Staying Cyber-safe on a Summer Vacation

Typical travelers heading out on their summer vacation check that they have the right supplies and clothes for their trip before they hit the road. *Expert* travelers will be also checking to ensure they are educated and prepared to be cyber-safe with their devices and data while on the road!

Thinking of your smartphones and devices as being just as important as your wallet is a proper step in the right direction. These devices contain everything from your banking and payment information to your treasured family photos, and ensuring they are secure and protected when away from home is paramount. Some key tips, strategies, and resources to aid you in being secure during your travels can be found below.

By following these tips and being a cyber-safe traveler, you will have a smooth and enjoyable vacation!

To Do Before Your Trip

Update your devices: 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.

Password/Passcode 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.

Back up your devices: 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.

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.

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 your device to lock after an amount of time: Once you have the passcode, password, or swipe pattern established, you should set an automatic device lock prompting for the access code after a specified time of inactivity. This will prevent a criminal from getting onto your device if you

accidentally leave it unlocked.

Book your trip with trusted sites: When planning your trip and booking transportation, lodging, and experiences, it is important to complete those transactions with trusted, known businesses. If possible, double check the reviews and reputation of a site you are unfamiliar with but are considering to use for your booking. By sticking to reputable sites, you guarantee a higher standard of security for your data and transaction.

Staying Secure During Your Trip

Keep track of your 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.

Securely recharge. Never plug your phone into a USB public charging station, such as those in the airport or in hotel room lamp and clock radio inputs, as these cannot be trusted. Malicious individuals can hijack your session or install malware on your device through those seemingly harmless means. Always connect using your own power adapter connected to a power outlet.

Delete data from your rental car. If you connect your phone to a rental car for navigation or other purpose, be sure to securely remove the device so that other individuals do not have access to your address book, device name, text messages (hands-free calling), or other sensitive information.

Limit your activity on public Wi-Fi networks: Public Wi-Fi that does not require credentials or logging in is not protected by encryption, so browsing and activity is not secure from prying eyes. To ensure your information is not put at risk, avoid logging into your personal accounts or making transactions while on public or hotel networks.

- Use your phone carrier's internet connection or use your phone as a personal hotspot (if your cell carrier's plan allows) when logging into personal accounts or conducting transactions.
- Ensure your device is set to ask your permission before connecting to a wireless network while on your trip.
- If you intend to use a hotel or establishment's customer wireless network, verify what network is the correct one to use with a member of the staff.
-

Do not overshare on social media: 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.

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.

Turn off auto-connect. 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.

When You Return home

Shred your boarding pass and luggage tag. Scannable codes on boarding passes and luggage tags include full name, date of birth, and passenger name record. These can also contain sensitive data from your airline record like passport number, phone number, email address, and other information that you would not want to share publicly. For this same reason, never post boarding passes on social media.

Scan for virus and malware. It is best to update your security software when you return home and scan for viruses and malware to be sure your device has not been compromised while you were away.

Additional Information

- FCC: Cybersecurity Tips for International Travelers
- ID Theft Center: Travel Safe Blog
- 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