Monthly Cybersecurity Tips Newsletter
VOLUME 17, ISSUE 6 • 2022

Cyber-Safe Travel

From the desk of Karen Sorady
MS-ISAC VICE PRESIDENT, MEMBER ENGAGEMENT

Summer is a popular time to travel whether it be for a relaxing overnight or a week away exploring a new destination. You are likely taking along that smartphone or other device to assist with directions, locating or identifying points of interest, and capturing that special photo. Practicing good cyber hygiene before, during, and after your trip will help secure your devices and allow you to connect with confidence when you're away from home.

***Quick note if you are traveling with business equipment**: It's best that you leave your work devices behind, however, if you can't leave home without them, ensure that you are following your organization's policies and procedures for protecting the devices and the information they contain while traveling.*

Before You Travel

Update your devices. Updating devices will fix security flaws and help keep you protected. Whether it's your computer, smartphone, or gaming device, be sure to update your operating system, applications, antivirus and malware software, and the like. If you haven't already turned on automatic updates, now is a good time to consider doing so.

Back up your devices. Back up information such as contacts, financial data, photos, videos, and other data in case a device is compromised during travel and you have to reset it to factory settings.

Lock your device. Make sure to lock your device when you are not using it. Set your devices to lock after a period of time and use strong PINs and passwords.

Enable multi-factor authentication (MFA). Add an extra layer of protection so that the only person who has access to your account is you. For more information on MFA, see https://www.cisa.gov/mfa.

During Your Travel

Guard your devices. Your devices are valuable, but your sensitive information is as well. Always keep your devices close at hand and secure in taxis, security checkpoints, airplanes, rentals homes, and hotel rooms.

Securely recharge. Never plug your phone into a USB public charging station, such as those in the airport or in hotel room lamp or clock radio inputs, as these cannot be trusted. Malicious individuals can hijack your session or install malware on your device through those seemingly-harmless means. Always connect using your own power adapter connected to a power outlet.

Delete data from your rental car. If you connect your phone to a rental car for navigation or other purpose, be sure to securely remove the device so that other individuals do not have access to your address book, device name, text messages (hands free calling), or other sensitive information.

Avoid public Wi-Fi. While public networks are convenient, they are a security risk. Avoid connecting to public Wi-Fi unless absolutely necessary. Instead, consider using your phone carrier's internet connection or use your phone as a personal hotspot if your plan allows.

If you do need to connect to public Wi-Fi, verify with the establishment the name of the network and use a virtual private network (VPN), software that will encrypt your internet traffic and prevent others from stealing your data. Verifying the network name is important as often times malicious individuals create similar connection points with a slight misspelling, hoping you will instead connect to their network.

Turn off auto connect. While auto connect is enabled, devices will seek out and connect to available networks or Bluetooth devices. This could allow cyber criminals to access your device without you knowing it. Disable auto connect, Bluetooth connectivity and near field communication (NFC), like airdrop, so that you can select the network and you can control the connection.

Limit what you share. Limit the information you share on social media while on vacation and consider posting updates about your trip after you return. Revealing too much information while away can put you and others at risk. Criminals can gain useful information from such posts, like knowing you are away from your home. Scammers may even attempt to contact your family and friends with a variety of scam tactics. Additionally, consider setting your social media accounts to only allow friends to view your posts.

Avoid the use of public computers. Public computers such as hotel business centers and internet cafes are often poorly managed and provide minimal security protection for users. If you must use a public computer, do not enter any username or password on the computer and do not connect or transfer data via thumb drive/USB.

When You Return Home

Shred your boarding pass and luggage tag. Scannable codes on boarding passes and luggage tags include full name, date of birth, and passenger name record. These can also contain sensitive data from your airline record, like passport number, phone number, email address, and other information that you wouldn't want to share publicly. For this same reason, never post boarding passes on social media.

Scan for virus and malware. It's best to update your security software when you return home and scan for virus and malware to be sure your device has not been compromised while you were away.

Conclusion and Resources

Knowing these helpful tips will aid in cyber-safe travel, allowing time to relax and enjoy your time away. For more information, see the additional resources below.

- FFC | Cybersecurity Tips for International Travelers
- CISA | Cybersecurity While Traveling Tip Card (PDF)
- National Cybersecurity Alliance | Cyber Trip Advisor: Vacation Travel Security Tips (PDF)

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.