ConnectSafely

www.ConnectSafely.org

Senior's Guide to Online Safety

Updated April 2018

Most American seniors are now online. As of 2018, nearly 66% of Americans over 65 were Internet users, according to a Pew Research Center survey. That number is getting bigger all the time, and for good reason.

The Internet is a great way to read the latest news, stay in touch with family, get medical information and manage appointments, renew prescriptions, and access medical records. It's how many of us shop and bank without leaving our homes. For an increasing number of seniors, it's a way to stay in the workforce and even launch a new career or business. And some seniors are going online to make new friends and to find romantic partners through online dating. Like all powerful tools, the Internet and mobile technologies come with some risks. These risks can be managed as long as you follow some basic rules of the road. So, for all the great things we cover in this guide, we also go over some precautions to help keep you safe.

The reasons seniors go online are as varied as the users themselves and include:

Participating in social and cultural activities

Getting medical advice and information including doctor reports and test results

Online banking, shopping and investing

Meeting new friends or romantic partners

Making travel arrangements

Keeping in touch with loved ones

Sharing and viewing pictures

Exploring and sharing political views

...And much more.

Communicating with friends and family

Whether it's text, talk, or video, the Internet is a great way to communicate.

You may remember spending a lot of money on long distance calls and keeping them as short as possible to keep costs down, but now you can call just about anywhere in the world for free or a couple of cents a minute, and make free video calls with services like Skype, Apple FaceTime, Google Voice and Facebook Messenger. For better or worse, old-fashioned letters have been largely (but not completely) replaced by email. And thanks to social networking services like Facebook, it's easier than ever to keep up with your friends and family, and let them keep up with you.

Social media allows you to exchange ideas, photos and videos, and even plan events with friends and family living far away.

But don't think that social networking is just for young people. A 2016 Pew Research Center study found that 62% of online seniors use Facebook, and that's just one of the major social networking services.

Stay Safe Tips

Use strong and unique passwords for your social media accounts and never share your passwords with anyone, unless you've designated someone you trust to manage your accounts. One reason for this precaution is to prevent someone from using your account to impersonate you– perhaps asking your friends and family to "help you out" by wiring "you" money in an "emergency," which is a common scam.

Make sure your passwords are long–at least eight characters–and include numbers, upper and lowercase letters and symbols; avoid using names or dictionary words. At ConnectSafely.org/passwords, you'll find tips and information on how to use multi-factor authentication and fingerprint recognition for more advanced security.

Most services have settings that let you control who can see what you post.

Use privacy settings. Most services have settings that let you control who can see what you post. Facebook, for example, has extensive controls, letting you post to only friends, your friends and their friends, or everyone on Facebook. You can also limit specific posts to a smaller group like only family members or specific people (you'll find more on privacy settings at ConnectSafely.org/seniors). Some services give you a choice between private and public posts, with private going just to people you designate. Before posting to any service, it's good to get to know its privacy policies and settings. There are also privacy settings for smartphones that can restrict who has access to your location, contacts, and other personal information.

Think before your post. Whether it's a picture, video, or comment, what you post and what you share is a reflection on you. Make sure you feel good about being associated with anything you say online and be sure not to post anything that you wouldn't want to share with the world. Even if you're using privacy settings to limit the audience, there is always a chance that what you post can be copied and shared by others.

Dealing with "spam" or unsolicited email can be challenging. It's pretty common to be plagued by junk email. Simply getting these messages isn't necessarily dangerous, but it can be annoying. In some cases they can be from companies you've interacted with in the past and, if they are legitimate companies, there is probably a link to a page where you can safely ask to be removed from their list. But if they are truly "spammers," they won't stop, even if you ask them to. The best thing to do is make sure you're using whatever spam filter is provided by your email service. Visit ConnectSafely.org/seniors for information on how to use the spam filters on popular Web-based email services like Gmail, Yahoo Mail, Comcast, Outlook and AOL. Avoid clicking on links in unsolicited email, as there is a chance they could link to sites designed to scam people or infect computers with malicious software.

Report abuse from anyone, including friends, family and caregivers.

Report abuse from anyone, including friends, family and caregivers. We hear a lot about children being "cyberbullied," but it also happens to adults, including seniors. If you are getting messages on social media or in email that are threatening, mean, extremely angry, accusatory or in any way abusive, don't respond; reach out for help and support from someone you trust or from adult protective services or law enforcement, and report the behavior to the site or service. All major social media companies, and online and mobile service providers have employees that respond to abuse complaints. ConnectSafely has links to abuse and privacy pages for major social networking and Internet and mobile service companies at *ConnectSafely.org/seniors.*

Scams

If an offer, email, or message sounds too good to be true or just seems plain fishy, go with your gut and do some additional checking.

Here's a roundup of common scams:

Personal emergency scam: Scammers email or post social media messages that appear to be from someone you know saying they are in distress, such as having their wallet stolen or having been arrested. If you get such a message, find another way to verify if it's true, such as reaching out directly to the person. If you get such a message from a friend, there is a good chance that their account was hacked and that it's a criminal who is out to steal your money.

You owe money scam: Be wary of emails that claim you owe money. If you hear from a bill collector or a government agency about money "owed" by you or a family member, don't respond unless you are certain it's legitimate. It's pretty common for scammers to send "bills" to people who don't actually owe them money.

Online dating scam: Many people have found love via dating websites, but others have been scammed out of money by online con artists. For tips on safe online dating and a list of red flags, see the section "Meeting new friends and romantic partners."

Infected computer scam: You might get a call from "Microsoft," saying your computer is infected or vulnerable to hacking, with an offer to fix it for you. Hang up. Microsoft and other reputable companies never make these calls. These are criminals trying to steal your money and plant viruses on your machine. Also be suspicious of any messages in email or that pop-up on your computer, in your Web browser or on a mobile app warning you of a virus or a security risk. If you have reason to suspect that your device is at risk, consult a trusted expert but never download software or apps that you aren't certain come from legitimate sources.

Speak out and don't be ashamed if you're victimized.

Speak out and don't be ashamed if you're victimized. Criminals are very good at what they do and there have been lots of very smart people who have been victimized online. If it happens to you, report it to a trusted person and law enforcement. Even if you let your guard down, it's not your fault if something bad happened to you.

Meeting new friends and romantic partners

The Internet is a great place to meet people, whether it's someone who shares your passion for an activity or cause, or a potential romantic partner.

There are many online groups and forums where people with similar interests meet and that sometimes leads to getting together for all sorts of activities ranging from walks and bike rides to meetings to discuss issues or political candidates.

Online dating is also very popular with seniors and many have met great people via online dating sites

Online dating is also very popular with seniors and many have met great people via online dating sites, leading to friendships, romantic relationships and sometimes marriage.

Stay Safe Tips

If you do arrange an in-person meeting with someone you meet online, **make sure the first meeting is in a public place**, like a restaurant, and bring a friend or at least let others know where you're going to be. Bring along your cell phone and have a friend call you during the meeting just to make sure all is going well.

Be aware of online dating scams. There are cases where seniors, as well as younger people, have been scammed into parting with their money and left heartbroken. With anyone you meet online, there is always the possibility they may not be who they claim to be.

Watch for red flags. They can include a person who claims or looks to be a lot younger than you or who sends you a picture that looks as if it came from a fashion site. The FBI warns people to be careful about anyone who claims to be from the U.S. who is traveling or working overseas and suggests that you only deal with reputable dating sites. Other red flags include the person pressuring you to leave the dating site to communicate via email or text messaging or someone who professes instant feelings of love. Be suspicious of anyone who is never actually available for a phone call or face-to-face meeting.

Look for abnormalities in the way a person writes and the type of grammar and words they use. It may not mean anything but it could be a sign that they are in a foreign country and may have no intention of actually meeting you.

Don't send money. Be especially suspicious and don't send money if the person asks for money, perhaps to get on a plane to come meet you or to help them deal with a personal or family crisis.

Sharing your views

Social networking sites are a great way to exchange views on a variety of subjects ranging from sports to politics to religion to the latest technology. As you can imagine, people sometimes engage in spirited debates on these and many other issues; there's nothing wrong with that. In fact, it strengthens our democracy to have a healthy exchange of ideas and opinions. Sometimes these debates–especially when politics is involved–can get a little too spirited, so here's some general advice.

Keep it civil. It's OK to disagree but try to be respectful of other people. Name calling and derisive comments are almost never effective and wind up alienating not only the person they're aimed at, but others as well. If someone is mean or disrespectful to you or others, it's best not to engage in a war of words, but to just move on. There are plenty of other people you can interact with. And know that if you express your opinions, there is always a chance that others will disagree, and some may be disagreeable in the way they disagree. Know fact from fiction. Somethings online are simply not true. Sometimes they're posted to deliberately smear a public official, political candidate, or celebrity and sometimes they're just honest mistakes. Don't believe everything you read and never forward or share something if you're not sure it's true because then you're the one who's spreading false information. If you see something questionable on a website, do research on a reputable site. Sites like Snopes.com and Politifact.com do a good job separating fact from fiction.

Social networking sites are a great way to exchange views

Online shopping, banking, charity and travel

The Internet has had an enormous impact on the way people shop, do their banking, make investments, plan travel, and even how they pay their taxes.

In the vast majority of cases, the experiences have been positive. Online shopping allows you to find items–which are sometimes hard or impossible to find in local stores–and typically get the lowest possible price by comparing prices with a variety of merchants. Online shopping can be easier than driving to a store–especially for those with limited mobility. It's also a convenient way to buy gifts for faraway friends and family. Yes, there are risks associated with shopping online, but they can be managed. Besides, there are also risks associated with driving to a store to make purchases.

Online shopping allows you to find items–which are sometimes hard or impossible to find in local stores

Online banking and investing is another great convenience. With a click of a mouse or a touch of a smartphone, you can transfer money between accounts, pay bills, and make investments.

Stay Safe Tips

Use strong and unique passwords. Once again, strong passwords are essential, just as they are with email and social media accounts. Never share your passwords with anyone, unless you have designated someone you trust to manage your accounts. Make sure your passwords have at least eight characters. Include numbers, upper and lower case letters, and symbols, and do not use names or dictionary words. At ConnectSafely.org/passwords, you'll find tips and information on how to use multi-factor authentication and fingerprint recognition for more advanced security.

Make sure your passwords have at least eight characters

Don't click on links in email or on social media from banks, credit card companies, government agencies, or other organizations, unless you're 100% certain they are legitimate. There is a common scam, called phishing, where someone sends you a link to what looks like a legitimate website, but it's actually a scam site created by criminals to steal your login or other personal information. Even if the company name is part of the Web address, it could still be a scam. Your safest bet is to type in the Web address like you normally do and if in doubt, call the organization.

Be wary of any offer that's too good to be true, such as being told you've won a contest that you didn't enter, or you're being offered an incredible price on a vacation or product way

below what you'd expect to pay. Be especially careful about offers for low-cost medications or medical coverage.

Only shop at reputable online merchants. Be careful about any online merchant that you have never heard of. Many are legitimate but some might be out to steal your credit card number or other financial information, or simply fail to deliver what you've paid for. When in doubt, ask someone familiar with online shopping or do some online research to see if there are reviews or comments about the merchant.

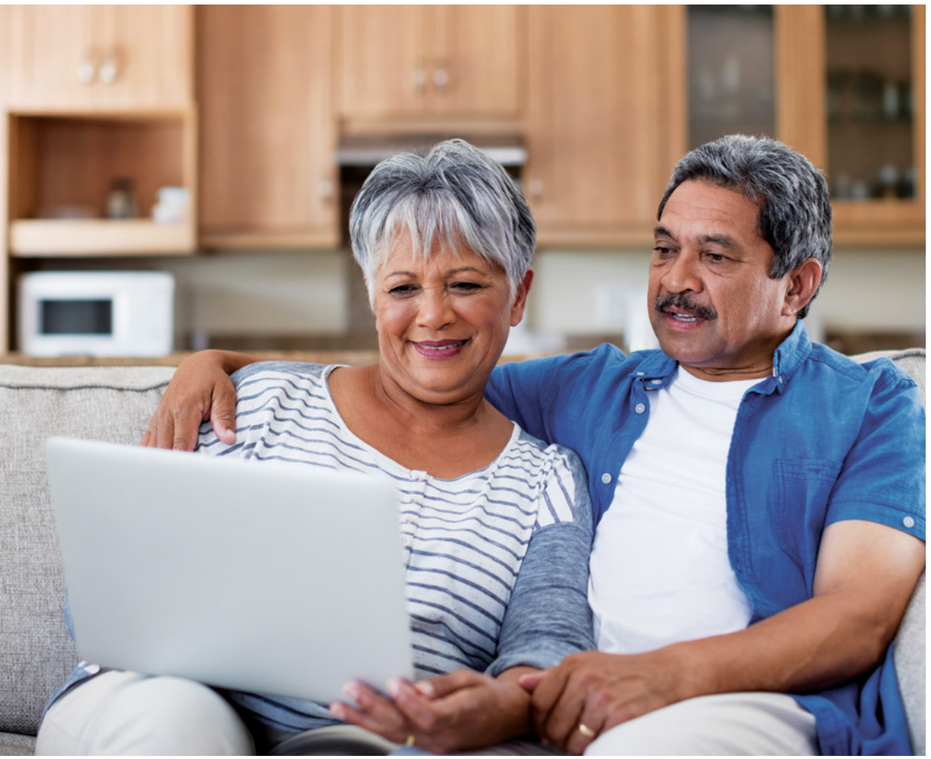
When shopping or banking look for secure websites with an https in the browser's address bar. The "s" stands for "secure." If it's just http, it's not a secure site. If you shop or bank using a mobile app, be sure it was issued by that company. Look for reviews from others or ask an expert if you're not sure.

Use credit cards if possible, otherwise use debit cards or safe online payment services, such as Paypal. Never send cash, cashier's checks, or money orders. Even sending a personal check can be dangerous. It's best to use a credit card because, if there is a dispute, the credit card company will stop the charge or refund your money while they investigate your claim. Debit cards also have protections but sometimes you have to wait to get your money back. Services like Paypal, Android Pay, and Apple Pay also have some protections but credit cards are still the best bet.

It's best to use a credit card because, if there is a dispute, the credit card company will stop the charge or refund your money

Be careful before you click. There are certain things that you may not be able to undo, such as buying or selling the wrong stock or buying a non-refundable flight or hotel room. Carefully review all transactions before confirming them. If you do make a mistake contact the company right away to see if it's possible to undo it. Many online merchants have a cancelation feature that lets you back out of a purchase, but you must do so promptly. Once an item is ready to be shipped it may be too late to cancel

the order. You can often return your purchases, but you're likely to have to pay for return shipping.



Make sure you understand the **return policies** from online merchants and know all of the charges, including shipping, handling fees, and taxes.

Do some research before donating to online causes. Crowd-funding sites like Kickstarter, Indiegogo, and GoFundMe are great places to be among the first supporters or purchasers of new products, donate to worthy causes and organizations, and even provide financial support for people with a compelling need, but you should proceed with caution. Read all the fine print and do a little research on the person or organization behind the pitch. If they're raising money for a cause, try to find out if it's real, and if they are launching a cool new product, make sure their pitch is realistic. When in doubt, move on.

Protect against identity theft. Never enter your Social Security number online unless you know you are at a legitimate site that has a real need for that information, such as applying for a bank account, credit card or loan (from a legitimate financial institution), or getting a credit report (such as the legitimate free annual credit report services authorized by the Federal Trade Commission). Unless you're sure it's a legitimate site, avoid posting your full birth date and place of birth, and be cautious when asked to enter any other personal information, such as your home address. Legitimate media sites like Facebook and financial institutions may be required to ask for your date of birth. Only disclose credit card numbers to legitimate online merchants. When in doubt, do some research to see what other people and reviewers say about them.

Even if you don't bank online, there is still a risk that you could be a victim of fraud.

Monitor your online financial accounts. Look for recent activity to be sure that there are no fraudulent charges to your credit, debit, or bank accounts. Check your online investment accounts to make sure there has been no unauthorized activity. If you find something suspicious, report it right away to the financial institution's fraud department or the toll free number on your credit or debit card. Even if you don't bank online, there is still a risk that you could be a victim of fraud. Let the institution know right away if there is an issue. In most cases you are protected against fraud but you must report it.

Charity scams. Most charities have websites and the option to donate online. That's fine as long as you're sure you're on the right site and that it's a legitimate charity that you support. Be careful if you get an email from what appears to be a charity asking you to make an online donation. If you're not familiar with the organization, check it out at CharityNavigator.org and if you are going to donate online, be certain that you're going to the charity's legitimate site. To be safe, type in the charity's Web address in the browser rather than clicking on a link.

Health and wellbeing

There are some excellent sites and apps that provide medical information and advice.

Some are useful for such things as understanding how specific drugs work or getting an overview of an illness or condition. There are forums where people dealing with conditions share experiences and answer each other's questions, and most companies that make drugs and medical equipment have websites with details about their products. These sites can be extremely valuable, but think twice before acting on anything you read on any website or app. Begin by knowing who is behind the site or app. In general, sites operated by the government (ending in .gov) or well regarded medical institutions like Mayo Clinic have reliable information, but be aware that some commercial sites, including ones operated by pharmaceutical companies, are there to promote products. That doesn't necessarily mean that they don't have useful information, but know who is behind them.

There are other sites whose information has not been vetted by medical professionals. Even with legitimate sites, don't rely on online advice for diagnosing an illness. Having a symptom association with an illness doesn't necessarily mean that you have that illness. Always check with a medical doctor or trusted healthcare provider before taking any action or medications. Never enter any personal or health information on a site or an app until you are certain that it is legitimate and will respect and protect your privacy. You'll find a list of reputable health sites at **ConnectSafely.org/seniors.**

You'll find lots of information online about food, including nutritional information and some great recipes. You'll also find lots of information about exercise, including videos on YouTube and other sites that show you how to do just about any exercise you can imagine. These instructional videos can be extremely helpful but be aware of your own limitations and consider consulting a doctor or a personal trainer before engaging in any new exercise. You'll find links to some great food and fitness sites and apps at **ConnectSafely.org/**

Having a symptom association with an illness doesn't necessarily mean that you have that illness.

Dealing with Medicare, Social Security and the IRS

There are ways that citizens can interact with government agencies online.

You can, for example, use websites like TurboTax.com to complete and file your tax returns; get Medicare information at Medicare.gov; and access information about Social Security benefits from SSA.gov. The IRS's website (www.IRS.gov) also has forms and plenty of information for taxpayers.

Get Medicare information:
Medicare.gov

Access information about Social Security benefits from:
SSA.gov

The IRS's website:
www.IRS.gov

! Stay Safe Tips

Beware of any calls or emails from someone claiming to be with the Internal Revenue Service. They are scams. If the IRS thinks you owe back taxes, they will send you a paper letter the old-fashioned way. When in doubt, check with an attorney or a tax advisor, or call the IRS directly. Dealing with Medicare, Social Security and the IRS.

The Social Security Administration will not use email to ask for personal information, such as your Social Security number or date of birth.

Only use legitimate sites or software to file taxes. The IRS offers advice for taxpayers who wish to "e-file," including a number of authorized services that can file your federal taxes for free. You can even prepare your taxes on a smartphone. Go to ConnectSafely.org/seniors for links to useful IRS sites as well as legitimate online tax preparation companies.

Don't send personal information in response to emails from Social Security or Medicare. The Social Security Administration will not use email to ask for personal information, such as your Social Security number or date of birth. When in doubt, call your local Social Security office or 800-772-1213. Be suspicious of anyone posing as a doctor, healthcare provider, or insurance company that asks for your Medicare number, or who claims to represent Medicare. When in doubt, call Medicare directly at 800-633-4227.

Security 101

1. **Be smartphone savvy.** Smartphones can track your location and reveal information about you, including your contacts. Be careful to only download and use reputable apps and be sure to password (or fingerprint) protect your phone. Know how to use tools to find or erase personal data from lost phones. Find more at ConnectSafely.org/cellphone-safety-tips.

2. **Secure your Internet router.** There is likely a small device in your home, called a router or broadband modem, that connects you to the Internet. That device has a password and username and sometimes the default passwords are very easy to guess. Routers can be hard to configure so if you're in doubt, contact an expert or your Internet service provider for advice on how to change the password.

3. **Protect your devices.** Ensure devices are password protected and, in the case of computers, make sure you have good security and firewall software in place. If you need help, reach out to knowledgeable friends or family, or your Internet service provider or mobile operator. Comcast and some other Internet Service Providers offer free anti- virus software, or you can purchase or obtain free security software from a reputable company such as the ones listed at ConnectSafely.org/securityvendors.

4 **Reach out for help.** There are many great places to get help with computers, smartphones and other technology. Many senior centers, some schools, and some religious or community groups offer free or low-cost classes. There may be family members who can help, but don't overlook others in your community such as tech-savvy high school students (call a local school and see if a student can be assigned to help you in exchange for community service hours). Both Apple and Microsoft have stores that offer free advice on products they support and you might also be able to get help from staff at other local computer or electronics stores. Always feel free to contact your cell phone carrier if you have any questions about your phone or service, including whether you're on the most economical plan for your needs.

5 **Avoid pressure to buy what you may not need and review your service plans.** Even legitimate services and merchants may sometimes try to talk you into buying equipment or services you may not need. It's not necessarily a scam, but could be that they simply don't understand your needs. When buying a cell phone or Internet plan, think about whether you need all the data they want to sell you, or whether you need that extra speed for an extra price. Once you've established service, review it periodically to see if you're using most of the data or other services you're paying for. You may be able to save money by downgrading your service.

Advice for seniors considering enlisting help from family members or caretakers.

Most seniors are self-sufficient but, as we age, sometimes we need a bit of help. There are many seniors who rely on family members, professional caretakers, or professional advisors to help them with their finances, taxes, legal affairs, housing, and other issues. Sometimes it's helpful or even necessary for caretakers to have access to a senior's online bank and investment accounts, medical records, and other online sites. There are various ways that caretakers can access a senior's accounts but it generally

Most seniors are self-sufficient but, as we age, sometimes we need a bit of help.

requires some type of power of attorney or other legal authorization. When in doubt, consult an attorney. If you are a senior considering enlisting someone else's help, be very careful to only authorize someone you trust completely. Whether you're the person being helped or the caretaker, consider consulting with an attorney to make sure that all authorizations are in order. The Consumer Financial Protection Bureau offers advice on having another person help you with banking and finance at ConsumerFinance.gov. One of the discussions on that page includes the advantages and risks of setting up a joint account.

Whatever you do, think very carefully before giving anyone–even a family member–access to any of your accounts including financial, health, or social media.

For more, including lists of agencies you can contact if you have been victimized, visit **ConnectSafely.org/seniors.**

www.ConnectSafely.org

ConnectSafely

INTERNET ESSENTIALS from Comcast

www.ConnectSafely.org