CYBERINSURE ONE

Online Safety for Seniors

A Comprehensive Guide to Keeping Seniors Safe Online

Senior Safety by the

While we know to be wary of strangers we meet in public, it can sometimes be difficult to remember that there are just as many, if not more, people with malicious intent on the internet. The telltale signs of someone who is dishonest and intends to do us harm can be vastly different online vs. in person. Who really is that person you're communicating with online?

With more and more people going online every day, many criminals have moved away from in-person petty crime and scams and toward online fraud and attacks. Seniors, unfortunately, have become a prime target for many of these scammers. However, there are many techniques that everyone can use to identify possible criminals online before they can cause any real harm.

Statistics, Online Crimes Against Seniors, By the Numbers

- $30 billion - The estimated amount that seniors lose each year due to online scams

- 954,000 - Estimated number of seniors that have to skip a meal or more due to financial hardships resulting from online scams and caregiver abuse
- Source: 2015 True Link Financial Study

Online Safety Basics

Seniors who learn how to be more cautious and aware of online scams will find that there are many benefits to the internet. There are some basic safety practices that seniors can use to help protect themselves online.

1

Never Assume A Stranger Online is Trustworthy

Unless you have a real-world relationship with the person trying to communicate with you over email, video chat and messaging, or social media, they're likely looking to take advantage of you. Sometimes an email offers a deal that is too good to be true. It is likely a fictitious offer or prize created to trick you into revealing private information, to wire money to a scammer, or to get you to install malicious software on your computer.

2

Never Provide Any of Your Sensitive Information Online

While some websites that request private information are trustworthy, such as an online tax filing website, there are many scams online designed to trick you into giving the scammer your private information. For example, a criminal might send you an email

information. For example, a criminal might send you an email, pretending to be a customer service representative. In the email, they might request your sensitive user account information, such as your online banking username and password. A real bank will never ask you for that information in an email, a website linked to from an email, or over the phone. If you have any concerns about whether you can trust an email or website, call the customer service phone number for the company or institution. It's likely that a scammer is attempting to steal your private information so that they can access your bank accounts and other sensitive accounts. They might even use that information to steal your identity.

3

Never Assume that Someone Who Knows Things About You Is Someone Who Can Be Trusted

It's relatively easy for scammers to get mailing lists for organizations, church groups, and community service groups. Scammers can purchase these lists illegally, while other lists are public and can be easily legally obtained. In addition, city, state, and federal government websites often have a fair amount of information freely available online. Because someone can easily get personal information about you and then use it to trick you into believing they're someone they are not, it is important that you are always cautious in communicating with strangers online, even if they do know information like your address, full name, the number of children or grandchildren you have, your pet's name, etc.

Here are some links to additional resources with tips on staying safe online:

WA State Attorney General

Tips for staying safe online as well as specific information on cyberbullying, information exposure, social networking and why seniors are more vulnerable.

Stay Safe Online

Online safety basics presented by the National Cyber Security Alliance to protect yourself, family and devices with their resources

yourself, family and devices with their resources.

Dummies

Dummies presents a comprehensive guide to internet safety for senior citizens. They give good web resource ideas for seniors to use.

Cell Phone Tracking Review

Nice visual presentation of how to stay safe online designed for senior citizens. Also gives advice on what to look out for.

McAfee

Anti-virus software maker McAfee offers tips on staying safe online that are good at any age.

SafeStars

Internet safety tips for kids and adults discussing scams, predators, social media and more.

Common Scams Against Seniors

There are three primary ways that scammers try to take advantage of seniors online. Each of these methods has additional specific scams within them, but knowing the ways that scammers target people is key to online safety.

Email Scams

While online security professionals, such as those in the police force and FBI, are aware of some very common email scams, seniors' trusting nature and good-heartedness can sometimes result in taking advantage of their goodwill. Email messages are a primary way that scammers target seniors.

The following are some common email scams:

1

Request for a short-term loan.

In this scam, the criminal writes an email using a personal message. In it, the scammer asks you to give them a small loan. They often say that they're in dire need of your help and that they will return your loan many times over at a not-too-distant date. An example of this scam is the Nigerian Prince email scam.

2

Request to validate your banking login information.

Scammers have learned how to create email messages and websites that look nearly 100% legitimate. However, a banking representative will NEVER ask you for your banking username or password. Although the email or website might look valid, it's almost certain your bank did not create it. If you have concerns that the email might be fictitious, contact your bank at their customer service phone number. This type of scam can also be used to gain access to your other online accounts, such as your email or social media logins.

Website Pop-Up Ads and Warnings

Some websites often open new tabs or windows when you visit them. Many of those pages are innocent, yet annoying, advertisements. However, others are malicious. Scammers use either fearful messaging or congratulatory text to encourage you to click links in the web page. Both tactics appeal to your emotions and encourage you to act quickly. In both cases, these are scams. Close the window or tab immediately and never click any links in those pages.

Here are some examples:

1

Install Required Security Software.

In this scam, the web page warns you that your computer is infected and that you must immediately install their security software. The page may look like a large company, such as Apple or Microsoft, has created it. Those companies, however, do not notify you of security problems through web pop-ups--it's something, rather, that scammers do.

2

You've Won a Prize.

This scam operates very similarly to the previous one -- a scammer sets up a website that notifies you that you've won a prize. They tell you that you only have to click the ad and give them some basic information to collect your prize. Similar to the Nigerian Prince email scam, the scammer might request a down payment to secure your prize, or they might ask you for your banking account information so that they can deposit your winnings. In any case, the messages are malicious and someone is attempting to scam you.

Impersonation in Social Networking and Online Dating Sites

Scammers also often use social media and dating sites, such as Facebook, to befriend you and claim that they know you. They will often collect information about you by researching your social media pages, hoping to gain your trust by knowing personal details about you. Some scammers also target seniors through online dating sites, pretending to be an interested suitor. Instead, the person they claim to be is someone totally different. If someone on a dating site requests very personal information from you or for you to loan him or her money, do not trust them.

To learn more about common scams against seniors, check out the following sites:

FBI

The FBI not only keeps track of all scams, but they publish this information so the public can stay informed and protected. Seniors and their caregivers should visit this site.

Identity Theft

Report identity theft on the Federal Trade Commission website if you encounter a situation where your information has been stolen online.

NCOA

The National Council on Aging released their top ten scams against seniors in the financial arena.

Clark

Ten scary financial scams against seniors and how to avoid them, with a large section on internet scams.

ACFE

The Association of Certified Fraud Examiners discusses elderly scams, how they are targeted and how to prevent them.

AARP

Tips from the AARP on how to protect your aging parents from common and sneaky scams, including depublicizing their phone number.

How to Report a Cyber Scam

There are many places where you can report online scams. If you believe that someone is attempting to use the internet to scam you, it's better to be proactive and cautious than risk being taken advantage of by an online scammer.

Here are the following resources for reporting a cyber scam:

AARP

The AARP has ElderWatch, where hundreds of volunteers work with the elderly to assist them in making decsions and staying away from scams.

Justice.gov

The United States Department of Justice has a section on their site for reporting computer, internet-related or intellectual property crime.

FBI

The FBI is the lead government agency for reporting and investigating cyber crimes.

IC3

The Internet Crime Complaint Center is a division of the FBI where you can file a complaint online.

USA.gov

This government site gives tips on how to avoid cyber crime, phishing scams and

internet fraud.

eConsumer.gov

This division of the International Consumer Protection and Enforcement Network is where you can report issues with ecommerce sites, dating sites, etc.

Protecting Your Parents Online From Financial Abuse

If you are the son or daughter of a senior that is actively using the internet, there are a few simple ways that you can help them be safe online.

Tell Them About Common Online Scams

This article can be a good place to start for helping to inform your parent about the potential dangers of scammers on the internet. In addition to the recommendations on this page, consider the following:

- **Do not assume that your parent knows about the various ways that someone might seek to take advantage of them.**
- **Ensure that you discuss online safety regularly. Clarifying that online safety is not just a topic for seniors is a helpful way to initiate a discussion with your parent about the risks and benefits of computing and the internet.**

Let Them Know You're There to Help

Some seniors might not be sure whether a message, website, or request is legitimate. Let your parent know that they can ask you about how scams work online and how to safely use the internet.

Consider discussing and sharing articles that include concrete examples about how people have been scammed online.

Help Secure Their Computers

While computers have been around for decades now, they can still be complicated today. Many computers aren't set up to act like push-button appliances and instead require that you understand some of their underlying internals in order to keep them secure. Most operating systems provide a way for you to set up security updates to install automatically and many applications now also include options to enable automatic updates.

If your parent's computer does not yet have a firewall enabled or antivirus installed, add and configure these security defense tools. Configuring such complicated applications and security protections can be overwhelming and confusing to seniors. The modern internet has only been around for 30 years and modern computing has consistently changed in the last 10 years. It's difficult for anyone to stay current on all of the developments in computing and the internet.

Finally, install software to backup their files. There are several online services that will allow you to backup your files for free or for very little cost. Some malicious software makes personal files unreadable by encrypting them, only releasing the files once the victim has paid the scammer a ransom. Having a backup of your parent's important files and cherished photos will help provide you and them with peace of mind.

Here are some other tips to help you keep your parents safe online:

AARP

Tips to help adult children keep their parents clear from fraud, particularly online, by following some simple tips and setting up safeguards.

Generation Law

This post from a law practice details some tips for adult children to help keep their aging parents safe online, especially through email.

Protect Seniors Online

Public education program with best pratices on avoiding scams online including a quiz to see if you are an easy target.

Senior.com

How home care can protect seniors from online scams by getting seniors more comfortable with technology.

Elder Abuse and Technology

Unlike 30 years ago, scamming someone today can be very easily done without ever having to speak with or physically meet someone. Many seniors today gravitate toward the internet so that they can meet new people, learn new things, and stay connected to their loved ones. Combining the increasing numbers of seniors going online with their limited experience using computers can mean that they are sometimes key targets for internet scammers.

While there is no solid information that says that seniors are more likely to be taken in by an online scam than any other demographic, scammers do know that the elderly spend more time on the internet during the day than other groups of people. In addition, since seniors often use the internet to stay in touch with family, scammers often use the names of relatives to violate their trust and steal from them, such as impersonating a grandson and requesting that money be wired to a scammer's account.

For more resources on elder abuse, including financial abuse, look at these resources:

NAPSA

Financial abuse is the fasting growing form of abuse among seniors, and one in nine seniors reports being taken advantage of in this way.

NCOA

Financial scams are the "crime of the 21st century." Here is a look at ten of the most

prevalent scams, including ones on the internet.

Time

Four Ways to Protect Your Aging Parents From Financial Abuse from Time magazine.

AARP

Report fraud or financial exploitation against seniors with ElderWatch from the AARP.

ABA

American Banker's Association gives advice on protecting the elderly from financial abuse.

New York Times

New York Times article on various acts and laws in place to protect a vulnerable elderly population from crimes.

Huffington Post

The article from the Huffington Post talks about Elder Abuse and Technology and how prevalent it is in today's society, what with the advent of email and senior vulnerability and inexperience online.

Older Adults and the Internet

Using a computer to access the internet can sometimes feel daunting to some seniors. Terminology that is commonplace to many younger people may seem foreign and confusing to seniors. One way to help seniors feel more comfortable using the internet is to highlight the things they can do with the internet, rather than teaching them the technology that powers those experiences.

For example, rather than learning about obscure technical jargon such as URL, browser, shortcut, HTTP, and cookie, make technology more accessible by focusing more on tasks like:

- **Sending an email to your family**

- **Translating French text to English**
- **Playing an online game**
- **Sharing photos with friends**
- **Researching a future vacation spot**

Many seniors prefer to use touchscreen devices, such as tablets. Larger touchscreen tablets can make computing and internet usage easier to use for many seniors. These devices often have support for reading text aloud and also enlarging text on the screen to make it easier to read.

According to a study conducted by the Pew Research Center, as of 2012, over half of seniors over 65 are now using the internet. Many seniors are finding that they can use the internet to find distant relatives, explore the stars, learn a new language, watch free courses from universities, and to play games with their friends and families. The internet provides a mechanism for seniors to explore a vast and interesting world, enabling them to travel to places they may have never dreamed existed.

To read more about older adults and the internet, check out the following resources:

Pew Research Center

The Pew Research Center for Internet and Technology gives facts and figures about older Americans and their internet usage over the years.

The Telegraph

Older adults are trying to stay connected with their younger family members and this article gives tips on how to make the elderly comfortable online.

Deseret News

Social media and the technology of the internet are changing things for seniors - they can connect with family and be free from isolation.

Center for Technology and Aging

Organization that seeks to improve the independence of older adults dealing with chronic health care issues.

CNN

CNN

Older adults can use technology to keep their independence according to this article by CNN.

NIH

Study measuring frequency of technology use between older adults and younger adults by the National Institute of Health

Top Ten Tips for Online Safety

- **Do not trust someone simply because they know personal information about you.**
  It's easy for a scammer to do some basic research about you and your family and to use that information to gain your trust.
- **Never send money to someone you do not know.**
  Submit scams like these to organizations like the AARP's ElderWatch group.
- **Always validate someone's identity before trusting him or her, especially when being asked to send money.**
  It's very possible that the person contacting you through email or social media isn't who they claim to be.
- **Keep your computer's software updated.**
  Set up your computer to automatically install security updates. If you need help, request a friend or family member for assistance.
- **Use antivirus.**
  Some scammers take advantage of security issues in your computer to steal information or make it unusable. An antivirus application helps protect your computer from this type of malicious software.
- **Back-up files on your computer or tablet.**
  Both personal computers and tablets can be set up to save back-up copies of your important files and photos.
- **Do not share private information on social media.**

While you might want to share your upcoming vacation plans with your friends and family on Facebook, strangers and scammers might also be able to see that post as well. Be cautious and ask a friend or family member to help you configure your privacy settings on your social media account so that strangers (friends of friends) aren't able to see messages that you intend to only be shared with your friends and family.

- **Use a password on your computer or tablet.**
  While many scammers try to trick you to install malicious software online, there are still many thieves that prefer to gain access to your private files in person. Adding a password to your computer or tablet, and not sharing that password, helps protect you and your private information from being stolen.
- **If something seems too good to be true, it likely is.**
  While a page on the internet might say that you've won tons of money or prizes, that message isn't unique to you. The message is coming from a scammer, and they want to take advantage of you. Other sites in this area also warn about your computer being infected. Don't install the software that they recommend. A scammer has likely created it.
- **When in doubt, ask a friend or family member.**
  The internet is a large and ever expanding place, and technology continues to change. Consider asking for a friend or family member to look over a potentially dubious email messages or websites. You may also report potential scams to the various sites listed above.

Conclusion

> The internet is a lovely place for watching funny cat videos, playing online Scrabble with a friend, or looking at photos of your grandchild's first day at school. It can also be a sometimes-dangerous space. The first step to being safe online is knowing that there are people that want to steal your sensitive information or scam

> you out of your money. Like the physical world, there are some very well intentioned people online. At the same time, some people have begun to use the internet to commit crime. Being aware and wary of common internet-based scams will help you to use the internet more safely and to thoroughly enjoy your time online.