Published on *VirginiaNavigator* (https://virginianavigator.org)

Cyber Safety While Traveling

"Do Nots" When Traveling

We've all been in the airport lounge or travel rest stop and tempted to use their public chargers. We've also used the hotel business office to access travel information or sat in a lobby to do some work using a Wi-Fi connection. This makes life easier, but it also leaves us vulnerable to attack. Malicious actors hack public chargers, essentially arming them as weapons for whatever plugs into the next — like your device. In addition, bad actors might set up Evil Twin Hotspots at public places where Wi-Fi Hotspots are set up for customers, including coffee shops, hotels, retail establishments, and airports. The goal is to trick people into connecting to a fake Wi-Fi hotspot to gain access to your IT devices and data.

- **Do not use public USB ports** to charge your mobile phone, laptop and all your electronic devices.
  - **Preferably, pack your own electrical outlet charger, car charger, and USB cables** to keep with you and use whenever you travel.
  - **If you have to use a public USB port, use a charge-only USB adaptor** that charges your devices but does not transfer data.
- **Never use an unsecured public Wi-Fi** Network for sensitive business practices such as banking or personal information exchange.
  - **If you use secured Wi-Fi** provided by your establishment, always verify the correct name of the public Wi-Fi network with the establishment.

More tips to travel safe

- Cybersecurity While Traveling
- Vacation and Travel Security Tips

To learn more about simple ways to protect yourself and those you care about from online threats anytime and anywhere, visit the VA Cybersecurity Spot.

DigitalVA

Source URL
https://www.digital.va.gov
Last Reviewed
Tuesday, August 20, 2024