June, 2017
Volume 12, Issue 6

Sun, Sand, and Cybersecurity

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

School's out and the beach and mountains are calling. It is that time of the year when so many of us pack our bags and hit the open road or head to the airport for a well-earned vacation. We may be ready to take a break from our normal lives, but we still need to be cyber secure while we are enjoying our time off! In this month's edition, we will explore some ways to be safe and smart with our devices, Internet usage, and social media while out travelling on vacation.

Stop-Think-Share

Always be careful about how much you post on social media about your vacations before and during your travels. Criminals can and do watch online posts to find people that are on vacation because that means you have left your home unattended. Before "checking in" to a location on a social network, consider what else you are sharing – like the information that you aren't home. Consider skipping the "check in" and making your vacation posts after you have gotten back. This is another way people can see you aren't home. Perhaps this will have the double benefit of letting you take the time to choose only the best photos to post after your trip is over! At the very least, consider using privacy settings that only let friends see your posts. Additionally, consider turning off GPS and auto-tagging/auto-check in features, if you have them enabled.

Disable WiFi auto-connect services

Some devices have an auto-connect feature that will search for and automatically connect to available and accessible WiFi networks without your interaction. This can allow your device to automatically connect to an unencrypted, public WiFi network, or even one that was set up by a malicious actor to eavesdrop on your browsing and connection activity.

If you want to connect to a store or hotel's network, check with an employee to see what the correct network is called, and see if they can provide a network password for a more secure, encrypted network. Always use a secure, encrypted network that requires login credentials if you have the option. In the event that isn't an option, and you can use your phone as a WiFi hotspot, use that instead to get a more secure connection for another device that can't make direct use of the cellular network's connection.
Additionally, make sure you do not choose to "remember this network" or "join this network automatically" once you have settled on a more trusted network for use during your vacation. If you have these settings switched on for a very generically named network, your device may connect you to a less secure one that happens to have the same name. Even if you have this turned off, there's another setting that will automatically connect you to a network you have joined before, which can be a problem

since your device doesn't know the difference between your coffee shop's "Guest" network and a malicious "Guest" network. Turn these settings off so you don't automatically connect, and choose to connect only to more trusted, safer WiFi networks.

Keep your devices close, and keep them locked when not in use!

Whether it's your laptop, tablet, or smartphone, be sure to keep your device on you or with someone you trust. Never leave a device unattended in an airport, train station, restaurant, hotel lobby or anywhere else in public while travelling. There is a common scam that targets people who leave devices sitting next to them. In this scam, another traveler will approach you and ask for help and then lay a newspaper or map down over your device. While you're distracted answering their question, they are picking up and pocketing your device under the cover of the newspaper or map!

Set a strong password: *Use at least 8 characters in upper and lower case, numbers, and symbols*
Set a strong pattern lock: *Use at least 7 points and double it back over itself with at least 2 turns*

MS-ISAC
Multi-State Information Sharing

STOP | THINK
CONNECT