July 2018
Volume 13, Issue 7

Sun, Sand, and Cybersecurity

From the desk of Thomas F. Duffy, MS-ISAC Chair

This month, in partnership with the National Cyber Security Alliance, we aim to provide some valuable tips on staying cyber safe while heading on a summer vacation. Whether you are out exploring or relaxing, it is important to strive to be as secure as possible with your digital devices and information. Unfortunately, travel can open you up to different points of vulnerability compared to normal everyday use at home, and we don't just mean accidentally going swimming with your cell phone. You see, while traveling you are operating outside of your normal, safe routines. This means using your devices on different networks and putting them down in different locations, including under your beach towel while swimming. By following some smart practices, you can connect with greater confidence during a summer escape.

Getting Ready to Go:

Avoid mayhem and make magical family memories by taking a few simple cyber safety steps before you head out of town. The goal here is to prepare your devices for travel and to keep them from being used against you.

- **Keep a clean machine:** Before you hit the road, make sure all security and critical software is up-to-date on your mobile devices and keep them updated during travel. These protections are your best line of defense against viruses and malware.
- **Lock down your login:** Your usernames and passwords are not enough to protect key accounts like those you use for email, banking, and social media. Fortify your online security by turning on multi-factor authentication, commonly referred to as two-factor authentication, when available. This typically pairs your username and password (i.e. something you know) with a message sent to your phone (i.e. something you have) or your fingerprint (i.e. something you are).
- **Password protect:** Use a passcode or security feature like a finger swipe pattern or fingerprint to lock your mobile device. Also set your screen to lock after a short period of time by default. If you do choose to use a finger swipe, make sure it has at least one turn (preferably two) and that a pin code has at least 6 numbers!
- **Think before you use that app**: New apps are tempting! It is important to always download new apps from only trusted sources like the Apple App Store or the Google Play Store. Additionally, consider limiting your apps access to services on your device, like location services.
- **Own your online presence**: Set the privacy and security settings on social media accounts, web services, and devices. It is okay to limit how and with whom you share information – especially when you are away.

While on the Go:
Once you and your gang are at your destination, you are in new territory and are facing new potential cyber threats. Here are some ways you can keep up secure practices while out and about.

- **Get savvy about *what you do* on other peoples' Wi-Fi and systems:** Do not transmit personal info or make purchases on unsecure or public networks. Instead, use your phone carrier internet service for these needs. For laptops/tablets, it is easy to use your phone as a personal hotspot to surf more securely using carrier data. Also, never use a public computer or device to shop, log in to accounts, or do anything personal.
- **Turn off Wi-Fi and Bluetooth when idle:** When Wi-Fi and Bluetooth are on, they may connect and track your whereabouts. Only enable Wi-Fi and Bluetooth when required, and disable your Wi-Fi auto-connect features.
- **Protect your $$$:** Be sure to shop or bank only on secure sites. Web addresses with 'https://' and a lock icon indicate that the website takes extra security measures. However, an "http://" address indicates your connection is not secure (not encrypted) and you should not transmit payment or sensitive information over to such a site.
- **Share with care:** Think twice before posting pictures that signal you are out of town. Knowing you are away from home is a great piece of information for a criminal to have and they may target your home for physical crime. Also consider limiting your social media apps' access to location services on your device, and omit location information while making your posts and sharing your pictures.
- **Keep an eye on your devices:** Laptops, smartphones, and tablets are all portable and convenient, making them perfect for a thief to carry away! Keep your devices close to you and hold onto them if strangers approach you to talk, as a common scam consists of a stranger distracting you and placing a map or newspaper over your device and walking away with it when finished talking.
- **Know your destination's laws:** If you are heading out of the country, check up on any specific laws on internet and device usage. Additionally, bring as few devices as possible and consider using a device specifically purchased for international travel.

Armed with these tips and practices, you should have a happy and cyber safe vacation ahead of you. To learn more about staying cyber safe and secure while travelling, head to the MS-ISAC's Security Primer covering this topic. For more information on NCSA, including countless resources on staying cyber secure, please visit staysafeonline.org.