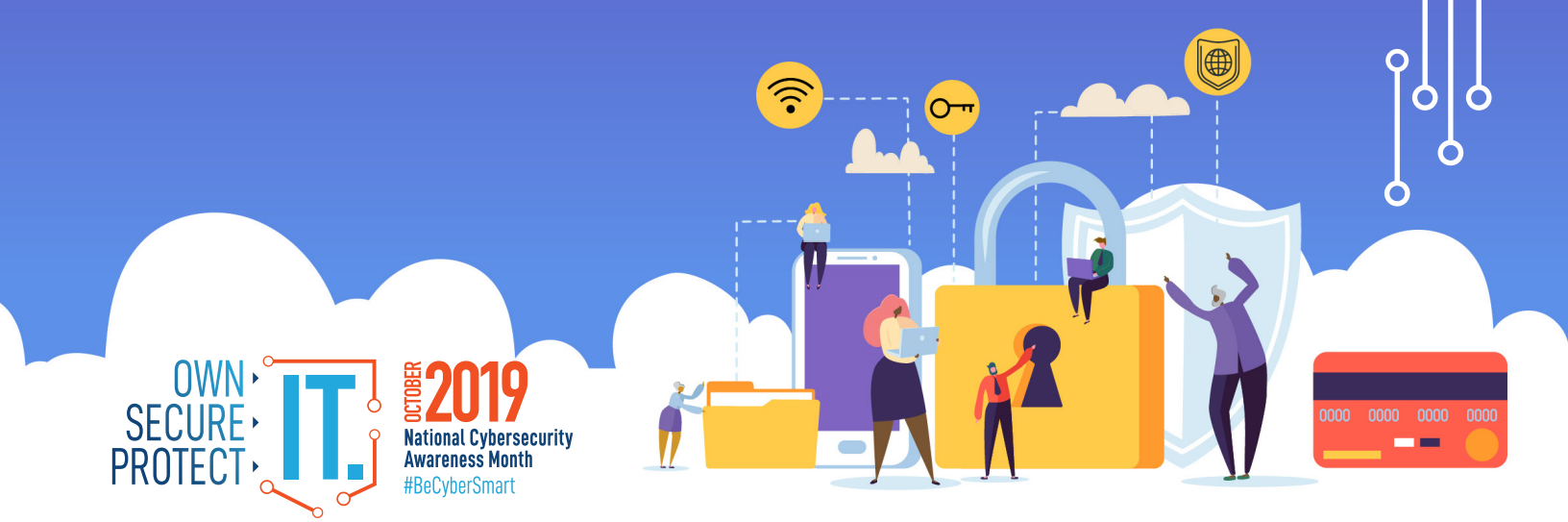

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

CYBERSECURITY WHILE TRAVELING

In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When you're traveling—whether domestic or international—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. #BeCyberSmart and use these tips to connect with confidence while on the go.

SIMPLE TIPS TO OWN IT.

Before You Go

- **If you connect, you must protect.** Whether it's 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. Read the Phishing Tip Sheet for more information.
- **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 and you have to reset it to factory settings.
- **Be up to date.** Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.
- **Keep it locked.** Lock your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or misuse your information. Set your devices to lock after a short time and use strong PINs and passwords. Read the Creating a Password Tip Sheet for more information.
- **Double your login protection.** 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. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.

During Your Trip

- **Stop auto connecting.** Some devices will automatically seek and connect to available wireless networks or Bluetooth devices. This instant connection opens the door for cyber criminals to remotely access your devices. Disable these features so that you actively choose when to connect to a safe network.

For more information about connecting with confidence visit: **https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019**

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

- **Stay protected while connected.** Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with "https://" when online shopping or banking.
- **Play hard to get with strangers.** Cyber criminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate—or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender. Read the Phishing Tip Sheet for more information.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that 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 aren't— at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.
- **Guard your mobile device.** To prevent theft and unauthorized access or loss of sensitive information, never leave your equipment—including any USB or external storage devices—unattended in a public place. Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.