BEST PRACTICES FOR USING PUBLIC WI-FI TIP CARD

Public Wi-Fi networks can now be found almost everywhere – in airports, coffee shops, libraries, restaurants, malls, and hotels – making it easy for anyone to connect to the Internet wherever they are. Although these Wi-Fi hotspots can be convenient, they are not always secure, potentially exposing you to online risks and presenting an opportunity for cybercriminals to steal sensitive information. It is important to understand these risks and take measures to protect yourself while connecting to Wi-Fi networks.

SIMPLE TIPS

- **Think before you connect.** Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, or café – be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. Cybercriminals can easily create a similarly named network hoping that users will overlook which network is the legitimate one. Additionally, most hotspots are not secure and do not encrypt the information you send over the Internet, leaving it vulnerable to cybercriminals.
- **Use your mobile network connection.** Your own mobile network connection, also known as your wireless hotspot, is generally more secure than using a public wireless network. Use this feature if you have it included in your mobile plan.
- **Avoid conducting sensitive activities through public networks.** Avoid online shopping, banking, and sensitive work that requires passwords or credit card information while using public Wi-Fi.
- **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 cybercriminals from being able to take advantage of known vulnerabilities.
- **Use strong passwords.** Use different passwords for different accounts and devices. Do not choose options that allow your device to remember your passwords. Although it's convenient to store the password, that potentially allows cybercriminals into your accounts if your device is lost or stolen.

- **Disable auto-connect features and always log out.** Turn off features on your computer or mobile devices that allow you to connect automatically to Wi-Fi. Once you've finished using a network or account, be sure to log out.
- **Ensure your websites are encrypted.** When entering personal information over the Internet, make sure the website is encrypted. Encrypted websites use https://. Look for https:// on every page, not just the login or welcome page. Where an encrypted option is available, you can add an "s" to the "http" address prefix and force the website to display the encrypted version.

Stop.Think.Connect. is a national public awareness campaign aimed at 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™