On-the-Go WiFi Safety

5 ONLINE SECURITY TIPS FOR SMARTER TRAVEL

Don't let online security concerns derail your travel plans.

Whether you plan to explore the US on a road trip, hit the beach in the Caribbean, tour a castle in Europe, or hike in South America, these five WiFi safety tips will keep you secure throughout your journey.

1

Keep a clean machine.

Ensure your devices are up-to-date with the latest antivirus, firewall protection and operating system patches.

2

Stop and think before you connect to public WiFi.

WiFi is available everywhere you go, including in airports, hotels, restaurants, parks, and museums, but these networks are completely open and insecure. Use common sense when you connect to public WiFi and be cautious about the sites you visit and the information you send.

3

Paid WiFi doesn't mean safe WiFi.

Just because you paid for WiFi access, it doesn't mean it's safe. There's no encryption to stop anyone from eavesdropping on your communications, so make sure you protect yourself from hackers.

4

Beware of evil twins.

Hackers sometimes set up evil twins – WiFi networks that look real – near legitimate public WiFi networks. If you connect to them, all of your communications can be captured. It can be hard to tell the difference so confirm the name of hotspot with the owner before you connect.

5

Use a VPN to encrypt information on all of your devices.

If you use public WiFi while you travel, the only way to guarantee your security is to use a virtual private network (VPN) like **PRIVATE WiFi** to encrypt your personal data in wireless hotspots. Remember, WiFi signals are just radiowaves. Anyone in range can "listen in" to what you send and receive. Antivirus or firewall software won't protect you – but a VPN encrypts all of your communications no matter where your travels take you.

Learn more at **security.berkeley.edu**

Infographic brought to you by:

STOP | THINK | CONNECT™

Private WiFi®