KNOW BEFORE YOU GO!

GEORGIA MUNICIPAL ASSOCIATION

2023 Cybersecurity Travel Reminders

Before You Go:

- Make sure your devices are always updated to the latest security software.
- Backup your mobile device data in case it is lost, stolen, or has to be wiped.
- Check phone app permissions–turn off camera, microphone, and location services so that they are only on when you are actively using them.
- Stop any "auto-connect" feature that automatically tries to connect with available wireless networks and Bluetooth devices.
- Enable multi-factor authentication whenever it is available to make sure that you are the only one who can access your accounts.
- Set your social network accounts to private and be careful about what travel information you share.

On Your Trip:

Protect Laptops and Phones from Loss or Theft

What Should I Do?

- Use the hotel safe to lock your devices when they are not with you.
- Lock your laptop in the trunk of your vehicle for brief stops.
- Do not take any device you do not really need on your trip.
- Always carry-on your phone and laptop.

Public Wi-Fi

What is the Risk?

- Others can see what you are doing on your computer on public Wi-Fi. This risk is lower if the Wi-Fi is password protected, but the owner and any other individuals who know the password might be able to see what you are doing and capture any usernames and passwords you enter.
- Many apps on mobile devices are designed for use with cell service, so some may not be secure to use on Wi-Fi.

What Should I Do?

- Make sure your device is set so that it does NOT auto-connect to available public Wi-Fi or Bluetooth devices.
- It is okay to use public Wi-Fi for general web browsing, but never enter your username and password for any account or website unless you are securely connected with a personal hotspot or VPN.

Public Cars (Rental, Uber, Lyft)

What is the Risk?

- **Plugging your phone into a USB port saves your personal information to the vehicle and makes it accessible to the vehicle owner and all other users.**

What Should I Do?

- **Use a USB data blocker to safely charge your phone.**
- **Use a cigarette-lighter-to-AC converter and charge from your regular charging block.**

Prevent Malware from Being Downloaded to Your Device at Public Charging Points

What Should I Do?

- **Use your charging block and charger or a USB data blocker.**

Prevent Malware from USB Devices Provided at Conferences or Trade Shows

What Should I Do?

- **Use the conference's laptop and send your presentation ahead of time for the conference leader to load it.**
- **If you must use your own device, make sure the presentation is already loaded onto it or use a safe thumb drive that has not been inserted into any untrusted devices.**

Boarding Pass

What is the Risk?

- **Depending on the airline, your boarding pass's barcode may contain information that can be used for identity theft and loyalty point theft.**

What Should I Do?

- **Opt for a boarding pass on your phone instead of on paper.**
- **Shred any paper boarding passes.**

RFID Chips in Passport, Drivers License, Credit Cards

What is the Risk?

- **RFID (Radio-Frequency Identification) scanners can collect information to be used for identity theft when in very close contact.**

What Should I Do?

- **Keep RFID enhanced cards and documents in a RFID blocked container or cover with aluminum foil.**

https://www.cisa.gov/sites/default/files/publications/NCSAM_TravelingTips_2020.pdf
https://staysafeonline.org/resources/vacation-and-travel-security-tips/
http://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers
http://www.rd.com/article/never-charge-phone-in-rental-cars/
http://www.travelawaits.com/2876670/fbi-warning-not-to-use-airport-charging-stations/