



OLDER AMERICANS TIP CARD

As technology constantly advances, it is important for everyone to learn about cybersecurity and the steps individuals should take to protect themselves from criminals. Although new technology has revolutionized the way we do things, from banking to lifestyle management, it is critical that we learn and teach others about the vulnerabilities our technology may face and how to be safe online and on the go.

DID YOU KNOW?

- Those over the age of 65 continue to trail the national average in broadband adoption (35 percent); however, nearly half (48 percent) of older Americans are Internet users, regardless of connection type.
- Baby boomers embrace new technologies 20 times faster than members of Gen Y, including social sites, podcasts and blogs.¹
- Seniors are defrauded at twice the rate of the rest of the population.²
- There was a 91% increase in targeted attacks campaigns in 2013 and a 62% increase in the number of breaches.³
- According to the Federal Bureau of Investigation (FBI), senior citizens are most likely to have a “nest egg,” to own their home, and/or to have excellent credit—all of which make them attractive to con artists.
- Per the FBI, elderly victims may not report crimes, for example, because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.

SIMPLE TIPS

- Install and regularly update firewall, antivirus, and anti-spyware programs.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies that ask for your personal information.
- Do not reveal personally identifiable information such as your full name, telephone number, address, social security number, insurance policy number, credit card information, or even your doctor’s name.
- 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.
- Beware of “free” gifts or prizes; if something is too good to be true, it probably is.

¹ Consumer Electronics Products and Services Usage Report, Accenture, March 2009.

² National Association of Triads, Inc.

³ Symantec 2014 Internet Security Report



RESOURCES AVAILABLE TO YOU

AARP.org

What is a firewall and how do I get one? The AARP provides technology how-to guides designed specifically for you that address computer basics.

FBI.gov

For a list of common fraud schemes aimed at older Americans, visit the Federal Bureau of Investigation (FBI) at <http://www.fbi.gov/scams-safety/fraud/seniors/>.

SeniorNet.org

SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults with computer technology education.

FTC.gov/passiton

The Federal Trade Commission's (FTC) Pass it On Campaign reinforces what older adults already know about some of today's most common scams, and provides them with a straightforward way to share that knowledge with their family members, friends, and communities.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
- If you have been a victim of identity theft, follow the steps provided by the FTC (www.ftc.gov) to recover and respond to identity theft.
- If someone has had inappropriate contact with you or someone you know, report it to www.cybertipline.com and they will coordinate with the FBI and local authorities.
- If you are the victim of online fraud, report it to the Department of Justice at www.justice.gov/criminal/cybercrime/reporting.

www.dhs.gov/stopthinkconnect.

www.dhs.gov/stopthinkconnect