

Safe Computing Tips for Seniors

Recently purchase your very first personal computer or received one as a gift? You are in good company! According to eMarketer, a leader in market research and trend analysis of the Internet and emerging technologies, close to 21 million Internet users are 62 years old or older (source: eMarketer, May 2008). And that's just in the United States. All over the world, more and more seniors are logging onto the Web for the very first time.

A growing number of seniors in the world

“In 2006, almost 500 million people worldwide were 65 and older. By 2030, that total is projected to increase to 1 billion—1 in every 8 of the earth's inhabitants. Significantly, the most rapid increases in the 65-and-older population are occurring in developing countries, which will see a jump of 140 percent by 2030.” (source: “Why Population Aging Matters: A Global Perspective”, National Institute on Aging, 2007)

With advances in healthcare, the number of senior citizens worldwide continues to rise. During their lifetime, “boomers” have witnessed historic changes in technology. Many seniors have embraced the personal computer and continue to play catch-up with technology. Unfortunately for them, cyber-criminals have been doing their best to stay one step ahead. They have modified their targeting techniques to include online scams and electronic junk mail, to their more traditional arsenal of telephone calls and mass mailings.

Why are seniors such a tempting target for criminals?

- Seniors' retirement savings or other such personal assets are seen as a goldmine by cyber-criminals
- Some seniors may have difficulty remembering exact details, or are unable to clearly explain the technical nature of an attack
- Senior citizens are often less likely to report electronic fraud because they are unsure of how to combat it, or because they may feel embarrassed by the attack

What sorts of ways do criminals attack seniors?

Electronic nuisances and attacks (or “malware”) may be divided into several different categories. Some of the most common types are:

- Phishing / Identity Theft
- Spyware / Adware
- Viruses
- E-mail Spam

Attackers often attempt to attract seniors through schemes that are of specific interest to them. Be especially wary of websites, offers, and unsolicited e-mails that advertise promotions that may seem too good to be true. A few common offers are:

- Discounted health insurance, prescription drugs, and home healthcare-related products
- Foreign sweepstakes, lotteries, and award notifications
- Credit card offers
- Investment opportunities
- Charity enquiries
- Home repair services
- Attorney, solicitor, or government advisements which ask users to deposit personal money in order to collect a larger sum that is being held in escrow

A few basic tips to avoid being victimized:

- Shred credit card receipts and old bank statements
- Close unused credit card or bank accounts
- Don't give out personal information via the phone, mail, or Internet unless you initiated the contact
- Never respond to an offer you don't understand
- Talk over investments with a trusted friend, family member, or financial advisor
- Require all plans and purchases to be in writing
- Don't pay in advance for services
- Consider enrolling in a credit monitoring service, such as *TrustedID*
- Install and activate a reliable home security solution, such as those available from BitDefender
- Update your antimalware, firewall and spam filter frequently
- Install and activate an Internet browser pop-up blocker
- Scan your computer for threats regularly
- Do not install any program or application that might require resource sharing without the permission of your system and/or network administrator
- Do not open e-mail and e-mail attachments from senders you do not know
- Do not open e-mail with odd entries in subject line
- Do not respond to e-mail requests for any personal information (such as user names and passwords, social security number, bank account or credit card numbers)
- Do not click any links indicated in e-mail, including the "unsubscribe" ones; you might trigger other malware and compromise your system's security
- Do not click the links contained in unwanted pop-up windows.
- Always delete the spam messages; if you accidentally open them, display the attached images or click on links in the e-mail, you may be letting criminals know your e-mail account is active and available to receive more spam
- When browsing the Internet, do not provide your e-mail address or personal information when requested by suspicious webpages
- Avoid placing your e-mail address on websites, guest books, newsgroups, contact lists, shopping or gift lists
- Use at least two e-mail addresses. Create one e-mail account and use it for your correspondence with people you know and a second e-mail account for the websites forms requiring an e-mail address to allow content access. Free web-based e-mail accounts are available from Yahoo, Hotmail, and Google

What to do if you are a victim of electronic fraud.

If you are a senior citizen (or a caregiver) and believe you have been victimized, you should immediately call your bank and/or credit card company to alert them. It is also advisable to contact your local law enforcement agency. Many countries offer specific telephone hotlines for crimes of this nature. It is wise to keep all contact and personal account information in a safe place and easy to locate (note: not on your computer), should you need to find it in an emergency since it is critical that you report it right away.