Stay Cybersafe on Vacation

Help protect yourself on your next trip with these cybersecurity tips

As summer approaches and life gradually returns to normal, a well-deserved vacation may be on the horizon.

Naturally, vacations are a time to forget about your daily responsibilities and worries. But letting your guard down with your cybersecurity can lead to a disrupted vacation—and long-term headaches, too.

So, whether your travel plans include a beach vacation with your family, a romantic getaway to Europe or city escapades with friends, use these tips to help protect your cybersecurity while you're away from home.

Before You Leave

Overpacking might be fine with your clothes. But not with your devices.

Only bring the devices you absolutely need. Doing so makes it easier to keep track of them and reduces your security risk too. Be strategic about your choices; a tablet or smartphone could be a better option than a laptop because those devices can often be more secure. Make sure your devices can be locked and require a complex passphrase or fingerprint/facial recognition to activate.

And don't overpack your wallet, either. Instead, just take the identification, credit cards and debit cards you plan to use. (It's a good idea, though, to have at least two payment options available.) Your credit cards should ideally have strong fraud protection in case your security is comprised while away. If you haven't already done so, opt in to receive fraud alerts from your credit card companies.

When was the last time you checked if all of your operating systems, browsers, applications and software (including anti-virus protection) are current? If it's been a while—or you don't have automatic updates enabled on your devices—take a few minutes now to update everything. Outdated systems can weaken your security. Plus, they're a nuisance to deal with when you're away. Who wants to struggle with an outdated GPS app when trying to find a hotel or restaurant?

At the Airport

While waiting for your flight, you notice the charge on your phone battery is low. So, you immediately scout around for a USB charging station.

Stop looking. It's dangerous to power up using the charging options available at public places, such as airports, hotels and coffee shops. Hackers sometimes embed their connections at these stations or install charging cords with malware so that they can steal data from your phone.

A better option? Travel with your own charger.

At Your Destination

After arriving at your vacation destination, you decide to unwind from the stress of your trip by relaxing at a local eatery. After ordering your food, you post a few photos to your social media accounts using a public, unsecured Wi-Fi hotspot.
Posting those photos using the public hotspot could be a serious mistake. Cybercriminals can intercept connections that aren't protected, and public, unsecured Wi-Fi hotspots are a prime target.

Instead, create a personal hotspot with your phone and securely connect through a Long Term Evolution (LTE), end-to-end encrypted channel. It's simple to do. Alternatively, use a Virtual Private Network (VPN), which provides an encrypted method of accessing the internet in public settings. VPNs are easy to implement and use, and available from many reputable companies for a nominal monthly fee.

If you're staying at a private rental house, be cautious about the safety of the rental home's WiFi system. Unfortunately the connection might not be secure. You're better off using a VPN or your phone's personal hotspot—especially when engaging in financial activities or accessing other confidential accounts.

Staying at a hotel? Don't use public-access computers (such as those in hotel business centers) because they may contain computer viruses that compromise your information, including login credentials. Be sure to always keep an eye on your own devices at hotels, too. Even the hotel safe isn't a foolproof security option.

Keep in mind, as you blissfully wander around enjoying the sights on your vacation, your devices might be automatically connecting to nearby wireless or Bluetooth networks when you walk or drive past them. This can jeopardize your security by exposing your devices to dangerous networks. Fortunately, you can easily fix this situation: disable the automatic connect option on your devices.

When Traveling Internationally

Foreign travel can be an exciting, rewarding experience. But it also presents added security risks.

So, besides applying the guidelines already mentioned, it's best to be extra cautious when travelling overseas. For example, try to limit any banking or other sensitive transactions.

Also, restrict using debit cards—which offer less financial protection than credit cards—to withdrawals from ATMs located inside reputable banks because these locations tend to offer greater security. When paying for a transaction with a credit card, use the chip reader rather than swiping your card when possible.

Traveling to a high-risk country? You might consider purchasing an inexpensive, disposable phone for the trip and discarding it once the trip is over and you've returned home. If your disposable phone becomes compromised by criminals, they won't have

access to all the personal data stored on your personal phone or the ability to connect to all your other devices and personal networks tucked away at home.