OUCH! December 2021

Top Cybersecurity Tips For Vacations

Overview

As the holiday season approaches, millions of people will be traveling. If you are among the many, here are some tips to help keep you cyber savvy and safe.

- **Mobile Devices**: Bring as few devices as you can. The fewer devices you bring while traveling, the fewer devices that can be lost or stolen. In fact, did you know that you are far more likely to lose a mobile device than have it stolen? Whenever leaving a hotel room, restaurant, taxi cab, train or airplane, do a quick device check and make sure you have all of your devices. Don't forget to have friends or family traveling with you to double check for their devices too, like children who may leave a device behind on a seat or in a restaurant.

  As for the devices you choose to bring, make sure you update them so they are running the latest operating system and apps. Keep the screen lock enabled. If possible, ensure you have some way to remotely track your devices if they are lost. In addition, you may want the option to remotely wipe the device. That way if a device is lost or stolen, you can remotely track and/or wipe all your sensitive data and accounts from the device. Finally, do a backup of any devices you take with you, so if one is lost or stolen, you can easily recover your data.

- **Wi-Fi Connections**: When traveling, you may need to connect to a public Wi-Fi network. Keep in mind you often have no idea who configured that Wi-Fi network, who is monitoring it or how, and who else is connected to it. Instead of connecting to a public Wi-Fi network, whenever possible connect to and use the personal hotspot feature of your smartphone. This way you know you have a trusted Wi-Fi connection. If that is not possible and you need to connect to a public Wi-Fi network (such as at an airport, hotel, or cafe), use a Virtual Private Network, often called a VPN. This is software you install on your laptop or mobile devices to help protect and anonymize your Wi-Fi connection. Some VPN solutions include settings to automatically enable the VPN when connecting to non-trusted Wi-Fi networks.

- **Public Computers**: Avoid using public computers, such as those in hotel lobbies or at coffee shops, to log into any accounts or access sensitive information. You don't know who used that computer before you, and they may have infected it accidentally or deliberately with malware, such as a keystroke logger. Stick to devices you control and trust.

- **Social Media**: We love to update others about our travels and adventures through social media, but we don't always know who every friend or viewer is online. Avoid oversharing while on vacation as much as possible and consider waiting to share your trip until you're home. Additionally, don't post pictures of boarding passes, driver's licenses, or passports as this can lead to identity theft.

- **Work**: If you will be working while on vacation (we hope not!), make sure you check what your work travel policies are ahead of time, including what devices or data you can bring with you and how to remotely connect to work systems safely.

Vacation should be a time for relaxing, exploring, and having fun. These simple steps will help ensure you do so safely and securely.

Guest Editor

Princess Young is a Senior Analyst at Southwest Airlines and leads the cybersecurity education and training efforts for 60,000 employees across the country. Princess enjoys engaging with employees so they can feel empowered to share the responsibility of cybersecurity, regardless of their role or title.

Resources

Securing Your Mobile Devices: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
The Power of Updating: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Virtual Private Networks: https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
Got Backups: https://www.sans.org/newsletters/ouch/got-backups/