West Virginia Executive Branch
Privacy Tip – Identity Theft Resource Center

The Elf on the Shelf might not be the only one causing mayhem this holiday season, scammers are too and they might be doing it through free public Wi-Fi at the airport. The risks associated with connecting to an unsecure network might not be top of mind, but before you hop on a plane this December to visit friends and family (or to just avoid the holidays all together) you'll want to think twice about connecting your device to the free public Wi-Fi that airports generally offer. Let's talk about the risks and why it should be top of mind, not only this season but year round.

Threat: Free Airport Wi-Fi

Do You Need to Worry: Yes, because so many airports offer free Wi-Fi, you're even more likely to fall for a spoofed network. For instance, you're sitting at the lounge before your flight and notice "FreeAirportWiFi" network to connect and do some browsing before take-off. 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); you might increase your chances of distributing malware to your device; hackers may be able to spy on everything you're doing online. On top of that, these are the 10 airports 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.

© Copyright 2018 - Identity Theft Resource Center
Used with permission

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