West Virginia Executive Branch

Privacy Tip – Safe Holiday Travel Tips

Here are a few tips to help you keep your internet-connected devices safe while you travel.

Threat: Free Airport Wi-Fi

- **Do you need to worry?** Absolutely! Many airports offer free Wi-Fi, which means you're even more likely to fall for a spoofed network. For instance, you're waiting for your flight and notice a "FreeAirportWiFi" network. As soon as you login to that unsecure network, you might run the risk of your data being intercepted by a third party (an attacker), or you might be logging directly into a scammer's network and will be sharing everything with a possible hacker. On top of that, airports are one of the main places you're more likely to be hacked.
- **What can you do about it?** To keep your data safe, consider using a virtual private network (VPN) to block any thief from seeing what you're doing. And, if you absolutely need to access public Wi-Fi and it can't wait until you're on a secure network, switch to your device's data connection.

Threat: Public USB Charging Ports

- **Do you need to worry?** Yes! The main problem is that the USB port doesn't just sent power, it sends data. A USB charging port that is behaving correctly won't try to access your data, however, one which has security vulnerabilities that have been exploited could access your data or even run dangerous code on your device. This attack is known as "juice jacking."
- **What can you do about it?** Newer phones will usually request your permission to share data. Do NOT allow anything but a trusted device to access your data. The USB port will still allow your phone to be charged without allowing access. You can also simply use an AC outlet for charging. There is no risk of data transfer as long as you use a trusted charging cable. Or, get a portable battery to charge your device. You won't have to go in search of an available charging station.

In the future, widespread wireless charging may eliminate the risk of an exploited USB port. You can charge your device at any public wireless charging spot without worrying.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.