Safe travel includes protecting your identity.

Vacation tips to guard your most valuable asset

16.7 million people became victims of identity theft last year. [1]

1 in 4 Wi-Fi hotspots can be hacked in minutes, [4] yet **82%** of travelers access public Wi-Fi abroad. [5]

23% of U.S. consumers know a victim of travel identity theft. [2]

$16.8 billion dollars per year in fraud losses are due to identity theft. [3]

55% of travel identity victims spend weeks to more than a year working to resolve issues. [6]

Plan & Prepare

Documents: Scan important travel and identification documents and store them in a secure online repository or with trusted family in case they are stolen or lost.

Get alerts: Register in the Smart Traveler Enrollment Program for government warnings.

Financial safety: Take only one or two credit (NOT debit) cards and remove other info from your wallet. Update banks and credit card issuers with travel plans and activate fraud alerts. Do not carry a lot of cash and leave checkbooks at home.

Mobile phone: Turn on password protection or biometric authentication. Turn off automatic Wi-Fi and Bluetooth. Disable file sharing. Backup photos and data. Clear browser history. [8]

Bag tags: Write name and phone number only on luggage tags—not your home address.

Mail: Place a postal hold on your mail delivery at your post office or online.

Home: Make it look like someone is home by asking someone you trust to pick up deliveries and activating a few lights with random timers.

RFID wallet: Protect RFID chip-enabled credit cards and passports from unauthorized scanning with an RFID-blocking wallet or document sleeve. [7]

Stay safe while traveling

Pickpockets: Wear a hidden money belt or travel wallet for cash, cards and passports. Bags should have sturdy straps across the chest. Don't wear flashy, expensive jewelry.

Safes: Place cash, credit cards and passports in hotel safe whenever not in use.

Hotel scams: Do not give credit card info to callers claiming to be from the "front desk" [9] or restaurants who slip "menus" under your hotel room door. [10] Both could be scammers.

Public Wi-Fi: Avoid public computers (including the hotel business center) to access anything sensitive. Do not connect your mobile devices or laptops to free, public Wi-Fi.

Social media: Don't post vacation photos or status updates that reveal you're away from home.

ATMs: If you must get cash while traveling, only use ATMs at banks to avoid card skimmers. [11]

How to get help

Suspect you're a victim of identity theft?
Many providers such as insurers, banks, credit unions and employers offer identity management services from CyberScout for low or no cost. Call your providers today.

CYBERSCOUT®
WE'LL TAKE IT FROM HERE™

[1] "2018 Identity Fraud: Fraud Enters a New Era of Complexity," Javelin Strategy & Research, February 2018 . [2] "Avoiding Summer Identity Theft: 5 Must-know Steps," Experian, June 15, 2017. [3] "2018 Identity Fraud: Fraud Enters a New Era of Complexity," Javelin Strategy & Research, February 2018 [4] "1 in 4 Wi-Fi Hotspots Just Waiting to Be Hacked," Kaspersky Lab, November 24, 2016. [5] International Travel Report, Kaspersky Lab, June 2016. [6] Survey for Experian conducted by Edelman Intelligence, March 2017. [7] "RFID Pickpockets—Stop 'em with RFID Blocking Gear," Corporate Travel Safety Blog, October 18, 2017. {8} "3 Eco-friendly Hacks to Protect Your Online Identity While Traveling," Blueandgreentomorrow.com March 2018. [9] "Avoiding Unexpected Costs and Identity Theft on Your Spring Getaway," WTNH Connecticut, February 2, 2018. [10] "Don't Fall for These Three Hotel Scams," TripSavvy, June 1, 2017. [11] "Protect Yourself from Identity Theft When Traveling," Kiplinger, May 23, 2017.