West Virginia
State Privacy Office

Privacy Tips

June: Traveling Without "Leaking" Data

Vacation season is a high-risk time for data theft. Public Wi-Fi at airports, hotels, and cafes is often unencrypted, meaning anyone on the same network can "sniff" the data moving to and from your device.

Hackers also set up "Evil Twin" networks with names like "Free_Airport_WiFi" to trick you into connecting so they can capture your usernames and passwords in real-time.

Your Action:

- Avoid public Wi-Fi for anything involving a password.
- Use your phone's cellular data (hotspot) whenever possible.
- If you must use public Wi-Fi, use a Virtual Private Network (VPN) to encrypt your connection.
- Also, never plug your phone into a public USB charging station; use a wall outlet or a portable battery to avoid "Juice Jacking" malware.

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