Traveling cyber-safe

As the holidays approach and travel picks up, cybersecurity risks rise right alongside flight prices! Travel leads to busier airports, busier hotels … and busier hackers.

When you're away from home, you don't have your secure network to protect you. And when you're dealing with the stress and hassle of traveling, you're more likely to make quick or careless decisions that lead your data and money straight into a hacker's hands.

For example, cybercriminals set up open Wi-Fi networks in airports and traveler lounges during the holidays. These networks may be called "Airport Guest" or something similar, and they look harmless.

But these networks allow hackers to spy on your browsing. While you check your email, they check your personal data.

Quick tips for a secure trip

- **Pack light.** If you don't need to travel with a smart watch or an extra laptop, leave it at home!
- **Don't share your trip details** on social media.
- **Use a VPN** to shield your data while browsing on public networks.
- **Avoid open Wi-Fi networks.** If you're at an airport or a hotel, ask staffers for Wi-Fi details.

Or hackers set up fake sites offering travel services. You think you're booking a flight, a hotel, or a pet sitter. But instead, you give them your money and data for a service that never happens.

Before you travel this holiday season, take a few minutes to review your cybersecurity.

Fake travel sites steal data

The Hacker News recently reported on the existence of a mass phishing scam aimed at travelers.[1] Hackers created more than 4,300 bogus domains, including keywords like "Booking" and "Airbnb", and sent out spam emails with phony reservations in more than forty languages. Victims were tricked into providing personal data for fake bookings.

1. https://thehackernews.com/2025/11/russian-hackers-create-4300-fake-travel.html