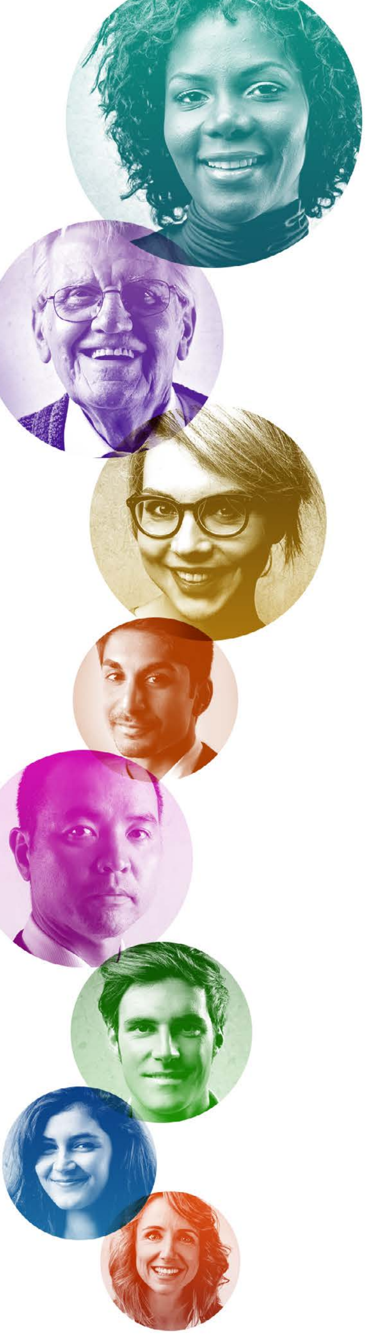


STOP.THINK.CONNECT. CAMPAIGN

MOBILE SECURITY

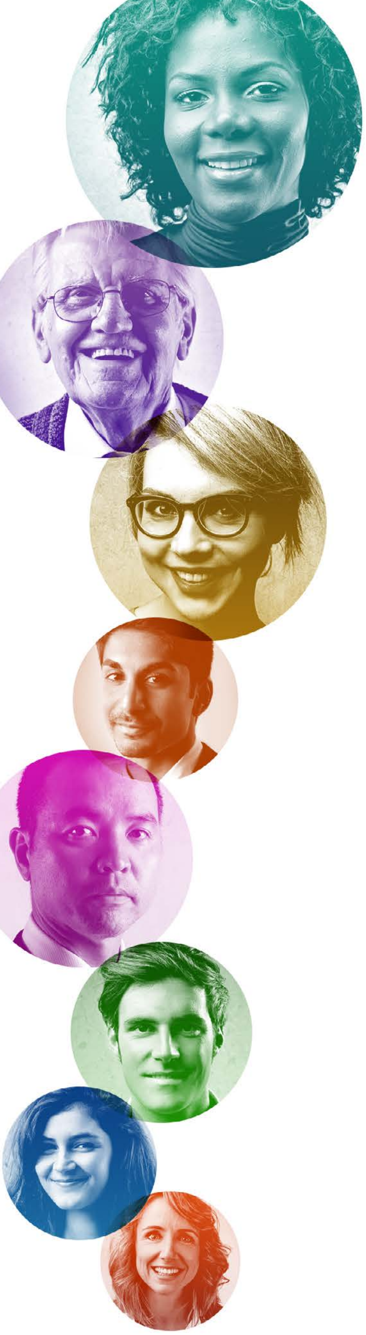
ONLINE SECURITY INCLUDES PROTECTING YOURSELF ON THE GO

Almost all Americans, regardless of age, are using mobile devices. Often, mobile devices are used for sensitive activities, including banking, online shopping and social networking. Some of these activities require users to provide personal information such as their names, account numbers, addresses, email addresses and passwords. Moreover, apps routinely ask for access to information stored on the device, including location information.

In addition, the use of unsecured, public Wi-Fi hotspots has increased dramatically over the past few years. These networks are accessible on airplanes, in coffee shops, shopping malls and at sporting events. While continued access provides us with more flexibility and convenience to stay connected no matter where we are, it can also make us more susceptible to exposure.

The more we travel and access the Internet on the go, the more risks we face on our mobile devices. 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 connecting to the Internet from a mobile device:

- **Think Before You Connect.** Before you connect to any public Wi-Fi 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. Using your mobile network connection is generally more secure than using a public Wi-Fi network.
- **Guard Your Mobile Device.** In order to prevent theft, unauthorized access and loss of sensitive information, never leave your mobile devices–including any USB or external storage devices–unattended in a public place. While on travel, if you plan on leaving any devices in your hotel room, be sure those items are appropriately secured.
- **Keep It Locked.** The United States Computer Emergency Readiness Team (US-CERT) recommends 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 to prevent others from accessing your device.
- **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.
- **Only Connect to the Internet if Needed.** Disconnect your device from the Internet when you aren't using it and make sure your device isn't programmed to automatically connect to Wi-Fi. The likelihood that attackers will target you becomes much higher if your device is always connected.
- **Know Your Apps.** Be sure to thoroughly review the details and specifications of an application before you download it. Be aware that the app may request that you share your personal information and permissions. Delete any apps that you are not using to increase your security.



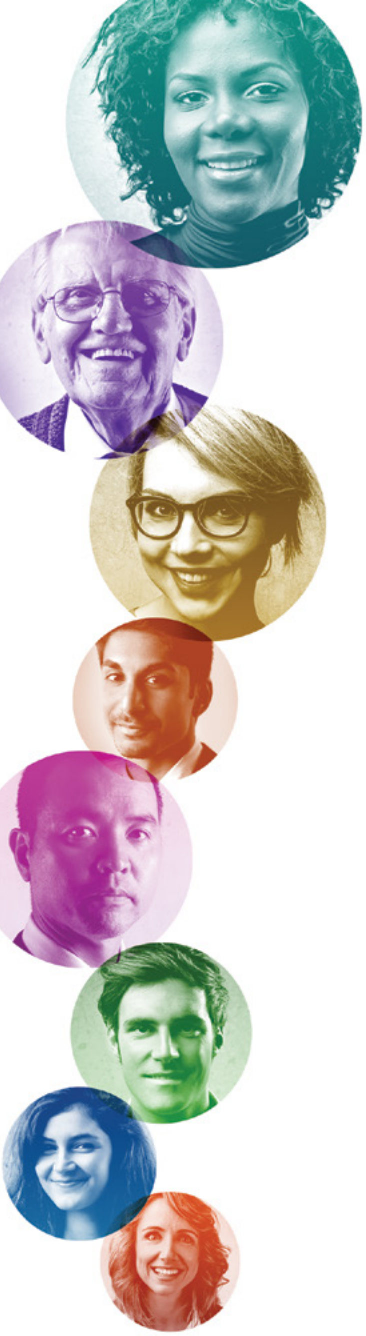
GET INVOLVED

The Stop.Think.Connect. Campaign is a national public awareness campaign aimed at increasing cyber safety amongst Americans. Help the Campaign educate and empower the American public to take steps to protect themselves and their families online. To get involved, become a **Friend** of the Campaign by visiting www.dhs.gov/stopthinkconnect. Once you are a **Friend**, there are many ways to stay involved:

- **Blog, tweet or post** about Stop.Think.Connect. and safe practices when it comes to new technology.
- **Spread the word.** Promote Stop.Think.Connect. messages and resources within your office and social groups.
- **Volunteer** within your community to mentor kids and teens on the basics of online safety.
- **Consider a career** in cybersecurity if you enjoy science, technology, engineering or math.

For more information on the Stop.Think.Connect. Campaign, visit www.dhs.gov/stopthinkconnect

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.



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?

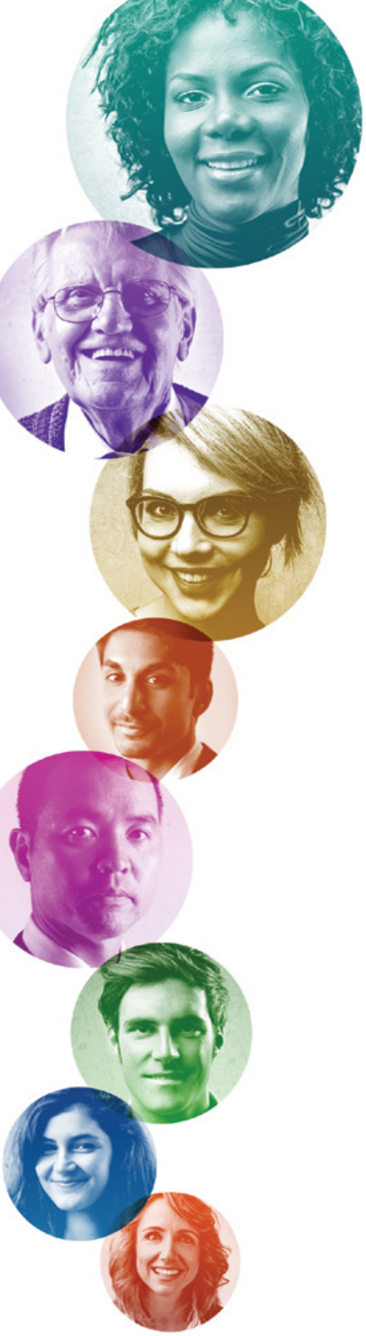
- **56 percent of American adults** own a smartphone.[1]
- **More than half of mobile application (app) users** have uninstalled or decided not to install an app due to concerns about their personal information.[2]

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™