CYBERSECURITY WHILE TRAVELING TIP CARD

Cybersecurity should not be limited to the home, office, or classroom. It is important to practice safe online behavior and secure our Internet-enabled mobile devices whenever we travel, as well. The more we travel and access the Internet on the go, the more cyber risks we face. No one is exempt from the threat of cyber crime, at home or on the go, but you can follow these simple tips to stay safe online when traveling.

CYBERSECURITY TIPS FOR TRAVELERS

Before You Go

- **Update your mobile software**. Treat your mobile device like your home or work computer. Keep your operating system software and apps updated, which will improve your device's ability to defend against malware.
- **Back up your information.** Back up your contacts, photos, videos and other mobile device data with another device or cloud service.
- **Keep it locked.** Get into the habit of locking 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 destroy your information. Use strong PINs and passwords.

While You Are There

- **Stop auto connecting.** Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to.
- **Think before you connect.** Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, train/bus station 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. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Only use sites that begin with "https://" when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.
- **Think before you click.** Use caution when downloading or clicking on any unknown links. Delete emails that are suspicious or are from unknown sources. Review and understand the details of an application before installing.
- **Guard your mobile device.** To prevent theft and unauthorized access or loss of sensitive information, never leave your mobile devices–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.

COMMON CYBERSECURITY THREATS WHILE TRAVELING

- **Unsecured wireless networks.** While public wireless networks provide great convenience, allowing people to connect to the Internet from almost anywhere, they are unsecure and can allow cyber criminals access to your Internet-enabled devices. Beyond the typical public wireless networks found at airports, restaurants, hotels, and cafes, they are increasingly available in other places, such as on airplanes and in public parks.
- **Publicly accessible computers.** Hotel business centers, libraries, and cyber cafes provide computers that anyone can use. However, travelers cannot trust that these computers are secure. They may not be running the latest operating systems or have updated anti-virus software. Cyber criminals may have infected these machines with malicious viruses or install malicious software.

  One example is keylogger malware which, when installed, captures the key strokes of the computer's users and sending this information to criminals via email. Through this malware, criminals are able to receive users' personal information, such as name, credit card numbers, birthdates, and passwords.
- **Physical theft of devices.** Thieves often target travelers. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If you are attending a conference or trade show, be especially wary — these venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms.

CYBERSECURITY AND OLDER AMERICANS

We more connected to technology than ever before. We can get our news the moment it happens; we can learn about complex subjects from information sources around the world; we can run errands, do our banking and shopping, without leaving home; and we share ideas and keep in touch with family and friends, no matter their location. All of this is due, in part, to cyber technology. Yet for all of its advantages, increased connectivity brings increased risk of theft, fraud, and abuse.

As of April 2012, 53 percent of Americans age 65 and older use the Internet or email – the first time this group has exceeded 50 percent in several years. Increasingly older Americans use the Internet to get involved in community groups, shop, plan travel, manage finances, and keep in touch with family and friends. But while the Internet brings many conveniences, it also comes with risks. Cybercriminals use sophisticated techniques to appear legitimate; they pose as friends or family members, banks, charities, mortgage vendors, and even healthcare and low-cost prescription providers to steal information in order to conduct identity theft, phishing schemes, credit card fraud, and more. Learning about ways to protect your identity and personal information online is just as important as understanding how to use the latest technology. Fortunately, making safer and smarter decisions online can be as simple as following these tips:

- Choose a password that means something to you and you only; use strong passwords with eight characters or more that use a combination of numbers, letters, and symbols.
- Keep your mobile devices in your possession at all times and always be aware of your surroundings.
- If you use social networking sites such as Facebook, be sure to limit the amount of personal information you post online and use privacy settings to avoid sharing information widely.
- Most businesses or organizations don't ask for your personal information over email. Beware of any requests to update or confirm your personal information.
- Avoid opening attachments, clicking on links, or responding to email messages from unknown senders or companies that ask for your personal information.
- Install and regularly update the security programs on your computer, such as anti-virus, and anti-spyware. These programs can help to protect the information on your computer, and can easily be purchased from software companies on the web or at your local office supply store.
- Beware of "free" gifts or prizes. If something is too good to be true, then it probably is.
- It is important to add only people you know on social media sites and programs like Skype; adding strangers could expose you and your personal information to scammers.

---

[1] Pew Research Internet Study, June 2012

PROTECT YOURSELF FROM ONLINE FRAUD

When seeking the following information online, you can take precautions to protect yourself from fraud:

Medical Advice

- Be sure to find out who is providing the information, know where you're going online.
- Many pharmaceutical companies create websites with information to sell products.
- Look for sites ending in .edu (for education) or .gov (for government).

Banking

- Avoid accessing your personal or bank accounts from a public computer or kiosk, such as the public library.
- Don't reveal personally identifiable information such as your bank account number, social security number or date of birth to unknown sources.
- When paying a bill online or making an online donation, be sure that you type the website URL into your browser instead of clicking on a link or cutting and pasting it from the email.

Shopping

- Make sure the website address starts with "https," s stands for secure.
- Look for the padlock icon at the bottom of your browser, which indicates that the site uses encryption.
- Type new website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

MOBILE SECURITY TIP CARD

Mobile devices enable Americans to get online wherever they are. Although mobile devices — from smart watches to phones and tables — can be extremely useful and convenient, there are also potential threats users may face with such technology. It's important to understand how to protect yourself when connecting on the go.

DID YOU KNOW?

- **56 percent of American adults** own a smartphone.[1]
- **More than half of mobile application (app) users** have uninstalled or decided not to install an app due to concerns about their personal information.[2]

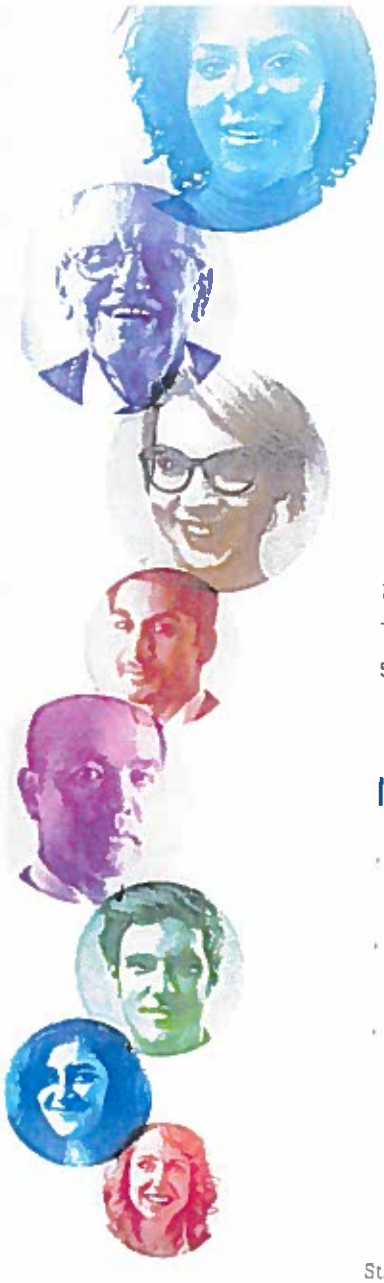
SIMPLE TIPS

1. **Use strong passwords.** Change any default passwords on your mobile device to ones that would be difficult for someone to guess. Use different passwords for different programs and devices. Do not choose options that allow your device to remember your passwords.
2. **Keep software up to date.** Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent attackers from being able to take advantage of known vulnerabilities.
3. **Disable remote connectivity.** Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can connect to other devices. Disable these features when they are not in use.
4. **Be careful what you post and when.** Wait to post pictures from trips and events so that people do not know where to find you. Posting where you are also reminds others that your house is empty.
5. **Guard your mobile device.** In order to prevent theft and unauthorized access, never leave your mobile device unattended in a public place and lock your device when it is not in use.
6. **Know your apps.** Be sure to review and understand the details of an app before downloading and installing it. Be aware that apps may request access to your location and personal information. Delete any apps that you do not use regularly to increase your security.
7. **Know the available resources.** Use the Federal Communications Commission's Smartphone Security Checker at www.fcc.gov/smartphone-security.

---

[1] Pew Research Center's Internet & American Life Project, May 2013

[2] Pew Research Center's Internet & American Life Project, May 2013



RESOURCES AVAILABLE TO YOU

US-CERT.gov

US-CERT provides tips for both individuals and organizations on how to protect against cyber threats. Visit www.us-cert.gov/cas/tips for more information.

OnGuardOnline.gov

This website, run by the Federal Trade Commission (FTC), is a one-stop shop for online safety resources available to individuals of all ages.

StaySafeOnline.org

The National Cyber Security Alliance offers instruction on security updates, free anti-virus software, malware software removal and other services.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
- If you think a site has collected your personal information in a way that violates the law, report it to the FTC at www.ftc.gov/complaint.
- If someone has had inappropriate contact over the Internet with you or a colleague, report it to www.cybertipline.com and they will coordinate with the Federal Bureau of Investigation and local authorities.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP THINK CONNECT™