The Dark Side of the Internet
Safety and Security

The internet creates excellent opportunities for seniors to meet people, conduct business, plan travel, access records, stay in touch with friends and family, and support hobbies and entertainment interests. You can learn how to take advantage of the opportunities without falling prey to predators so you can have peace of mind when you go online.

Factors that contribute to increased risks for seniors

Every age group has unique vulnerabilities in addition to general Internet risks, and seniors are no exception. Few entirely new types of crime are created to target seniors; the issue lies in how existing crimes are tailored specifically to exploit older Internet users.

For example, while an online scam targeting minors is going to promise trips to Disneyland or cool toys scams aimed at seniors are more likely to offer discount drugs and low-cost insurance. Phishing scams frequently target seniors with 'bank notices' or official looking 'government documents'.

In addition to being targeted for different types of crime, seniors may share characteristics that make them vulnerable online. Here are some of the major factors that make seniors vulnerable.

Lack of computer skills

Though many seniors are very computer savvy, many more are not. Often their computers are not properly secured. Even when you have installed security software, it is critical that you set up automatic updates, turn on a firewall, use secure passwords, and so on.

If you do not feel that you are able to set up your computer's security, it may be well worth hiring a computer technician from a reputable company to review your settings for security and fix any problems you may have. Make sure you have checked the company through the Better Business Bureau and that whoever comes to your home is fully licensed and bonded.

However, keep in mind that giving access to your computer may put your private information at risk. Because you may be anxious about using the computer you may be more likely to believe someone who claims that there is something 'wrong' on your computer and more willing to follow the instructions they give you to 'fix' it. Sometime scammers ask for remote access to your computer so they can help you.

Brought to you by

COMTECH SOLUTIONS

Unless you trust someone such as a friend or family member to keep your best interests at heart and respect your privacy, do not give them access to your computer.

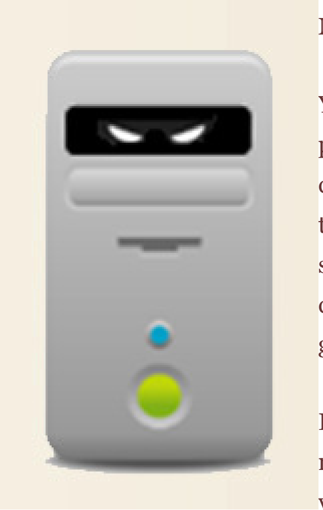
Lack of Internet skills

Though many seniors are cutting edge users of Internet services, most of you are beginners when it comes to computer technology.

Just spending more time online will help you feel more comfortable with the ins and outs of navigating online and interacting on Web sites. Once you've familiarized yourself with the tricks scammers and some less reputable companies use, you can simply avoid them. There are many Web sites, books, and courses offered for every level of user. Many of these courses are offered at low cost through colleges across the state.

An important thing to note is that people who are computer savvy, perhaps because they worked with computers before retiring, are sometimes more at risk online because they believe that being computer savvy means they are Internet savvy – but in reality navigating the Internet safely is more a matter of understanding human behavior than understanding technology.

Understanding the reach of content posted online, how criminals try to deceive you, or the trustworthiness of a site for example, has nothing to do with how well you can use a computer.



More Trusting

You have a wealth of experience in judging the character of people you meet in person, but you have probably developed fewer skills for assessing the character of the people and companies you meet online. You are typically more trusting and respectful of official looking material than younger generations, so are more apt to fall for scams. And you are more worried about notices that claim there is a problem with your information that might somehow sully your good name.

In the online world, unless you know for sure with whom you are dealing, you must assume that you could have landed on a 'look-a-like' site trying to scam you.

No one can build a fake bank or store on some street corner for a few days, so you never have to worry about whether the bank or store is real. When you enter, you quickly get a sense of whether it is a reputable place or not. If you have a problem with a purchase you can march right back through the door and demand service.

On the Web, those physical attributes and clues are all gone. Anyone can build a Web site that looks as official and legitimate as any other site for very little money. They can scam search engines to make their Web sites show up as one of the first results when someone runs a search. Anyone can copy the exact look and content of any other Web site. This means that the fakes are sometimes very, very hard to identify no matter what your age.

Seniors and social networking sites

Seniors who use social networking sites that cater to older users are targeted with quizzes and surveys that often have very invasive questions about your health, wealth, and personal lives. Quizzes are created for revenue. Ask yourself who profits from you answering the questions and who else gets to see your answers. Understand that any information posted in these quizzes is likely to be used by many companies. Answer a medical quiz and you may find your insurance claims, even your ability to get insurance, are affected. Quizzes can also generate targets spam 'offers' based on your answers.

Cyberbullying and seniors

Cyberbullying is not just a problem among young people; seniors are also affected. One clear difference is that, whether you want to face it or not, cyberbullying of seniors is most often done by family members. Cyberbullying 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 target.
- Financial abuse aimed at finding their account information, setting up online access to their accounts, and stealing their money.

If you don't let people abuse you in person, don't let them use technology to do so online.

Online dating and seniors

Online dating is becoming very popular for seniors, some of whom have lost a partner due to death or divorce. While this is an excellent way to meet new people, it is also a way for predators to find potential victims. Their goal may be to get your money, or inflict physical or emotional harm.

Confidence tricksters make their living by building trust – and a lonely senior who has perhaps had a long relationship with one partner and is now seeking another person to share life with is often a very easy target.

Information exposure and seniors

Seniors generally buy into a few myths about information exposure online. The first myth is that if you don't use a computer you aren't exposed online. In reality, just because YOU didn't put information online doesn't mean it isn't there – virtually everyone has information online that has been placed there by several sources.

Here are a few examples:

- Publicly available government records will show if you own a home, vote, have a criminal record (or speeding ticket), and much more.
- Your home is listed online and its image is available through any Internet mapping service.
- Unless you have been very careful to ensure your phone number isn't in a phone book, it's online. Even if you have been careful, type it into any browser window and see if it brings back your information – chances are that it will.
- If you donate to a charity without doing so anonymously the charity's Web site probably lists you among all their donors as a thank you.
- If you volunteer with an organization, belong to a church group, sports group, action committee, and so on, chances are they list you on their Web site.
- If your grandchild has a blog (an online journal) your name, location, and income may have been mentioned online.
- If a relative enjoys genealogy, your name and your relatives names may be online.

The second myth is that if you haven't fallen for an Internet scam you won't be the victim of an Internet crime. The truth is that you may never know what the Internet connection is (or even if there was one) in most crimes. For example, information found online may give a criminal the incentive and means to rob your home or steal your identity.

The third myth is that the information you post online will only be looked at by people who you know. Actually everything on the Internet is being copied and referenced – constantly. Even if you take your information off the Internet, a copy of it may still be there. Reduce exposure by removing personally identifiable information from anything you or family members post online.

Tips for seniors to stay safer online

- Never trust a link sent to you by someone you don't know. By clicking the link you may be taken to a site that may look like your bank or credit card company, but isn't. One thing a criminal can't fake is the actual Web site address of a company or bank. Instead of clicking a link in an e-mail, search for the Web address using a search engine to find the real one. Use that to ask the company about the message you received, or call using the number listed on your statements. Mark the real site as a favorite in your browser so that one click brings you there safely every time.
- Never trust an e-mail that asks for your personal or account information (called a phishing scam). These usually seem convincing (the shabby ones have spelling errors, but the high quality scams look impeccable). No bank or reputable company is going to send you an e-mail asking you to correct your information, validate your identity, re-enter your password, and so on.
- The smarter scams often contain text warning you against fraud. They do this because many people believe that an e-mail that warns them to be careful must be legitimate. That is not always true. This also extends to sites that claim they have protections in place for your privacy and security.
- Never respond – or even open an e-mail with a deal that is too good to be true unless it is from a company that you know well and expect to get these kinds of offers from them. Scammers want you to react without taking time to think things through, their e-mails frequently sound urgent, such as:
  - …"if we don't hear by tomorrow your account will be closed" (and you'll notice that the date of "tomorrow" never is listed).
  - …"this offer won't last, order now to ensure"…
- Never believe that someone you don't know is going to give you money.
- Do not believe a person from another country who just needs you to "help transfer funds" and they need your bank account number to do so. Such scammers promise to give you a huge amount of money for helping them out. The result is an empty bank account.
- If you never entered a lottery, you did not win the lottery. Such scams ask you to provide your information and bank account number so they can transfer your prize money. Don't. The result is an empty bank account.
- Don't believe a really rich, famous person just wants to help you out… and that the celebrity also mysteriously needs your address, phone number, bank account information to do so. The result is an empty bank account.

Guard your information well. It is better to be rude than to be ripped off, so demand validation, verification, and authentication before giving your information to anyone. If you still feel uneasy, say no or check further. With a little knowledge the internet can be a safe and useful source of fun, information and communication.