OUCH! June 2024

SANS SECURITY AWARENESS

Going on Vacation? Simple Steps to Make it Cybersecure

Overview

The summer season is upon us, and soon millions of people will be traveling all over the world. If you are going on vacation, here are some travel tips to help keep you cyber savvy and safe.

Mobile Devices

Avoid overpacking: Only bring the mobile devices you need when going on vacation. By mobile devices, we mean devices including laptops, tablets, smartphones, smart watches, eReaders, and portable gaming devices. The fewer devices you bring, 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 you are to have it stolen? Quite often just keeping track of your devices can be your biggest challenge. Create a habit that whenever you leave a hotel room, restaurant, taxicab, 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 -- especially children who may leave a device behind on a seat or in a restaurant.

As for the devices you do bring, make sure you update the operating system and apps before you leave so that they are running the latest versions. Often the simplest way to do this is to enable automatic updating on the device. This ensures that your devices have any vulnerabilities patched and are running the latest security features. Keep the screen lock enabled, and if possible, ensure you have some way to remotely track your devices if they are lost. In addition, you may want to enable 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 that if one is lost or stolen, you can easily recover your data.

Wi-Fi Connections

When traveling, you may want to connect to a public Wi-Fi network. Examples of public Wi-Fi networks include the free Wi-Fi networks at the airport, coffee shops, or at restaurants. Keep in mind, you often have no idea who configured a given 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, when possible, use the personal hotspot feature of your smartphone to connect your personal devices to the internet. This way you know you have a trusted Wi-Fi connection.

Another tip to reduce the amount of data you use on your vacation is to download what you need at home before you leave for your trip. This can include downloading versions of maps to easily navigate your destination offline in your preferred navigation app or downloading any digital entertainment beforehand such as audiobooks, eBooks, games, or movies.

Public Computers

Never use 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 that computer accidentally or deliberately with malware, such as a keystroke logger. Stick to your own devices that you control and trust.

Social Media

We all love to update others about our adventures through social media, but you don't know who will be reading all of your posts. Avoid oversharing while on vacation as much as possible and consider waiting to share your adventures until you're home from your trip. Also, don't post pictures of boarding passes, drivers licenses, or passports, as this can lead to identity theft.

Customs and local laws

Check the laws of the country you are visiting; your legal rights vary from one country to another. Content which may be tolerated at home may be illegal in another country. Know before you go.

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

Marisa Midler is a Cybersecurity Engineer in the CERT Division at the Carnegie Mellon University Software Engineering Institute. Marisa is a Certified Information Systems Security Professional (CISSP) and has earned degrees at Carnegie Mellon University (MS) and the University of Pittsburgh (BS/BA).

Resources

The Power Of Updating: https://www.sans.org/newsletters/ouch/power-updating/
Emotional Triggers – How Cyber Attackers Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
One Simple Step to Securing Your Accounts: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/