

From airport WiFi to ‘juice jacking’: 7 ways to protect your data when traveling

Travel can be full of cybercrime land mines. Here are expert tips to avoid them.

By Natalie B. Compton

Yesterday at 4:48 p.m. EST



Whether your online data is locked down may be the last thing on your mind as you rush through the airport checking departure times and work emails.

Add in coronavirus worries and “we can expect that travelers are highly distracted and will let their guard down,” Daryl Crockett, a security data expert and CEO of ValidDatum, a data management and cybersecurity company, said in an email.

Hackers have advanced tactics to prey on victims online, and a fraudulent airport WiFi connection is only one of the ways in which they trap travelers. Hank Schless, senior manager of security solutions at the cybersecurity company Lookout, points out that we may have been taught to install protections like anti-virus software on our computers, but our personal devices remain vulnerable — and a preferred entry point for cybercriminals.

“They leverage the trust we have in these devices against us and know that they’re a treasure trove of personal and corporate data,” Schless said in an email.

Despite the risks, “there are certainly ways to be safe,” said Paige Hanson, chief of cyber safety education at the anti-virus and security software company Norton.

Here are seven ways travelers can protect themselves against hackers.

Scrutinize the public WiFi options before connecting

The public WiFi we often rely on away from home can be filled with cybersecurity land mines. Places with lingering travelers — like airports, train stations and coffee shops — can be prime targets.

“While many airports offer free WiFi connectivity, you should make sure you’re joining the real, official network from the airport and not a lookalike network that is set up to lure travelers into giving up their usernames and passwords,” Jeff Sakasegawa, trust and safety architect at the fraud protection company Sift, said in an email.

Schless said attackers have been known to set up fake networks with convincing names like “Starbucks_Guest_WiFi” or “Free_PennStation_Internet,” where they can hijack your device. This method can route all of the victim’s traffic through their system, which could expose their sensitive work data or personal information, such as log-in credentials.

Hanson said travelers should treat their public WiFi use “like someone is looking over your shoulder” and avoid logging into sensitive accounts such as your bank, medical provider or even social media.

Use your own charger

Another significant risk for travelers is using a charger that isn’t yours, Schless said. He warns against ever accepting a stranger’s offer to borrow their charging cord.

“Attackers can exploit USB cords and load malicious software into them that loads itself onto your device the second you plug it in,” he said.

In 2019, the Los Angeles County district attorney’s office warned travelers of the USB charging scam also known as “juice jacking.” They discouraged travelers from using charging stations that could expose devices to malware attacks that can lock devices then export sensitive information such as passwords and bank account numbers.

Turn off auto-connect functions

If your personal devices are programmed to auto-connect to WiFi networks, Hanson recommended turning that off while traveling.

Additionally, she said, travelers should turn off their WiFi and Bluetooth when not in use for further protection.

There is an added bonus to turning off these settings: You’ll save precious battery power.

Turn on account alerts before travel

To stay up to date on your accounts while traveling, Crockett told travelers to turn on alerts for their credit card and banking apps. Doing so will let the company alert you if there is unusual spending or log-ins.

Crockett also advised travelers to know how to lock their debit or credit cards before hitting the road. If you lose or misplace them during the trip, you can lock them to prevent fraudulent use.

Add two-factor authentication or biometric log-ins

Rather than relying on just a password to unlock accounts, Hanson suggests adding two-factor authentication when it’s available. Two-factor verification works by requiring both a password and a unique code. Even if a hacker had your password, they would need to physically have one of your personal devices to get the code for the second step.

Even better: Hanson suggests enabling biometrics — i.e., a fingerprint or face ID — to open your devices or apps.

Consider a VPN

Crockett recommended that travelers get a Virtual Private Network (VPN) that will encrypt most of the data sent and received over phone or laptop. She suggested going to McAfee to find a package that offers VPN protection for multiple devices. Many workplaces also offer VPNs on company devices.

Hanson warned against using a free VPN. “If it’s free, you might be the product,” she said.

Another option is downloading a security app for your phone to prevent mobile phishing attacks.

Be wary of subscription renewal emails

The most common way for attackers to steal login credentials these days is through socially engineered phishing campaigns, Schless said. By posing as an airline, credit-card company or online retailer, there is a lower chance that a scam will be detected or be blocked by automated protections.

“On mobile devices, these campaigns can be executed across SMS, email, social media platforms, third-party chatting apps, gaming and even dating apps,” Schless said.

For example, Crane Hassold, director of threat intelligence at Abnormal Security, a cloud email security platform, said he has recently noticed cyberattacks targeting travelers by impersonating the Transportation Security Administration via email.

Here’s how it works: A scammer will send out an email telling the recipient that their TSA PreCheck is due for renewal. The renewal email link leads to a fake but legitimate-looking site where hackers can accept a payment and steal a victim’s personal information.

Hassold said the TSA would never send emails like this. Travelers should go directly through the [TSA website](#) for information on their existing accounts.

More travel tips

Return to travel: [Your guide to traveling again, in 5 steps](#) | [What to do if your flight gets canceled](#) | [Getting through to airline customer service](#) | [Who’s welcome back on cruises](#) | [When to get a covid test for travel](#) | [Are PreCheck, Global Entry or CLEAR still worth it?](#) | [Do you know how to tip?](#) | [What do travel advisories mean?](#)

Road trips: [Should you fly or drive?](#) | [Best planning tips](#) | [Snacks](#) | [Overlanding advice](#) | [Rental cars](#) | [National park tips](#) | [Rental car disasters](#)

Camping: [Finding a campsite](#) | [Plan your meals](#) | [Solo camping](#) | [First-time tips](#) | [Watch out for wildlife](#)

Planning: [Where to leaf peep this fall](#) | [National park alternatives](#) | [How to get your passport](#) | [A case for making a travel journal](#) | [Get started on holiday travel planning](#) | [How to find ‘greener’ flights](#)