U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

December 2017

Cybersecurity While on Holiday

Cybersecurity threats don't take a holiday when you do. If you're headed out of the office for an extended absence, be aware that cyber threats continue. In fact, some threats may be at an increased risk if you're outside of the familiar, protected environment of the office or home.

When traveling, you must take extra precautions to safeguard personal and sensitive information you carry inside your phone, laptop, and tablet. You can protect yourself and others by leaving any equipment that you won't need behind (just make sure it's secure where you leave it). If you do need to take your work-issued computer and personal internet-connected devices, be sure to add these to-dos to your travel preparedness list.

Bring and Use Your Own Power Adapters and Cords

It's never safe to charge your devices using anything other than your own power adapters. Cyber thieves may install malware onto hotel lamps, airport kiosks and other public USB charging stations. If you absolutely must charge your device on the road, and you don't have access to your charger/adapter, power down your device before you connect it into any airport chair or public USB charging station.

Back Up Your Electronic Files

Before you leave, back up your contacts, photos, videos and other mobile device data with another device or cloud service. And make sure your back-ups are encrypted and secure!

Install Security Updates and Patches

Be sure to patch and update operating systems and software (including mobile device apps). This should be a regular practice, but it is particularly important if you will be unable to update while traveling. Updates and patches can fix security flaws and enable security software to detect and prevent new threats.

Create New Passwords and Change Passwords

Change passwords you will use while traveling, and add multi-factor authentication, if possible. Don't skimp on password creation either—a numerical sequence is not ideal. Passwords should be at least 10 characters or longer with a combination of letters, numbers, and symbols. Consider using a passphrase – a combination of words that are easy to remember, such as "Mydogatemyhomeworkandgotindigestion". Once you're home, change your passwords again!

Lock Devices Down
Most smartphones, laptops, and tablets come equipped with security settings that will enable you to lock the device using a PIN or fingerprint ID. Do this on every available device. In the event you misplace or lose a device, this will be the first line of defense against a security breach.

Remove or Encrypt Sensitive Information on Mobile Devices
If you do not need to access sensitive information while traveling, don't bring it. But if you need the information while you are traveling, make sure sensitive information is encrypted. For example, laptops should have full-disk encryption.

Turn Off WiFi Auto-Connect and Bluetooth
Go into your device's Settings feature, and disable the WiFi auto-connect option so that you manually connect when it is safe to do so. Similarly, disable Bluetooth connectivity. If left on, cyber thieves can connect to your device in a number of different and easy ways.

Avoid Public WiFi
Avoid connecting to any public WiFi network. You didn't connect to the free, open WiFi on the airplane, so continue that mindset on the ground. Using your mobile network (like 4G or LTE) is generally more secure than using a public wireless network.

Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Always log into your work networks through VPN, and only use sites that begin with "https://" when online shopping or banking.

Ensure Physical Security of Your Devices
NEVER let your devices leave your sight. If you cannot physically lock devices in your hotel room safe or other secure place, take them with you. There are no good hiding spots in your hotel room! Many breaches occur because a device was left unattended when an opportunistic thief struck. When traveling with laptops and tablets, the best protection is to carry them with you. It's never safe to pack your devices in your checked luggage.

Create Unique PINs
Don't use the same PIN for the hotel safe and a mobile device, especially one that you're storing in the hotel safe! Do you really want to make it that easy for a thief?

Use Geo-Location Cautiously
Most social media sites are happy to automatically share your location as you post photos and messages. This also tells thieves back home that you are away, which is a great time to break in. So, limit the information you post regarding your location at any point in time.

For HIPAA Covered Entities and Business Associates
The HIPAA Security Rule requires that covered entities and business associates conduct a risk analysis to identify risks and vulnerabilities and to mitigate identified threats and vulnerabilities.

Risks to ePHI created, received, maintained, or transmitted on workplace owned equipment, and personal equipment if permitted, when workforce members travel must be included as part of a covered entity's or business associate's risk analysis and risk management process.

The HHS Office for Civil Rights (OCR) web site provides guidance on the HIPAA Security Rule as well as guidance on specific cybersecurity topics. We recommend you bookmark these pages so you can refer to them easily whenever you have a question or need some guidance.

Bon voyage! And safe cyber travels.