THE INTERNET SURVIVAL GUIDE

for travelers



What you'll find in this guide:

- Know Your Surroundings
- Your Survival Kit
- Your Biggest Threats
- Emergency Response

Powered by PHIN

KNOW YOUR SURROUNDINGS

What do these mean?

Travel can take you outside your usual digital surroundings as well as your physical ones. Unfamiliar Wi-Fi networks, booking websites, QR codes, charging stations, and messages about flights or accommodations can all create opportunities for scammers.

Phishing: A fake email that tricks you into clicking, sharing info, or sending money.

Smishing: Phishing by text message.

VPN: Virtual Private Network. It encrypts your connection on networks you don't control.

Qishing: A malicious QR code that sends you to a fake or dangerous site. These can be found covering non-malicious QR codes for parking, informational signs, and more.

Public Wi-Fi: A shared network in airports, hotels, cafés, and stations.

Major red flags to look out for:



🚩 **Urgency:** your booking will be canceled or your payment failed, so act now.

🚩 **Unexpected payment requests:** a hotel, host, or airline asks you to pay again or somewhere new.

🚩 **Moving off-platform:** someone wants payment or chat away from the booking service.

🚩 **Suspicious Wi-Fi:** a generic or almost-correct network name.

🚩 **Strange links or QR codes:** you're sent somewhere you didn't expect.

🚩 **Too good to be true:** stays, flights, or tickets far cheaper than anywhere else.

You're allowed to be spontaneous on vacation, but your cybersecurity shouldn't be.

YOUR SURVIVAL KIT

For help setting anything up, reach out to your IT provider.

Update your phone, tablet, laptop, browser, and important apps before traveling. Updates often fix security weaknesses, and hotel Wi-Fi is not where you want to discover you needed one.

Use strong, different passwords. Store them in a password manager. One stolen password shouldn't unlock your email, banking, social media, and travel accounts.

Lock your devices. Use a PIN, password, fingerprint, or face recognition and make sure devices lock automatically. Your phone contains considerably more valuable stuff than the emergency pair of underwear in your suitcase.

Turn on device-finding (like "Find My iPhone") and automatic backups for photos, videos, and any other important information. Doing this is much more valuable *before* you lose your device.

Use trusted connections. Your mobile data is preferable to unfamiliar public Wi-Fi for sensitive activity. If you do use public Wi-Fi, confirm the correct network name with staff and avoid accessing sensitive accounts unless necessary.

Turn off automatic device pairing. The last thing you want is to automatically connect to "Joe's laptop" without even realizing it.

Set up MFA (multi-factor authentication) on email, banking, and travel accounts. Where possible, use an authenticator app instead of text messages, especially if you'll be switching SIM cards while traveling.

Check that your account recovery information is current before traveling. Keep important booking information and emergency contact details somewhere you can access even if your phone is lost, stolen, or broken.

Do your research before booking. If the accommodations seem too good to be true, they probably are. Check that it's a real, reputable host before booking.



Before you connect, click, scan, book, pay, or share:

ALWAYS PAUSE & PONDER:

Who is this?

Is it really your airline, hotel, or host? Check the email address, not just the display name and logo.

What do they want?

Another payment? Your card details? A password, login code, or passport info? Be extra careful with unexpected requests for sensitive info.

Why has something changed & does it make sense?

- Why has your hotel suddenly changed its bank details?
- Why does your host need payment outside the platform?
- Why is an airline you've already paid sending a new payment link?

When does it need to be done?

Travel deadlines make urgency convincing. Don't let "your booking will be canceled" rush you into making a quick, bad decision.

Where can I verify it?

Open the official airline, hotel, or booking app yourself, or use contact information from your original booking, not the information provided in the suspicious message.

YOUR BIGGEST THREATS

1 "FREE AIRPORT WI-FI"

You spot “Airport_Free_WiFi” and connect without thinking. But scammers create networks with believable names to lure travelers in.

What should you do? Ask staff or look for signage that tells you the correct network name, avoid sensitive tasks on untrusted Wi-Fi, and forget public networks after use.

2 "THERE'S A PROBLEM WITH YOUR BOOKING"

A convincing message with real-looking details about your hotel, flight, or rental says there’s a payment problem, and you need to click a link or pay again.

What should you do? Don’t use the link. Open the booking service’s official app or website yourself and check your reservation there.

3 "SCAN HERE."

QR codes are everywhere when you travel: menus, parking, tickets, transit. A fake code stuck over a real one can send you to a convincing scam site.

What should you do? Check that a QR code hasn't been stuck over another one. Preview the web address before opening it and be especially cautious if the destination asks for payment or login details.



4 "AN AMAZING PLACE FOR HALF THE PRICE."

A beautiful villa appears at a price your vacation budget loves. But the property might not exist, and the photos may be stolen.

What should you do? Research properties independently and be wary of pressure to pay off-platform, especially by wire transfer or crypto.

5 "CHARGE YOUR PHONE HERE."

Public USB charging ports are convenient, but plugging an unknown cable or USB port directly into your device can introduce unnecessary risk.

What should you do? Use your own charger in a standard outlet or carry a battery pack. If you must use an unfamiliar USB connection, don't approve unexpected prompts to share data.

6 "GREETINGS FROM PARADISE!"

Posting your vacation in real time tells strangers where you are, and worse, where you're *not* (home). Photos can also reveal boarding passes, passports, room numbers, or your exact location. Especially now with AI, someone may be able to identify your location from a photo alone.

What should you do? Check backgrounds, don't share travel documents, and save the photo dump until you're home. Yes, even if the sunset is *really* good.

WHEN IN DOUBT, OPEN THE OFFICIAL APP AND CHECK IT YOURSELF.

OH, CRAP. SOMETHING WENT WRONG.

Now what?

A scam is annoying at home. It's considerably more annoying when you're thousands of miles away with 12% battery. Act quickly, but don't panic.

STEP 1

Stop communicating with the suspicious person and don't make more payments. Disconnect from suspicious Wi-Fi and unplug unfamiliar cables and/or devices.

STEP 2



If you shared banking or card information, contact your bank or provider immediately using the number in its official app or on your card.



If you shared a password, change it anywhere you've reused it and enable MFA. Prioritize your email account.



If your phone or laptop was lost or stolen, use device-finding to locate, lock, and/or remotely erase it. Contact your mobile provider if your phone or SIM is involved.



If a booking account was compromised, contact the booking provider through its official app or website and check for unauthorized changes.

STEP 3

Check important bookings and financial accounts for anything unusual and **tell your travel companions** what's happened, especially if it could affect them too.

STEP 4

Report fraudulent accounts, listings, messages, or other instances of fraud or theft to the appropriate authorities. Save messages, emails, transaction information, screenshots, and other evidence.

In the US, report fraud at ReportFraud.ftc.gov and internet crime at ic3.gov

STEP 5

Get back to enjoying your trip. Preferably somewhere with a cocktail and absolutely no QR codes.