Safe Travels

Security tips for today's challenges

By Vikki Moran

Balancing convenience and security are daily pursuits, but when you are vacationing, you really want the peace of mind that security brings you. Nothing can ruin a trip like costly fraud or theft. Safeguarding your personal information may seem daunting, but these steps can help.

Scammers Ready to Set You Up on Social Media

Per JP Morgan Chase Bank, "Scammers have set up shop on social media selling items and tickets for what looks like a great deal."

If a deal is too good to be true, it probably is. Social media is great for keeping current on people and places, but never buy directly from one of these platforms. Use only trusted sites to book trips, or purchase and plan your trip with a travel agent.

Expedia, Hotels.com and Trivago are reputable examples of online resources. Costco Travel and AAA provide easy-to-access travel agents if you do not already have a preferred one in your area. Contact your credit card company, too, as many offer booking services.

Cellphone Dangers

Are you using your cellphone while traveling abroad?

If so, make sure your phone has facial verification. This biometric ID is a great way to ensure only you have access to your most precious information. For banking or credit card apps, you can establish this security preference in the application settings and within the security settings of your device.

The ID process is simple: By uploading a government-issued ID, taking a selfie and providing other identifying credentials, you will be more secure in no time. Both Apple and Samsung phones offer excellent security. Check out what your cell company provides in the way of facial recognition.

Password Protection

Unique passwords are important.

Nearly 90% of Americans think that using unique passwords is essential; however, few people actually do. They reuse the same passwords repeatedly for many online platforms. Change your passwords regularly and vary them across different sites.

There are excellent programs that keep track of your passwords for you. Some, such as Bitwarden and LastPass, have free versions. Subscriptions such as Dashlane or 1Password are easy to use, but there are many options out there, so check them out carefully before selecting one.

Avoid Public Wi-Fi

Hackers take full advantage of public Wi-Fi. Lax security precautions in many publicly available networks allow hackers to steal your personal information and passwords. As a safer alternative, use mobile data or your hotspot.

Airports, hotels and entertainment venues are also easy targets for theft. Carry your chargers and USB cables with you. Do not use any offered at no charge. By plugging into an unknown cord, you are helping would-be thieves access your phone and all the information stored in the websites and applications you have used.

USB cords and device chargers are relatively easy to store in your carry-on bags and can offer you peace of mind. Some luggage companies, such as eBags, even sell small cord cubes for easy carry-on storage.

Beware of QR Codes in Public

QR codes can be little doorways to your precious data that you unknowingly open to fraudsters. Fraudulent codes are designed to make you think you are grabbing information for your trip, but instead, hackers gain access to your financial accounts.

The FBI says cyber thieves are now replacing legitimate codes by pasting professional-looking fakes over them. AARP recently shared that the FBI advises people not to download a QR code scanner because most phones today have a built-in scanner in their cameras. There is no need for anything else.

Place Fraud Alerts on Banking Sites

This service allows you to set a dollar amount or track every time your bank accounts are accessed. When traveling, you need to know if anything or anyone is accessing your funds while you are off enjoying yourself. I've set my preferences to alert me whenever a charge of more than $100 is processed for both my checking and savings accounts. You can change your notification limit setting when you get home.

Check your most used sites to see if they allow a verbal password. Verbal passwords are much safer than typed alphanumeric passwords.

Set spending thresholds on your credit cards when traveling. You can always call and extend them, if necessary, but chances are you will know your travel budget and can set reasonable safety stops.

Road Trip Tips

Check out what skimming devices look like before setting out on the road. If you pull into a gas station with suspicious-looking devices on the pump, be safe and move on to the next station.

Tap, don't swipe, your credit card. If tapping is possible—and most times it is—use it. Tapping and not sliding helps avoid card scamming. Europe and parts of Asia have been far ahead of the United States with this technology and have been tapping at merchants for many years.

Always squeal on the bad guys. If you receive phishing or scam emails or texts, report them. The generated report blocks them. Use blocking devices and applications for scam calls, too.

Cash Is King

We are becoming a cashless society; however, when you travel, you may pay less if you use cash. Change your bills into the local currency before you leave for any overseas travel. Airport kiosks are safe but costly. Store your cash safely on your body, and never carry all your money in one spot.

Split any cash you carry with travel companions. Pickpockets are still prevalent in tourist areas. Better yet, take only a little money. If discounts tempt you on a purchase, go to a reputable ATM with the logos you use at home, and remove what you need to complete your transaction. ■

ADOBE STOCK PHOTO BY WESLEY JVR/PEOPLEIMAGES.COM