July 2015
Volume 10, Issue 7

Sun, Sand, and Cyber Security

Clark County Information Technology

From the Desk of Louis Carr, Jr., Chief Information Officer

Every summer, vacationers put their house lights on timers and their mail on hold when they travel away from home. It's just as important when taking a vacation to take similar precautions with good cyber habits. Many cyber criminals specifically target travelers...

Criminals often set online lures to sell fake vacations or tickets. These may be just simple advertisements or sophisticated scams using realistic websites, complete with phone operators that will "assist" you.

Home Alone

Social media posts with pictures of tourist attractions may update your friends and family, but they also tell criminals that you're on vacation and your house is empty. Other older posts may contain personal details or pictures of your home, telling thieves what items of value are in the house or how to circumvent security systems.

Stolen "Keys"

Sensitive data, such as login names and passwords, are especially valuable to criminals. One way criminals obtain such data is by installing a "keylogger" on hotel public computers. The keylogger records every keystroke typed on the computer and then transmits that information to the criminal.

Missed Connection

Some cyber criminals specialize in "sniffing" the Wi-Fi and public networks in airports and coffee shops, allowing the criminal to collect and read all information sent over a wireless network.

Other criminals use a practice called "juice jacking", where the criminal rigs a public charging kiosk to siphon information directly from your device when you plug into it.

Who's the Boss?

The cyber security threat doesn't end with you; Social engineers often use information about a boss' vacation to gain physical access or commit financial fraud. The social engineer knows that they can reference the boss and the boss will not be reachable to verify whether he/she really did order the "repairman" or gave instructions for a fraudulent wire transfer.

When in Rome...

Different countries have different laws, which may allow government employees or law enforcement full access to your device without your knowledge or permission. Some countries are known to collect all data residing in that country, while others collect data

from devices left in hotel rooms. This may be very important in countries that do not have the same freedom of speech as the United States. Some of these countries are known to have jailed tourists who posted negative comments online about the government or who posted criminal activities online, such as the use of alcohol or drugs.

Luckily, with a little care it's possible to avoid these problems. Follow these simple tips to ensure that the only memories from your vacation are good ones:

Easy Tips to Protect Yourself

- Use discretion when posting personal information on social media. This information is a treasure-trove to social engineers. Do not post information about travel plans or details; save the pictures and updates until after you return home.
- Set email away messages to only respond to known contacts in your address book.
- Disable geo-locational features, such as automatic status updates and friend finder functionalities.
- Remind friends and family members to exercise the same caution.

Easy Tips to Protect Your Devices

- Keep your electronic devices with you at all times.
- Before traveling abroad, change all passwords that you will use while traveling, and upon return change the passwords of any accounts that were accessed while abroad. This includes passwords used by social media websites and email providers, for which you have automatic logins.
- Do not access sensitive accounts (e.g. banks, credit cards, etc.) or conduct sensitive transactions over public networks, including hotel and airport wi-fi and business centers, or Internet cafés.
- Use up-to-date anti-virus, anti-spyware, and anti-adware protection software; apply recommended patches to your operating system and software.
- Use wired connections instead of Bluetooth or Wi-Fi connections, whenever possible.
- Do not plug USB cables into public charging stations; only connect USB powered devices using the intended AC power adapter.
- Know the local laws regarding online behavior, as some online behaviors are illegal in certain countries.

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™

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.