

Tech Tuesday: Building a Digital Defense Against Travel Tech Fails

July 20, 2021



TECH TUESDAY: Travel Tech Scams

- Update all anti-virus/malware on devices.
- Change all passwords & PINs to new options before leaving and once you return.
- Don't allow your device to auto-connect to WiFi or Bluetooth while traveling.
- Safer option: use your data connection or a VPN.
- Report scams to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against technology fails while traveling.

You and your family are finally getting to take a vacation this summer after months of lockdowns and closures. The world finally seems to be getting back to normal. Unfortunately, cyber thieves are just waiting for you to pack your bags.

According to our friends at the Federal Communications Commission (FCC), here are some ways to keep you and your digital devices safe while you travel:

Leave any devices you don't truly need at home.

For those devices you do take, make sure to update all anti-virus and malware options before departing **and** again after returning home.

Also, before you travel, make sure to change your passwords and PINs to new, strong options that you do not use at home. When you get back after your trip, change them again to another new option.

Make a backup of your device in case your phone or laptop gets hacked or targeted in a ransomware attack. Remember – back-ups should always be kept offline so the bad guy can't access those as well. Make sure your wireless and Bluetooth auto-connect and remote-connect settings are off while traveling. They are handy to use when at home, but on the road you could accidentally connect to a malicious network without even knowing it. Likewise, it's tempting to take advantage of free WiFi options when in airports, hotels, coffee shops, and elsewhere – but be careful. If you can get in, so can a hacker. If you must connect to a public network, make sure to only use "https" sites. Also remember – never do shopping, banking or access sensitive data – such as your health care portal – while on a public network. Using your own data network connection or using a VPN are always better options. If you are the victim of any online fraud, you should also report the incident to the FBI's Internet Crime Complaint Center at **www.ic3.gov** or call your FBI local office.