TAKE CYBERSECURITY WITH YOU WHEN TRAVELING

In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When you are traveling, whether domestically or abroad, it is always important to practice safe online behavior and take proactive steps to secure internet-enabled devices. The more we travel, the more we are at risk for cyberattacks. Whether traveling with personal or business devices, you should always comply with user rules for international travel. Use these tips to connect with confidence while on the go.

KNOW YOUR CYBER BASICS

• "If You Connect IT, Protect IT." Whether it is your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software. • Back up your information. Back up your contacts, financial data, photos, videos, and other mobile device data to another device or cloud service in case your device is compromised.

• Enable multi-factor authentication (MFA). Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

• Know who to call for support. If you experience any system issues, you should know whom to call for IT support. If your device is compromised, you should have a plan on the actions you will take.

• Never click and tell. Do not tell the social media world that you are going to be away from your home. Disable geo-tagging and do not post your travel pictures on social media until you return from vacation. Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people do not realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you are not— at any given time.

• Stay protected while connected. Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—turn on your browser's advance FOLLOW-ON RESOURCES security settings and be sure to confirm the name of the network and exact login • Social Media procedures with appropriate staff to ensure that the network is legitimate. If you Cybersecurity Tip Sheet do use an unsecured public access point, practice good internet hygiene.