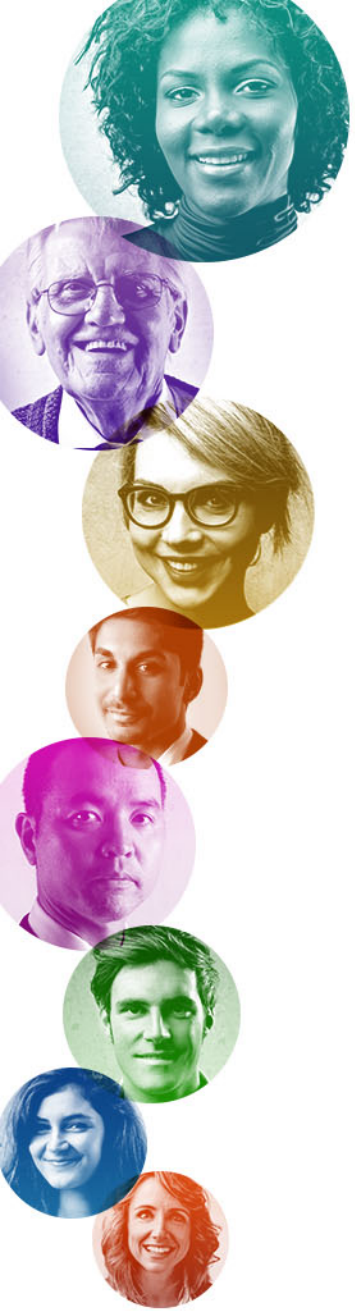
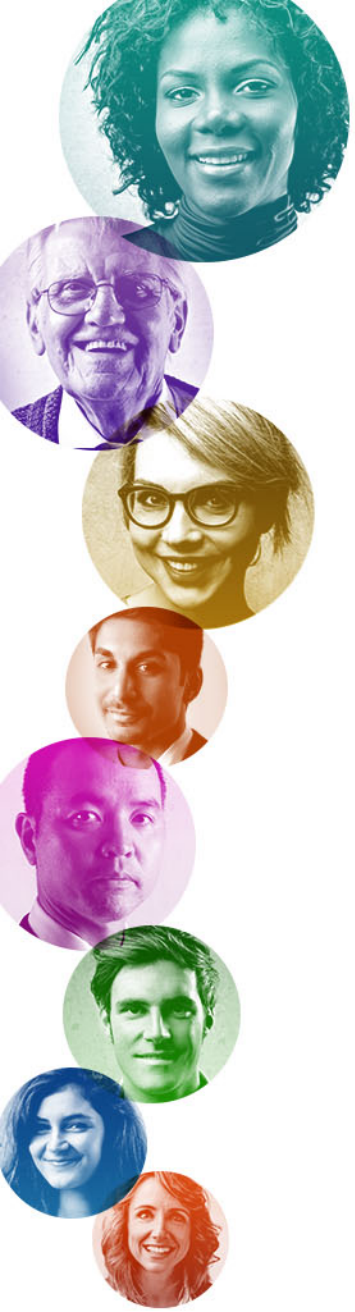

STOP.THINK.CONNECT™
A NATIONAL CYBERSECURITY AWARENESS CAMPAIGN
OLDER AMERICANS PRESENTATION
Homeland Security
STOP | THINK | CONNECT™



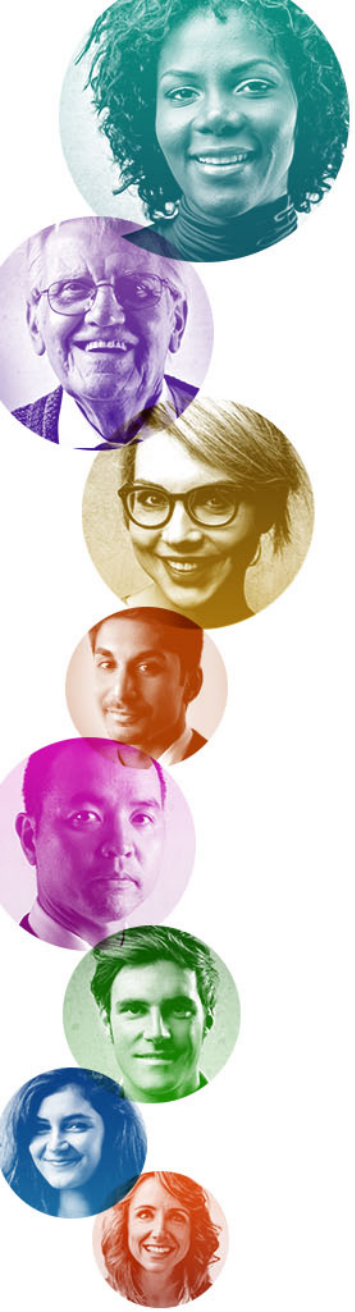
ABOUT STOP.THINK.CONNECT.

- In 2009, President Obama issued the *Cyberspace Policy Review*, which tasked the Department of Homeland Security with creating an ongoing cybersecurity awareness campaign – Stop.Think.Connect.™ – to help Americans understand the risks that come with being online.
- Stop.Think.Connect.™ challenges Americans to be more vigilant about practicing safe online habits and encourages them to view Internet safety as a **shared responsibility** at home, in the workplace, and in our communities.



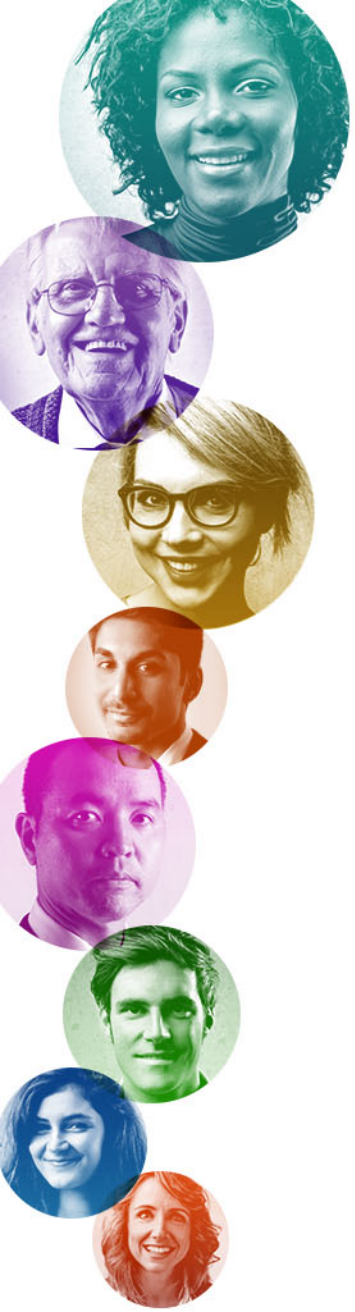
POLL THE AUDIENCE

- How do you use the Internet?
- What are your main concerns about using the Internet?
- Have you ever had your identity stolen?
- Do you have antivirus software on your computer and update it on a regular basis?



USING THE INTERNET

- Email, instant messaging, and personal websites now provide easy ways for everyone to stay connected, informed, and involved with family and friends. The Internet also provides an easy way to shop, plan travel, and manage finances.
- Many scammers target Americans ages 65 and older via emails and websites for charitable donations, online dating services, online auctions, buyer's clubs, health insurance, prescription medications, and health care.
- Many of the crimes that occur in real life – happen on the Internet too. Credit card fraud and identity theft, embezzlement, and more – all can be and are being done online.
- At home, at work, and in the community, our growing use of technology, coupled with increasing cyber threats and risks to our privacy, demands greater security in our online world.

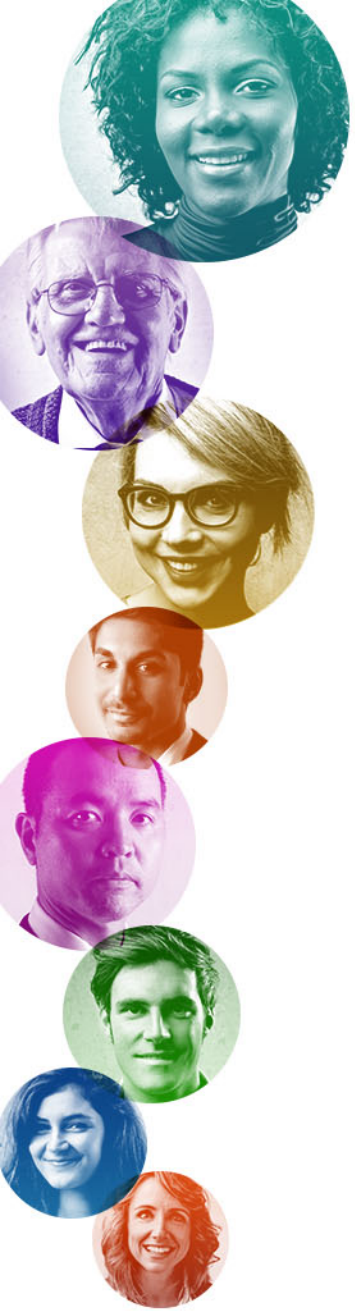


IDENTITY THEFT

Identity theft *is the illegal use of someone else's personal information in order to obtain money or credit.*

Tips

- Don’t use the same password twice.
- Choose a password that means someone to you and you only; use strong passwords with eight characters or more that uses a combination of numbers, letters, and symbols.
- Do not reveal personally identifiable information online such as your full name, telephone number, address, social security number, insurance policy number, credit card information, or doctor’s name.
- Avoid opening attachments, clicking on links, or responding to email messages from unknown senders or companies that ask for your personal information.
- When making online donations, make sure any charity you donate to is a legitimate non-profit organization and that you type in the web address instead of following a link.
- Be sure to shred bank and credit card statements before throwing them in the trash; talk to your bank about using passwords and photo identification on credit cards and bank accounts.
- Check your bank and credit card statements monthly for unusual charges.

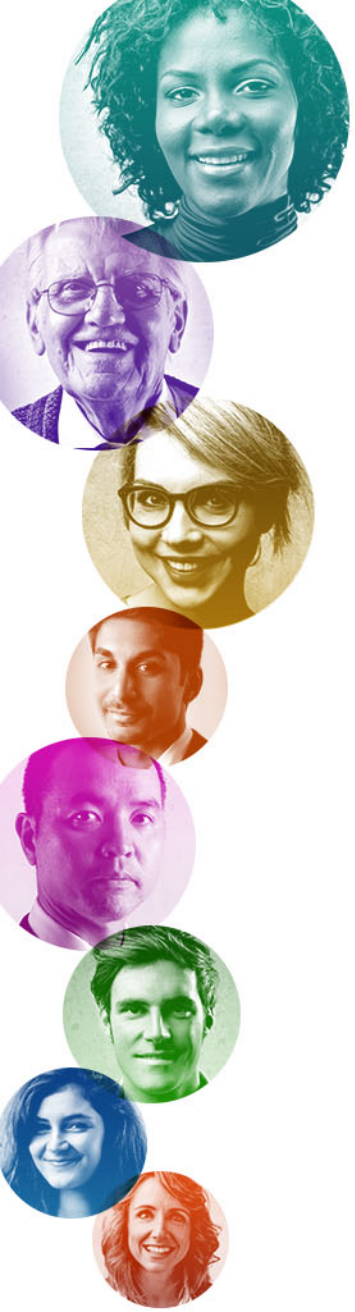


FRAUD & PHISHING

Fraud *is the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right.* ***Phishing*** *is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.*

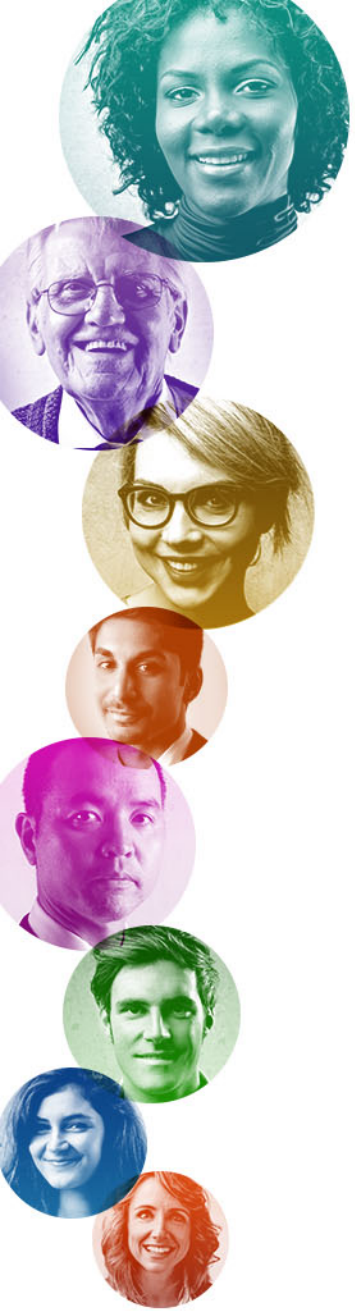
Tips

- Most organizations – banks, universities, companies, etc. - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies.
- Don't access your personal or banking accounts online from a public computer or kiosk.
- Beware of "free" prizes; if you think an offer is too good to be true, then it probably is.
- Make sure you change your passwords often and avoid using the same password for multiple accounts.
- Install and regularly update software firewall, antivirus, and anti-spyware programs. These software programs can help to protect the data on your computer, and can easily be purchased on the web or at your local office supply store.



RESOURCES AVAILABLE TO YOU

- ***AARP:*** The AARP provides specifics on internet safety, how to protect your privacy, and the most up-to-date virus protections.
- ***FBI:*** This is a list of common fraud schemes aimed at older Americans.
- ***SeniorNet.org:*** SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults computer technology education.
- ***Fraud.org*:** Fraud.org helps protect consumers from being victimized by fraud.
- ***FTC's PassItOn Campaign***: The PassItOn Campaign enlists people 65 and older in an effort to recognize and report fraud and other scams. Topics include imposter scams, identity theft, charity fraud, health care scams, paying too much, and "you've won" scams.



CALL TO ACTION

Cybersecurity is a shared responsibility that all Americans must adopt in their communities in order to keep the nation secure in the 21st Century.

Become an advocate in your community *to help us educate and empower the American public to take steps to protect themselves and their families online.*

How to get involved:

- Become a *Friend* of the Campaign by visiting **www.dhs.gov/stopthinkconnect.**
- Download and distribute Stop.Think.Connect. materials, such as the brochure, bookmark, and poster, in your neighborhoods and communities.
- Lead or host a cyber awareness activity in your places of library, recreation, or worship.
- Discuss the importance of cybersecurity with your friends and family.
- Inform your community about the Stop.Think.Connect. Campaign and the resources available.
- Blog or post about the issue of cybersecurity and the Stop.Think.Connect. Campaign.
- Get your local senior center or library involved and informed on cybersecurity.


YOU HAVE AN
IMPORTANT ROLE
HELPING US PROTECT
CYBERSPACE
Homeland
Security
STOP | THINK | CONNECT