CYBERSECURITY AND OLDER AMERICANS

We more connected to technology than ever before. We can get our news the moment it happens; we can learn about complex subjects from information sources around the world; we can run errands, do our banking and shopping, without leaving home; and we share ideas and keep in touch with family and friends, no matter their location. All of this is due, in part, to cyber technology. Yet for all of its advantages, increased connectivity brings increased risk of theft, fraud, and abuse.

As of April 2012, 53 percent of Americans age 65 and older use the Internet or email – the first time this group has exceeded 50 percent in several years. Increasingly older Americans 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. Fortunately, making safer and smarter decisions online can be as simple as following these 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.
- Keep your mobile devices in your possession at all times and always be aware of your surroundings.
- If you use social networking sites such as Facebook, be sure to limit the amount of personal information you post online and use privacy settings to avoid sharing information widely.
- Most businesses or organizations 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 the security programs on your computer, such as anti-virus, and anti-spyware. These programs can help to protect the information on your computer, and can easily be purchased from software companies 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.
- It is important to add only 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

When seeking the following information online, you can take precautions to protect yourself from fraud:

Medical Advice

- Be sure to find out who is providing the information, know where you're going online.
- 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, such as the public library.
- Don't reveal personally identifiable information such as your bank account number, social security number or date of birth 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 or cutting and pasting it from the email.

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 or cutting and pasting from the email.

HOW TO STAY INVOLVED & FREE ADDITIONAL RESOURCES

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

- Become a Friend of the Stop. Think. Connect.™ 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, free 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 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 you community. For more information visit http://www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™