June 2019
Volume 14, Issue 6

Staying Cyber-Safe on a Summer Vacation

MS-ISAC Multi-State Information Sharing & Analysis Center

Enterprise Information Security Program

Tacoma

From the Desk of Ron Jimerson, Chief Information Security Officer

Typical travelers heading out on their summer vacation check that they have the right supplies and clothes for their trip before they hit the road. *Expert* travelers will be also checking to ensure they are educated and prepared to be cyber-safe with their devices and data while on the road! Thinking of your smartphones and devices as being just as important as your wallet is a proper step in the right direction. These devices contain everything from your banking and payment information to your treasured family photos, and ensuring they are secure and protected when away from home is paramount. In partnership with the National Cybersecurity Alliance (NCSA), we have put together some key tips, strategies, and resources to aid you in being secure during your travels.

To do before your trip:

Update your devices: One of the simplest and effective ways to stay cyber-secure is to continuously update your devices. Those updates don't just contain new features, but fix security flaws and keep you protected!

Password/Passcode protect your devices: Always establish a strong passcode with at least 6 numbers or a swipe pattern with at least 1 turn of direction when protecting the lock screen of your smartphone. On laptops, a minimum of an 8-character password or phrase is recommended including uppercase and lowercase letters, special characters, and numbers.

Set your device to lock after an amount of time: Once you have the passcode, password, or swipe pattern established, you should set an automatic device lock prompting for the access code after a specified time of inactivity. This will prevent a criminal from getting onto your device if you accidentally leave it unlocked.

Book your trip with trusted sites: When planning your trip and booking transportation, lodging, and experiences, it is important to complete those transactions with trusted, known businesses. If possible, double check the reviews and reputation of a site you are unfamiliar

with, but are considering to use for your booking. By sticking to reputable sites, you guarantee a higher standard of security for your data and transaction.

Staying secure and connected during your trip:

Keep track of your devices: Not only are your devices themselves worth a great deal of money, but your sensitive information that is accessible by that device is also valuable. Ensure you keep your devices close at hand or secured away safely when not in use. Theft of mobile devices, from smartphones to tablets and laptops, is all too common and can spoil a fun trip to a great extent.

Limit your activity on public Wi-Fi networks: Public Wi-Fi that does not require credentials or logging in is not protected by encryption, so browsing and activity is not secure from prying eyes. To ensure your information is not put at risk, avoid logging into your personal accounts or making transactions while on public or hotel networks.

- Use your phone carrier's internet connection, or use your phone as a personal hotspot (if your cell carrier's plan allows) when logging into personal accounts or conducting transactions.
- Ensure your device is set to ask your permission before connecting to a wireless network while on your trip.
- If you intend to use a hotel or establishment's customer wireless network, verify what network is the correct one to use with a member of the staff.

Don't overshare on social media: Consider posting updates about your trip after you return. Criminals may see you are away from home based on social media content and attempt to steal from your home! If you also share too many details about where you are on your trip, some scammers may 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 and content.

Allowing apps to use your phone's location services has its own privacy concerns, as the app is likely recording or using that data, and may automatically add geotagging to social media interactions in that app as a result! Three popular methods of location sharing are geotagging (adding a location tag to a social media post or picture), posting a photo in which the background can be easily identified (like Times Square or the Eiffel tower), or "checking in" at a business.

By following these tips and being a cyber-safe traveler, you will have a smooth and enjoyable vacation! There are more resources available from NCSA and our partners on staying secure on trips and at home, check them out below to learn more:

https://staysafeonline.org/blog/top-tech-tips-for-cybersafe-summer-travel/

https://www.cisecurity.org/newsletter/securing-devices-by-making-simple-changes/

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.