



Monthly Security Tips

NEWSLETTER

Department of Accounting and General Services
Information & Communication Services Division

June 2013

Volume 8, Issue 6

Keeping Senior Citizens Safe Online

Senior Citizens are Online Too

Senior citizens are embracing the digital age in greater numbers every year. Fifty-three percent of adults ages 65 and older now use the Internet and online tools such as email, according to the Pew Internet & American Life Project. Among those Internet users, seventy percent report going online daily.

Not surprisingly, the Internet offers many benefits to older Americans, including the ability to better stay in touch with family members, near and far and across generations. A 2012 study by Microsoft and AARP found that online communication often was credited for improving dialogue among family members.

The Internet helps senior citizens connect with society, bringing vital information and resources to them. For instance, they can bank and shop from the convenience of their homes. There are many sites geared toward the needs and interests of senior citizens, and growth of such sites is expected to continue.

What are the Risks?

There are risks associated with being online, and, sadly, many scammers target senior citizens.

Older Americans should be wary of the following types of emails, websites, or social media messages that:

- Offer “free” gifts, prizes or vacations, or exclaim, “You’re a winner!”
- Offer discount prescription medications or other “can’t miss” deals.
- Appear to be from friends or family members, but the message is written in a style not usually used by that person, has numerous misspellings, or otherwise seems unusual. This is an indication your friend or family member’s account may have been hacked.
- Appear to be from official government agencies, such as Social Security Administration, or banks, requesting personal information.
- Set ultimatums such as “your account will be closed,” or “the deal will expire” to create a sense of urgency, and trick the victim into providing personal information.

Cyberbullying of Senior Citizens

Though there is a lot of focus on cyberbullying among children and teens, cyberbullying affects senior citizens as well.

Cyberbullying (mostly through e-mail) of seniors can take several forms, but the most common are:

- Emotional abuse with rage, threats, accusations, and belittling comments, often followed with periods of silence or ignoring the victim.
- Financial abuse aimed at obtaining the victim’s account information, setting up online access to their accounts, and stealing their money.

Speaking out against cyberbullying can be particularly difficult for seniors who may not even know what the term means. As with victims of any age, seniors may feel violated and powerless, be confused and in denial over what's happening, feel shame and self-blame for being a victim, and fear even more bullying or being ignored if they speak out. Additionally, according to the Washington State Office of the Attorney General, in many cases, seniors are the victims of cyberbullying by family members.

What to do: STOP. THINK. CONNECT.

To protect against these online threats, there are several basic precautions all Internet users should take, regardless of age or experience online. The following tips are provided by *STOP. THINK. CONNECT.*, the national online safety awareness campaign.

Keep a Clean Machine

- **Keep security software current and updated:** Have the latest security software, web browser, and operating system installed on your computer. Enable the auto-update feature to ensure you have the most up-to-date security, if that's an option.
- **Protect Wireless Network:** Ensure your wireless router requires a secure password.

Protect Your Personal Information

- **Make passwords long, strong and unique.** You have should have a different password for each online account, using a combination of upper and lower case letters, numbers and symbols.
- **Think before you act:** Most organizations – banks, charities, universities, companies, etc., – will not ask for personal information via email. Be wary of requests to update or “confirm” your information.
- **Post with caution:** Information you post online, especially on social networking sites, can be collected in an attempt to steal your identity. Keep information such as birthdates and addresses confidential unless you are on a secure and reputable website.
- **Own your online presence.** Understand how privacy settings work on social networks and websites you frequent. Set them to your comfort level of sharing.

Connect with Care

- **Protect Your Money:** When banking or shopping online, enter information only into security-enabled sites that begin with *https://*. The “s” means the data is encrypted in transit. Never enter bank or credit card information into a website that begins *http://*.

Be Web Wise

- **When in doubt, throw it out:** Links in emails, social media posts, and online ads are often how scammers access your computer. If you are instructed to click a link in a message you don't trust, even if you know the sender, delete the message or mark it as junk mail.
- **Back it up:** Store valuable work, photos, music and other information on a backup hard drive or online “cloud.”

Recognize Cyberbullying

- If you think you, or someone you know, is a victim of cyberbullying, report it to the local law enforcement, or a local senior center for further advice and assistance.

Resources For More Information:

For additional information, please visit:

- **STOP. THINK. CONNECT. Older American Resources:**
<http://www.dhs.gov/publication/stopthinkconnect-older-american-resources>

- **OnGuardOnline.gov: How you can help older Americans avoid fraud:**
<http://www.onguardonline.gov/blog/how-can-you-help-older-americans-avoid-fraud-talk-about-it>
- **"Stay Safer on the Internet," a senior's guide to online safety by Microsoft:**
<http://go.microsoft.com/?linkid=9677449>
- **Washington State Office of the Attorney General: Internet Safety for Seniors:**
<http://www.atg.wa.gov/internetsafety/seniors.aspx#Top>

For more monthly Cyber Security Newsletter tips, visit: www.msisac.org/awareness/news/

Brought to you by:

 <p>Information & Communication Services Division (ICSD) Cyber Security Team http://ags.hawaii.gov/icsd/cyber-security/</p> <p>The mission of the ICSD Cyber Security Team is to preserve the confidentiality, integrity, and availability of the State of Hawaii's electronic information resources.</p>	 <p>Multi-State Information Sharing & Analysis Center www.msisac.org</p> <p>The mission of MS-ISAC is to provide a common mechanism for raising cyber security readiness and response in each state and with local government.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The information provided in the Monthly Security Tips Newsletters is intended to increase your security awareness and to help improve the organization's overall cyber security posture.