Consider that people in your immediate environment may be able to see your screen or your keyboard, especially in public areas (for example, protect your passwords from prying eyes) and log off when you have completed your work session.
- Empty the Trashcan and "recent" files after each use. Clean up the browser after each use, deleting the history files, cache, cookies, URLs and temporary Internet files.





WIFI

- In some cases, free Internet access points are set up for malicious purposes and are intentionally given misleading names to give the impression they are trustworthy access points. For example, a hotel may have set up an access point called "HotelABC Internet". A threat actor may set up a malicious access point close to the hotel called "SecureHotelABC Internet". The signal strength of this latter access point may be superior to the hotel's access point. The user may believe this latter connection is to be preferred. The traveller should therefore check with the hotel or conference organizer for the name of the legitimate access point.
- Be especially careful with public WiFi networks. It may be tempting to connect to them when the 4G/LTE network is weak or failing. However, doing so may put your information at risk. To avoid any threat, we recommend you only use secure "VPN" or "HTTPS" connections when you have no choice but to use public networks.



Public Computers

- Never use a public computer (at an exhibition or conference for example) to log in to your professional session or to make financial transactions, because this type of device is highly vulnerable to cybercriminal threats. Hackers may have installed a **keylogger** or other malicious software, enabling them to steal your login credentials, access codes and passwords. The only use you should make of public computers is looking for tourist information.



Loading Stations

- Airports and other hospitality structures now offer **free charging stations for computer devices**. This may seem convenient and helpful, but it also comes with risks. Bring your own charger or **backup battery**. Avoid connecting to any charging station that a traveller or conference speaker offers you.
- You should also avoid connecting your telephone or laptop to USB devices and storage media obtained from unknown sources.



Do not trust social media networks

- Do not trust public communications, especially on social media networks. Avoid posting information about your destination, the goal of your trip or your length of stay.
- If you really want to post photos of your trip, be sure to change the **confidentiality parameters of your posts** and be sure to limit access to people whom you really trust (families and close friends for example). Above all, avoid **public sharing**, since this means anyone can see your posts.



Security incidents

- Report suspicious incidents without delay to IT tech support at soutien.ti@hec.ca.

Once you return from your trip, watch for any suspicious activity on your computer or cell phone. Immediately report any anomaly to IT tech support.

Useful links

<https://cyber.gc.ca/sites/default/files/publications/ITSAP.00.001-e.pdf>

<https://cyber.gc.ca/sites/default/files/publications/itsap70015-e.pdf>

<https://cyber.gc.ca/sites/default/files/publications/ITSAP.00.001-e.pdf>



3000 chemin de la Côte-Sainte-Catherine
Montreal, Quebec H3T 2A7 CANADA
Telephone: 514 340-6000