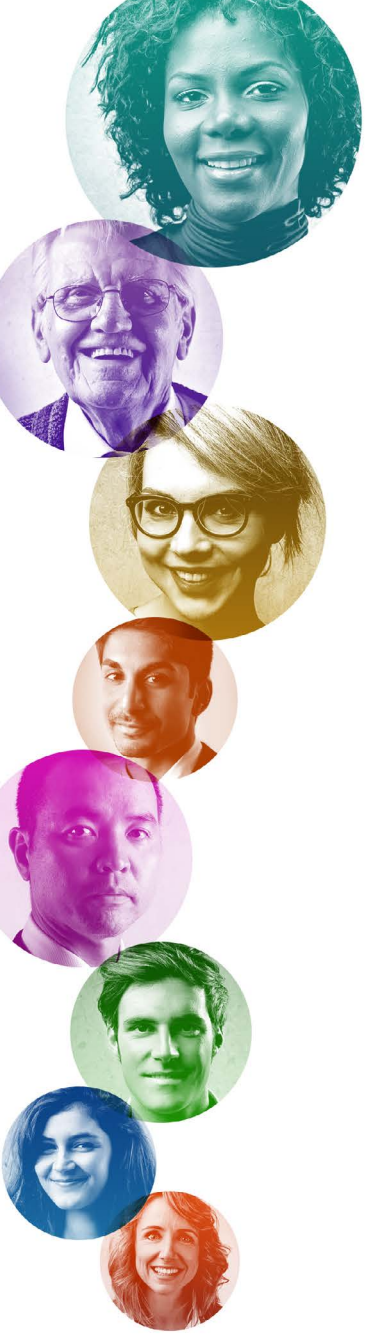
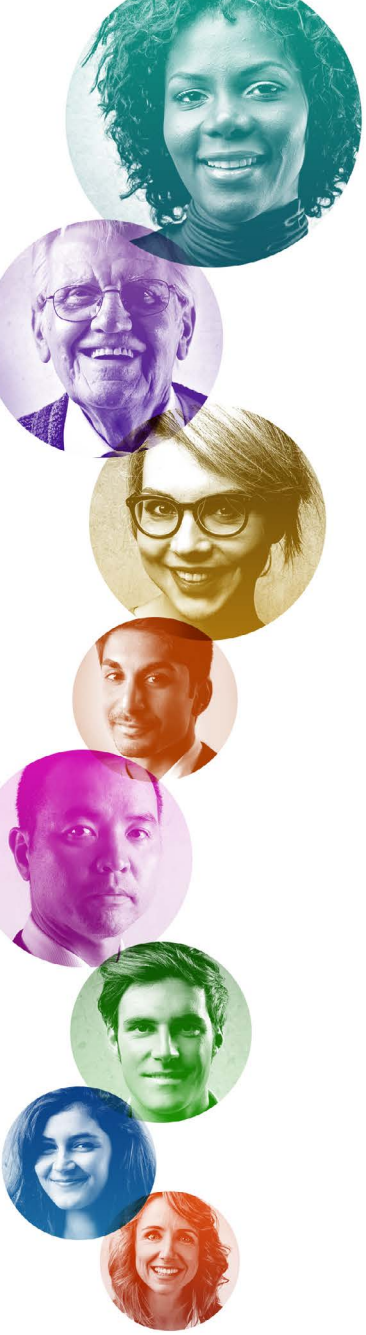


CYBERSECURITY FOR OLDER AMERICANS

With smartphones at the tips of almost everyone's fingers, it's no secret that we're more connected than ever before. We get our news the moment it happens; we learn about complex subjects from information sources around the world; we run errands—banking and shopping— without leaving home; and we share ideas and keep in touch with colleagues, friends and family, no matter their location. All of this is due, in part, to cyber technologies. It doesn't matter who we are or where we live, cyberspace is an essential part of our daily lives. Yet for all of its advantages, increased connectivity brings increased risk of theft, fraud and abuse. As of April 2012, 53% of Americans age 65 and older use the Internet or email—the first time this group has exceeded 50% in several years.[1] More Americans in this group 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 gadget. Fortunately, making safer and smarter online decisions can be as simple as following some common sense 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.
- According to a 2012 Pew Internet research study, **nearly 70%** of Americans age 65 and older report that they have a mobile phone, up from 57% in May 2010. Even among those currently age 76 and older, 56% report owning a cell phone of some kind, up from 47% of this generation in 2010. As these numbers continue to increase, be vigilant when on the go. Keep your mobile devices in your possession at all times and always be aware of your surroundings.
- The same study found, as of February 2012, **one-third** of Internet users age 65 and older use social networking sites such as Facebook, and 18% do so on a typical day. If you are posting information on any of these or other social networking sites, be sure to limit the amount of personal information you post online and use privacy settings to avoid sharing information widely.
- Most organizations—banks, universities, companies, etc.—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 your firewall, anti-virus and anti-spyware programs. These 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.
- Beware of "free" gifts or prizes. If something is too good to be true, then it probably is.
- Only add 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

Take the following precautions online to protect yourself from fraud:

Seeking Medical Advice

- Be sure to confirm that the source of information being provided is credible and legitimate.
- 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.
- Don't reveal personally identifiable information such as your bank account number or social security number 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.

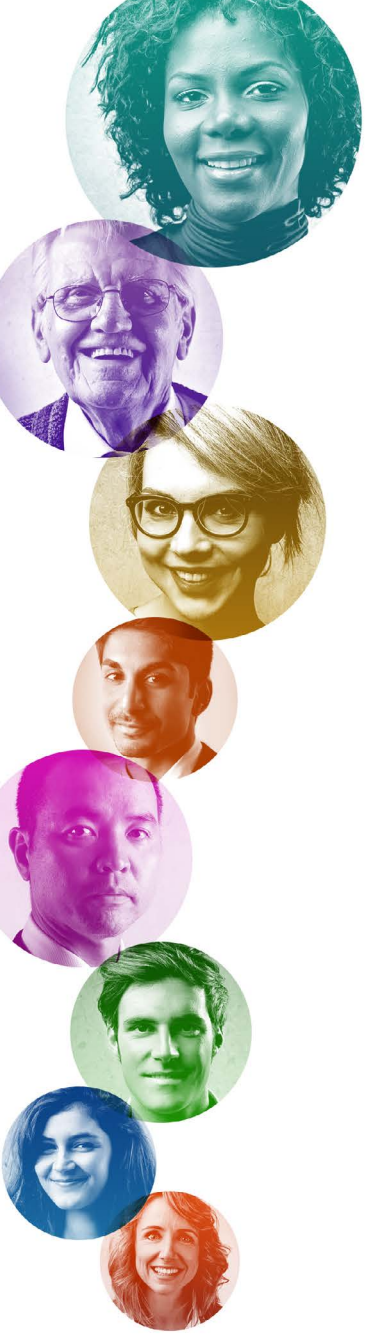
Shopping

- 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.

HOW TO STAY INVOLVED AND ADDITIONAL RESOURCES

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

- Become a Friend of the Campaign by visiting www.dhs.gov/stopthinkconnect.
- Discuss safe online practices with your fellow employees, neighbors, friends and family.
- Inform your community about the Stop.Think.Connect. Campaign and the resources available.
- Blog or post on social networking websites about the issue of cybersecurity and the Stop.Think.Connect. Campaign.
- Host a cybersecurity activity in your community.



DEPARTMENT OF HOMELAND SECURITY

For more information about DHS cyber programs, including additional tips and resources, visit www.dhs.gov/cyber.

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.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™