STOP.THINK.CONNECT.™

# Cyber Tips for Older Americans

## WHAT IS CYBERSECURITY

Cybersecurity is general Internet safety, which includes protection of anything connected to or accessible by the Internet- from networks themselves to the information stored in computers. Technology has changed tremendously in the past 25 years, and it only continues to advance. The Internet has brought us so many benefits; email, electronic messaging, and personal websites allow us to stay connected, informed, and involved with family and friends. The Internet also provides an easy way to shop, plan travel, and manage finances. However, with these increased conveniences comes increased risk.

> Baby boomers embrace new technologies 20 times faster than members of Gen Y, including social sites, podcasts, and blogs. [i]

Just like any other public environment, the Internet requires awareness and caution. Just as you use locks to keep criminals out of your home, you also need safeguards to secure your computer. Many of the crimes that occur in real life are now done - or at least facilitated - through the Internet. Theft, abuse, and more can be and are being done online. Many scammers target older Americans via emails and websites for charitable donations, dating services, auctions, health care, and prescription medications.

Below are some common sense rules from the real world that apply in the online world.

- **Don't judge a book by its cover**. Cyber criminals hide behind the anonymity of the Internet. What you say and do online is visible to others, and it's not erasable. Don't communicate or reveal any personal information to strangers online. Personal information includes your name, address, age, phone number, birthday, email address, social security number, and insurance policy numbers – even your doctor's name.
- **Look before you leap**. Don't enter contests, join clubs, or share your personal information for any reason, unless you know you are on a reputable website. Do not open attachments, click links, or respond to email messages from unknown senders or companies that ask for your personal information. Most organizations – banks, charities, universities, companies, etc. - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- **All that glitters is not gold**. Be wary of emails offering "free" gifts, prizes, or vacations. These are tricks designed to get you to give up personal information. Personal information can be pieced together to steal identities, money, or credit.
- **A chain is as strong as its weakest link**. Once we understand the dangers we face online, we need to tell other people who might not be as cyber smart and savvy. Every Internet user, no matter how young or old, is our Nation's first line of defense against people who might want to do harm. If we all become more aware of who we talk to, what we say, and what we share online we can all make a big difference.

# Protecting Against Online Fraud

Be sure to remember these tips when navigating the Internet to avoid fraud.

Seniors are defrauded at twice the rate of the rest of the population. [ii]

- **Seeking Medical Advice**. When you go to any medical-related website, be sure to consider: How current is the information? Check to see when the information was released. Do not rely on a single website for information, consult a few sources and be sure to check who exactly is providing the information. Many pharmaceutical companies create websites with information to sell products. Look for sites ending in .edu (for education) or .gov (for government).
- **Banking**. When using online banking services, check to be sure the sites you navigate are secure. One quick clue to determine whether a website is safe is if the URL begins with "https://." When using a public computer–such as one at your local library–avoid typing your personal information. Look for the padlock icon at the bottom of your browser, which indicates the site uses encryption. Also, type website URLs directly into the address bar, do not follow links.
- **Shopping**. If you shop online, check your credit card statements as often as possible and use a credit card for online purchases. Credit cards have some protections that debit cards do not, such as the ability to question unusual charges.

Look for this padlock icon in your Internet browser when shopping and banking online.

## HOW TO GET INVOLVED

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 http://www.dhs.gov/stopthinkconnect. Once you are a Friend, there are many ways to stay involved:

- Impress your children or grandchildren. Blog, tweet, or post about Stop.Think.Connect. and safe online behavior.
- Spread the word. Promote Stop.Think.Connect. messages and resources within your families and communities.
- Encourage your local community center, library, or to hold an educational cybersecurity program.
- 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 work, school, recreation, or worship.
- Discuss the importance of cybersecurity with your friends and family.
- Inform your community about the Stop.Think.Connect. Campaign and available resources.
- Get your local senior center or library involved and informed on cybersecurity.

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

i. Accenture
ii. National Association of Triads, Inc.

Homeland Security

STOP | THINK | CONNECT™