Keeping Seniors Safe Online [New Guide]

Esther Kane 10/06/2020 Security

More and more seniors and older adults are using the Internet these days for everything from shopping to catching up on the news to entertainment. Nevertheless, what they may not be aware of are the dangers that lurk on the Internet – some specifically targeting seniors.

10 Tips On Keeping Seniors Safe Online

Following are 10 strategies that you can use to keep yourself and/or your senior loved ones safe online.

1. Make Your Passwords Strong To Decrease The Chances They Can Be Cracked

We all struggle with having to manage so many passwords – I get it. But if your passwords are too easy to decipher – then your information online will be that much easier to get into.

Many seniors make these password mistakes:

- They use a familiar phrase like their birthday, address, a grandchild's birthday, their dog's name, etc.
- They use the same password that they've used for years or maybe slightly adjust it with a new number
- They use the same password for everything

Anything familiar that can be tied to you or your family can be found online and used by hackers and scammers as your password.

Check out these third party password manager programs that may make generating and keeping your passwords much easier.

How Do Hackers And Scammers Get Your Information?

My mom-in-law only uses her computer to read her email and to play bridge games. So she has never entered personal information on any online account.

Yet, when I type in her name and the state, she lives in – the 3rd search result on Google is her. Along with the city, she lives in, her current age, her birthdate, her political party, her address, her current neighbors, her children's names and other relatives.

All this information is there for me to view free – with just one simple search. So yes, hackers and scammers can find out a lot more about you than you can think.

What Makes A Good Strong Password?

Here are some tips on how to make the best possible passwords for your online activities.

- Never use a full word or phrase. Examples would be "iloveyou" or "apples".
- Never use a series of numbers. Examples would be "223344" or "6789"
- Mix your passwords with capitalized letters, numbers and symbols. Example: tbRa91@VrpSn6&GxPL
- The more nonsensical the password can be, the better
- Longer passwords are better than shorter ones.

Read our article, What Is A Good Way For Seniors To Remember Passwords, for more information about choosing online passwords.

2. Be Careful When Entering Personal Information On Unfamiliar Websites

More and more of us are shopping online, which is wonderful. But you want to be careful where you do your shopping.

There are 2 reasons to be cautious:

- A website can look like a very legitimate establishment but looks can be deceiving, especially online.
- A smaller online store may not have the security measures that the larger ones do so even though they may be legit – their database may be hacked and then your personal information will be visible (and usable) by the hackers.

I would recommend to do a little research and look for these signs:

- The website address MUST have https:// instead of just http: This indicates that the site is under a secure SSL certificate.
- Check the site to make sure there is a contact phone number and go ahead and call that number to make sure that you can actually speak to someone.
- Your credit card information should be processed through a merchant account like Paypal or Shopify, etc. If they are asking you to put that information on a form – then I would recommend to back off from making that purchase.
- Check the domain at WhoIs to see how old the site is and any other information you can find.
- Another tool to find the history of a website is Internet Archive. This may give you additional information on what the website used to look like or what it used to be.
- You can also try to check on the company on sites like Yelp or LinkedIn. See what people are saying about it on Facebook and Twitter.

If you are just not sure and want to stay as safe as possible then I would recommend to shop only from known organizations such as Amazon, Wayfair, Overstock, Walmart, Target, etc.

3. Always Have A Secure Internet Connection

Many seniors use a service like Geek Squad or a computer technician to set up and maintain their systems. So, you don't have to fret about the technical details here but basically, there are 4 things you should do to secure your internet connection:

- Make sure the router is using WPA2 connection
- Make sure the router is set up with a password
- Activate the firewall that comes with your operating system
- Set the settings of your browser(s) to optimal security

These professionals who set up your computer system will (they certainly should) do all of this for you.

4. Install An Antivirus And Malware Program On Your Computer

An antivirus and malware software program like Norton is a very important addition that everyone should have on their computers.

You can purchase one program that has both antivirus and malware services or you can purchase them separately. The Norton software program has the two integrated.

These do come with yearly fees and as someone who has lived through a few attacks and hacks I can tell you that the investment in these programs is well worth it.

5. Avoid Clicking On Links In Your Emails

Emails are the easiest way that hackers and scammers can take advantage of seniors.

There are four tips about emails that I can give you that will greatly help to keep you safe…

- Never open a forwarded email. These are emails that have FW: in the subject line. If there is a virus in that forwarded email – your computer may get infected.
- Never click on a link in your email unless you know absolutely for sure that it is a legitimate website address. Instead, go to your browser and go directly to that website (the main URL) and from the website, go find the page they are referring you to.
- If you do not recognize the name that the email is from – don't open it – delete it. The general rule is "When in doubt, throw it out."
- Use your email program's filter to delete certain email immediately so you won't even have to deal with it. You can set your filter to delete emails with certain words like "Viagra" and you can also create filters to delete emails from certain websites as well.

I would recommend that if you are not familiar or comfortable with any of these that you ask the pros at Geek Squad or your computer technician to do these for you.

6. Be Careful About What You Download And Where You Download It From

Another easy way that scammers can target seniors is through downloads.

Whether the prompt is from a website, an email or an ad on Facebook or other social media program – the safety tip is the same. Unless you are absolutely sure that the website address is valid – don’t download it.

Instead, go directly to the website that the download is supposed to be on and find the program that you want to download.

7. Be Careful About Purchasing Items Through A Social Media Site

Social media programs, like most Internet programs make money from advertisers. So, they push advertisers to everyone who uses them.

Because advertisers pay for their placements, there are very little (if any) security checks to ensure that these advertisers are legit, that they provide what they promise, etc.

So, because of this I strongly recommend to avoid purchasing anything that is advertised either on a search engine or social media program like Facebook.

Note: I personally have purchased 4 items from Facebook and every single one of them was not as advertised and certainly not worth what they were selling at. This is my personal experience.

I very strongly recommend that you watch the documentary Social Dilemma on Netflix. It will explain much of how the Internet and social media companies work.

8. Be Careful About What You Say Online

As many individuals across the world have learned, what you say online matters in more ways than one. It’s not always easy to delete your comments and even if you can do so – it may be too late.

So, be careful and thoughtful about what you type in – especially on any social media program.

My rule of thumb is to try to wait 24 hours before I respond to anything.

9. Be Extra Cautious About Who You “Meet” Online

Many seniors can be lonely. Whether they are divorced or widowed or have lost many of their inner circle friends and family – they find themselves in the situation of being alone and lonely.

There are a few Internet programs targeting seniors for dating and activities, etc.

Be careful about who you end up having conversations with online. In fact, there are many services available that can run a background check on anyone – you may feel safer to purchase this for someone you may be interested in.

This is no guarantee of course that you will be 100% safe but it is an extra step that is recommended.

10. Designate One Person You Trust With The “Key” To Your Data

If you are alone it’s always a good idea to have a designated person – a type of executor who can find your vital information if they need to. Some examples of what you would trust this person with are…

- the key to the safe deposit box
- a key to your home
- where to get all your passwords
- where all your legal documents are

This will make it much easier for everyone if anything were to happen to you. If you got ill and had to go to the hospital or passed away suddenly or went into a coma for whatever reason.

Conclusion

By following these 10 strategies, you will be able to keep yourself safer from the dark side of the Internet and all the damage that it could do.