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.

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