Vacation and Travel Security Tips

Even if you leave your desktop computer at home, you'll probably stay connected when you're vacationing – you can check your phone on the beach or on a mountaintop. Travelers often rely on technology to enhance vacations, like by sharing photos online or finding lodging on an App. As you embark upon your next adventure, remain cyber safe following some simple practices to keep your vacation plans free from cybercriminal meddling.

Getting Ready to Go

Add a simple cybersecurity checklist along with your packing routine before you depart for some rest and relaxation.

Travel Lightly

Limit the number of devices you take with you on your trip. The more laptops, tablets and smartphones you take with you, the more risk you open yourself up to.

Check Your Settings

Check the privacy and security settings on web services and apps. Set limits on how and with whom you share information. You might want to change some features, like location tracking, when you are away from home.

Set up the "find my phone" Feature

Not only will this feature allow you to locate your phone, it gives you the power to remotely wipe data or disable the device if it gets into the wrong hands.

Password Protect Your Devices

Set your devices to require the use of a PIN, passcode or extra security feature (like a fingerprint or facial scan). This will keep your phone, tablet or laptop locked if it is misplaced or stolen.

Update Your Software

Before hitting the road, ensure all the security features and software is up-to-date on your devices. Keep them updated during your travels by turn on "automatic updates" on your devices if you're prone to forgetting. Updates often include tweaks that protect you against the latest cybersecurity concerns.

Back Up Files

If you haven't backed up the data on your devices, like photos, documents or other files, do so before heading on vacation. If your device is lost, stolen, broken or you otherwise lose access to it, you won't lose all your data. You can back up your data on the cloud, on an external device like a hard drive or, preferably, both.

On the Go

After you follow the cybersecurity to-do list before hitting the open road, there are best practices you can follow while exploring to keep your devices, data and accounts safe.

Actively Manage Location Services

Location tools come in handy while navigating a new place, but they can also expose your location – even through photos. Turn off location services when not in use, and consider limiting how you share your location on social media.

Use Secure Wi-Fi

Do not transmit personal info or make purchases on unsecure or public Wi-Fi networks. Don't access key accounts like email or banking on public Wi-Fi. Instead, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

Think Before You Post

Think twice before posting pictures that indicate you are away. Wait until you getting back to share your magical memories with the whole internet. You might not want everyone to know you aren't at home.

Protect Physical Devices

Ensure your devices are always with you while traveling. If you are staying in a hotel, lock them in a safe if possible. If a safe is not available, lock them in your luggage. Don't leave devices unattended or hand them over to strangers. Using your device at an airport or cafe? Don't leave it unattended with a stranger while you go to the restroom or order another latte.

Stop Auto Connecting

When away from home, disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to. If you do not need them, switch them off. While out and about, these features can provide roving cybercriminals access to your devices.

If You Share Computers, Don't Share Information

Avoid public computers in hotel lobbies and internet cafes, especially for making online purchases or accessing your accounts. If you must use a public computer, keep your activities as generic and anonymous as possible. Avoid inputting credit card information or accessing financial accounts. If you do log into accounts, such as email, always click "logout" when you are finished. Simply closing the browser does not log you out of accounts.

Additional Resources

FCC: Cybersecurity Tips for International Travelers
CISA: Cybersecurity While Traveling Tip Sheet
ID Theft Center: Travel Safe Blog
NerdWallet: How to Travel Safely
Consumer Reports: What You Need to Know About Cyber Safety While Traveling
Iris Powered by Generali: 10 Summer Vacation Identity Protection Tips
AARP: Fraud Watch Network
State Department: High-Risk Area Travelers

- National Cybersecurity Alliance