International Cyber Security Guidance

International travel exposes your device to risks that take many different forms. The good news is that vigilance and a few simple steps can protect you, your device, and your information.

Cyber security should not be limited to the home, office, or classroom. It is important to practice safe online behavior and secure our Internet-enabled mobile devices whenever we travel, as well. The more we travel and access the Internet on the go, the more cyber risks we face. No one is exempt from the threat of cyber crime, at home or on the go, but you can follow these simple tips to stay safe online when traveling.

Before You Leave

- **Know your destination's IT security laws and practices**. It's common for some governments to monitor and store Internet activity or copy data from your device without your consent. Certain countries restrict encrypted devices. **CryptoLaw**.org is a useful starting point to research country-specific encryption laws. If government officials ask you to enter your password, do so immediately.

- **Install updates** to your software and operating systems to prevent cyber criminals from exploiting known bugs. **Update your mobile software**. Treat your mobile device like your home or work computer. Keep your operating system software and apps updated, which will improve your device's ability to defend against malware.

- **Change passwords**, and use different passwords for different accounts.

- **Keep it locked.** Get into the habit of locking your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or destroy your information. Use strong PINs and passwords.

- **Back up your data** and media to a device you'll leave at home. **Back up your information.** Back up your contacts, photos, videos and other mobile device data with another device or cloud service.

- **Sanitize your devices** to clear them of documents or media that could be perceived as provocative or inflammatory by certain governments.

- **Less is best**. Bring the least amount of information and data and the fewest devices possible.

During Your Trip

- **Turn off your device**, or at least the Wi-Fi and Bluetooth capabilities, when not in use.

- **Stop auto connecting.** Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to.

- **Limit use of public terminals**, and don’t use accounts requiring usernames and passwords—especially on public machines.
  Think before you connect. Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, train/bus station or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Only use sites that begin with “https://” when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.
  Think before you click. Use caution when downloading or clicking on any unknown links. Delete emails that are suspicious or are from unknown sources. Review and understand the details of an application before installing.
  Guard your mobile device. To prevent theft and unauthorized access or loss of sensitive information, never leave your mobile devices–including any USB or external storage devices–unattended in a public place. Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.

- **Clear your Internet browser** after each use to delete your history, cookies, cache, and downloaded or temporary files. Alternatively, use your browser’s private browsing or incognito feature.

- **Report incidents** when you believe your device or confidential information may have been compromised. Contact your local IT department as soon as possible.

- **Run antivirus software** to scan your device for malware, and follow the instructions to correct any issues.

- **Change passwords again**, using different passwords for different accounts.

COMMON CYBERSECURITY THREATS WHILE TRAVELING

- **Unsecured wireless networks.**

While public wireless networks provide great convenience, allowing people to connect to the Internet from almost anywhere, they are unsecure and can allow cyber criminals access to your Internet-enabled devices. Beyond the typical public wireless networks found at airports, restaurants, hotels, and cafes, they are increasingly available in other places, such as on airplanes and in public parks.

- **Publicly accessible computers.**

Hotel business centers, libraries, and cyber cafes provide computers that anyone can use. However, travelers cannot trust that these computers are secure. They may not be running the latest operating systems or have updated anti-virus software. Cyber criminals may have infected these machines with malicious viruses or install malicious software. One example is keylogger malware which, when installed, captures the key strokes of the computer's users and sending this information to criminals via email. Through this malware, criminals are able to receive users' personal information, such as name, credit card numbers, birthdates, and passwords.

- **Physical theft of devices.**

Thieves often target travelers. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If you are attending a conference or trade show, be especially wary — these venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms.