A CYBER-SAFE ADVENTURE

A review of the latest security threats and how you can avoid them

THIS MONTH'S TOPICS:

There's a lot that goes into planning and having a successful vacation. Finding the right location, setting the time, booking the lodging, and purchasing the airfare tickets will set the stage for the journey. With all this preparation required, scammers see their opportunity for a costly trick at our expense.

During your trip, cyber threats don't disappear. What we post, whom we interact with, and what we connect with can all become a vulnerability if safeguards are not followed.

This doesn't mean we should be fearful of planning and partaking in a well-deserved vacation. It just means we need to keep cybersecurity in mind during these times and never let our guard down. This month's newsletter can help those with wanderlust stay cyber-safe during a vacation of a lifetime.

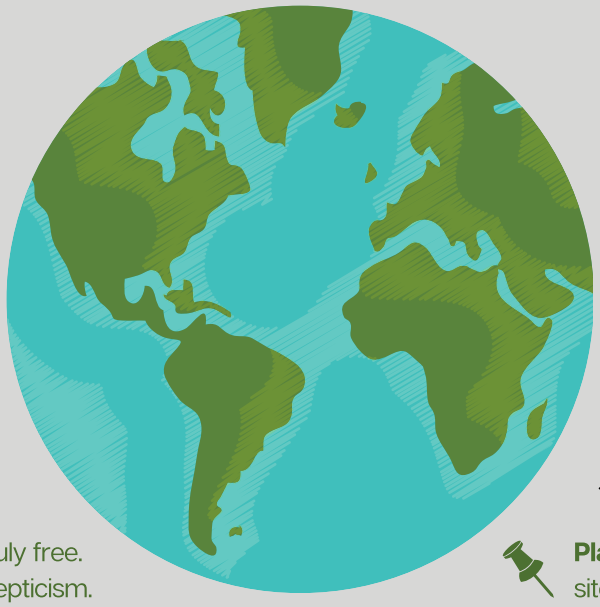
The Most Common Travel Scams

If we don't learn from history, we are doomed to repeat it. Take note of some of the common travel scams and how they can be avoided for your next adventure.

The Free Trip

Free trip scams are common. Some may actually have a trip to offer, but require you to pay fees, enroll in a bogus club or listen to a sales pitch. Other offers are created by scammers intended to get your sensitive information or trick you into clicking a malicious link.

Be Smart! - Most free trips aren't truly free. Treat these "deals" with extreme skepticism.



The "Too Good to Be True" Rental

Scammers have been known to take advantage of vacation home rental sites. They'll place a beautiful home with all the bells and whistles for a cheap nightly price. The cons could include a bait and switch to a far less perfect location or may just be an effort to steal your information.

Plan Wisely - Always use reputable listing sites and read reviews carefully.

Pickpocketing

Pickpocketing can ruin a trip in a matter of seconds. Those who have mastered the craft can perform their theft without you even noticing. Not only can a thief walk away with your money, but a stolen credit card, phone, or passport can be much more damaging.

Protect it! - Keep your unnecessary travel items at home, or locked in a safe back at your hotel.

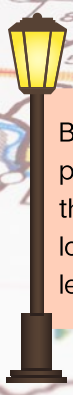
Skimmers are commonly found at gas stations and ATM terminals

Navigating Skimmers

Skimmers are malicious credit/debit card readers disguised as real payment terminals that can record and transmit card data to send to the installing criminal.

To spot a skimmer, look for signs of tampering such as:

- A broken security seal
- Bulkiness around the card reader or pin-pad
- Loose attachments



Because they generally require some physical alteration to the original machine, they are more commonly found in locations where the criminal would find less observance of their actions.

To protect yourself from a skimmer, try:

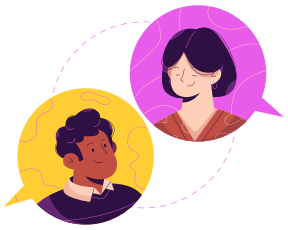
- Paying with cash at a gas station
- Using credit features instead of debit
- Use payment machines closer to the main building
- Monitoring your bank accounts monthly or set up alerts for unusual daily spending

Creating Your Cyber-Safe Travel Checklist

Creating a checklist can be a great way to stay on target for your trip. Why not take this approach and extend it to cybersecurity?

Book the Trip

Watch for scams like offers for a free trip or suspicious vacation home rentals.



Request Time off From Work

Talk with your supervisor if your planning on working while traveling.

Arrive at the Airport

Use a verified and secure Wi-Fi connection, pack a mobile hotspot or check if your phone can become a hotspot.

See the Sights

Pay with your credit card or with cash when possible. But keep your belongings close or in a safe.

Enjoy the Trip of a Lifetime!

Although tempting, avoid posting about your trip on social media until you return.

SCAM OF THE MONTH

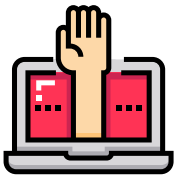
Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Mina was traveling abroad and enjoying a life-changing cultural experience. She was always on the go, taking in all the city sights she could see while updating her blog along the way. To make her blog upload efforts easier, Mina set her phone up with the Auto-Connect feature so she could automatically connect to any Wi-Fi network that she'd previously connected to. Mina took a break at a Sam's Cafe and her phone connected to the "SamsCafe" network. She began updating her blog then realized she needed to check her bank balance. She used her phone and logged into her bank's mobile website to review her balance. A few hours later, Mina received a message from her bank that her account had insufficient funds and it had been wiped out earlier that day.

Did you spot the red flags?

- Mina turned on Auto-Connect in an effort to save time accessing the internet.
- Mina connected to her banking portal while on an unsecured Wi-Fi network.
- Mina failed to verify the legitimacy of the Wi-Fi network she was connecting to.

Avoid Auto-Connecting/Auto-Joining free Wi-Fi networks. This feature works by having your device remember a specific SSID (Service Set Identifier). Scammers can create their own fake Wi-Fi networks and set their own SSIDs to mirror the account they are mimicking. So, your device will be connecting to a verified SSID but it will be one owned and managed by the scammer.



This is an example of a Man-In-The-Middle Attack where an attacker uses their technology to position themselves between their victim and the platform they are connecting to. By remaining in the middle, the attacker can watch, record and manipulate their target's activity, without them knowing. Thus, the websites visited and passwords entered can be easily observed or the attacker could direct their victim to a malicious webpage.

Protect Yourself

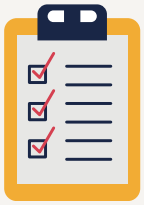
1. Try using a VPN (Virtual Private Network) to help create a secure connection.
2. Use legitimate Wi-Fi connections that you can verify.
3. Set up Two-Factor Authentication on critical accounts.

Even with these additional security layers, the best approach is to avoid accessing sensitive accounts and information when on a public Wi-Fi connection.

Pack an Extra Pair of Security!

Key Takeaways

Take scammers out of the equation when traveling. Be aware of the possible threats before, during and after your trip and make sure your entire traveling party is following the same safeguards.

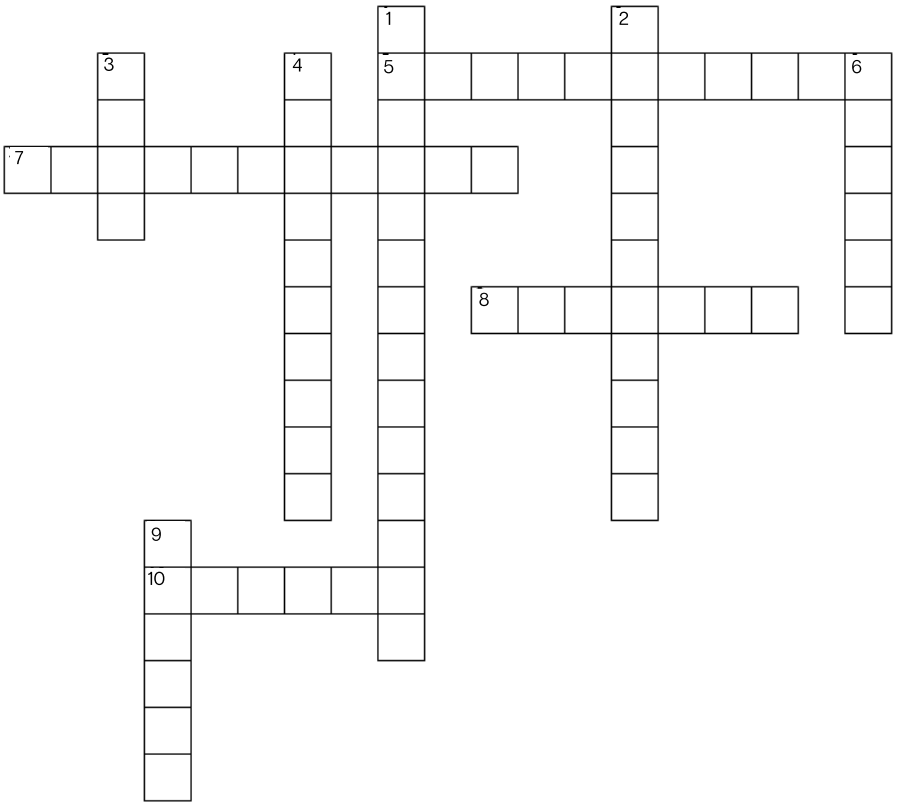


Think through your travel checklist and prepare for the tricks along the way. Make sure your travel companions are aware and following the same guidelines too.

Watch for skimmers. These malicious card readers can record your card data for a criminal. Check for signs of tampering anywhere you can swipe your card.

Protect yourself from free Wi-Fi vulnerabilities. Avoid using the Auto-Connect features and take additional precautions such as 2FA and use VPN connections.

A Cyber-Safe Travel Crossword



ACROSS

5. Avoid allowing your devices to do this on free Wi-Fi networks.
7. Avoid this when traveling, especially with unnecessary electronic devices.
8. Malicious credit/debit card readers disguised as real payment terminals.
10. These alternatives to hotels are popular among travelers but watch for deals that are too good to be true.

DOWN

1. This attack involves a scammer positioning themselves between their victim and the platform they are connecting to, watching their activity.
2. Avoid updating this during your trip, wait till after you return.
3. Be skeptical when trips are offered at this rate.
4. This type of physical theft can be done without you even noticing.
6. This activity is meant to be fun, but could be risky if you're not cyber-safe.
9. Paying with this type of card generally means more fraud protection benefits.

Answers: 1. MainTheMiddle 2. SocialMedia 3. Free 4. PickPocket 5. AutoConnect 6. Travel 7. Overpacking 8. Skimmer 9. Credit 10. Rental