

Cyber Security and Your Summer Vacation



Enterprise Information Security Office Monthly Security Tips Newsletter

From the Desk of Deborah A. Snyder, Acting Chief Information Security Officer

The summer vacation season is underway and for many of us that means lounging on sunny beaches, reading a book under a shade tree, or hitting the road for a new adventure. It can also mean identity theft and other crimes if we aren't careful about our online activities and protecting our information. Cyber crime does not take a summer vacation; we need to remain vigilant. Fortunately, by following some best practices, we can minimize the risk of becoming the next statistic.

- **Save the Social Media Vacation Posts Until You Get Back Home**

It may be tempting to post details of where and when you'll be traveling. By revealing such specifics, you are providing information that could be used by criminals to target your home while you're gone. Another common scam involves compromising email accounts to contact your friends or family with requests for help, claiming that you were robbed while on vacation and need money. Sending private posts and photos during your vacation to family and friends is ok, but if you post them publicly, you increase the risk of someone using that information for malicious activities. Also, make sure your children understand what, and when, they should post or not post regarding your vacation plans.

- **Do Not Use Public Computers and Public Wireless Access for Sensitive Transactions**

Whether you're entertaining the kids by streaming a video on a tablet, downloading new travel apps on your smartphone, or even taking your tablet poolside, there are precautions you should take to make sure your personal information is safe.

Wi-Fi spots in airports, hotels, train stations, coffee shops, and other public places can be convenient, but they're often not secure and can leave you at risk. If you're online through an unsecured network, you should be aware that individuals with malicious intent may have established a Wi-Fi network with the intent to eavesdrop on your connection. This could allow them to steal your credentials, financial information, or other sensitive and personal information. It's also possible that they could infect your system with malware. Any free Wi-Fi should be considered to be "unsecure." Therefore, be cautious about the sites you visit and the information you release.

Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi. Also consider using a cellular 3G/4G connection, which is generally safer than a Wi-Fi connection.

- **Protect Your Smartphone, Laptop, or Other Portable Devices While Traveling**

Don't let your devices out of your sight. Just as your wallet contains lots of important and personal information that you wouldn't want to lose, so do your portable devices. Never store your laptop as checked luggage. If there is a room safe available at your hotel, use it to securely store your devices.

Make sure your laptop and other mobile devices have the latest anti-virus installed. Your device manufacturer should notify you whenever an update is available.

Use of security software is a must. Many of these programs can also locate a missing or stolen phone, tablet, or other similar device. These programs will back up your data and can even remotely wipe all data from the phone if it is reported stolen. Make sure you have strong passwords and encryption, where possible, on these devices in case they are lost or stolen.

For More Information

For more information about how to stay safe in cyberspace, visit the Enterprise Information Security Office at www.its.ny.gov/eiso.

Provided By:



The information provided in the 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.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.