The Ultimate Online Safety Guide for Seniors

1. First Line of Defense: Protect Your Devices

Any device you connect to the internet automatically becomes a possible target for cybercriminals.

Without appropriate protection, you may expose yourself to threats like scams, fraud, or even identity theft.

These steps can help you to protect yourself and keep devices like laptops and smartphones secure.

Protect Your Devices
*****
Strong passwords
Antivirus software
System updates
Security settings
WizCase

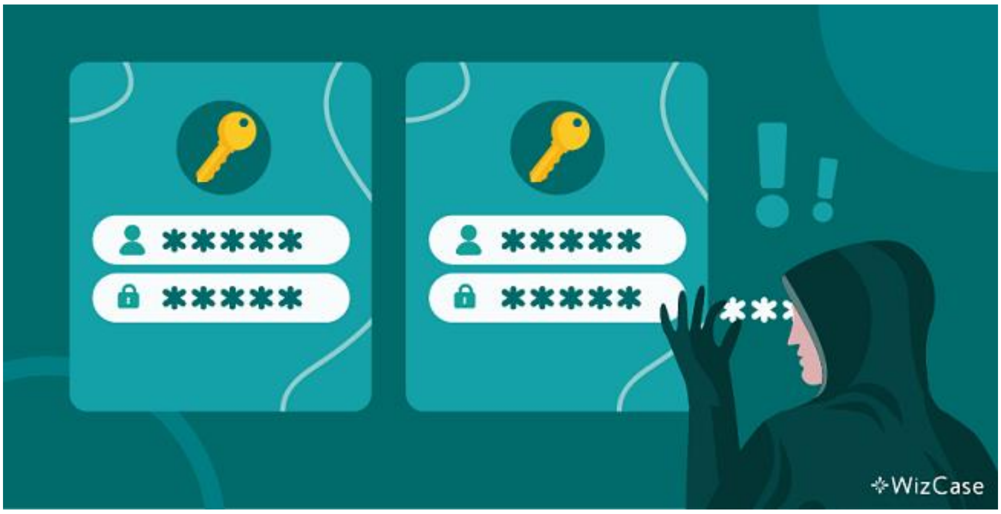
Protect Your Data With Strong Passwords

Hackers now have advanced equipment that can guess over 100 billion passwords in just 1 second.

Easy-to-remember passwords, like “12345”, “password”, or “iloveyou” leave your accounts and devices vulnerable to a break-in.

Ideally, your passwords should be at least 8 characters long and contain a mix of uppercase and lowercase letters, numbers, and even special characters, like “!”, “/”, and “%”.

Avoid using words that hackers could find and link to you, including names of your family members, wedding dates, or the address of your first home. You may think these details are unique, but they can be easily retrieved through social media or phishing.



It’s also important not to use the exact same password across lots of different accounts.

This is because, even without you doing anything wrong, hackers have been known to break into companies’ databases and gain access to all of the company’s users’ details – including their passwords.

Lots of people benefit from using a password management service to create and remember all of their passwords.

Some internet browsers and smartphone operating systems offer this feature built-in with their products. There are also numerous subscription-based password managers available with varying levels of extra security and features. But the free and easy-to-use built-in options are a good choice for most internet users.

Personally, I use a system for creating unique passwords for each of my accounts that I can easily remember because it follows a set process. This way I don't have to rely on a third party to keep my passwords safe.

Avoid Viruses By Using Antivirus Software

Computer viruses are most commonly spread through creative scams such as phishing emails, or through download links on scam emails or disreputable websites.

Every virus is created with a different goal in mind. Sometimes it's to silently collect your personal data saved on your device (like pictures of your family, financial information, or login details for your accounts) and send them directly to hackers. Other times, viruses delete your existing files or even damage the computer and make it completely unusable.

Viruses targeting business systems can cause huge amounts of damage, reputationally and financially. Regardless of its purpose, the havoc caused by a virus can be expensive to fix, and important documents like precious photos and tax records could be lost forever.

Antivirus software does exactly what it says it does: it protects your devices from viruses.

Antivirus programs search for malicious files by continuously scanning your devices. As soon as they detect a virus, these programs immediately remove the threat from any files the virus tried to infect. Most antivirus software works autonomously in the background keeping you protected at all times.

Stay on Top of Your System Updates

Every tech device comes with software that dictates how it works and what you can use your device for. This software may come with unforeseen vulnerabilities that hackers can use to break into your system.

Software developers work hard to fix any weaknesses as soon as they're detected. These "patches" are released in software updates.

That's when you'll get a small pop-up window on your screen that tells you to update your device.

It's important to keep updating your devices and apps when you're asked to.

Lots of devices also have an "auto-update" feature that you can use to stay on top of updates.

Personalize Security Settings on All of Your Devices

All devices (including your computer, mobile phone, and tablet) come with a set of default security settings that you should adjust for additional protection.

A lot of security and privacy settings can be customized.

How to Customize the Security and Privacy Settings on Your Phone, Tablet, or Computer

On your phone or tablet

- **iPhones and iPads** – Go to **Settings > Privacy**, **Settings > Face ID & Passcode**. Apple also has a guide to privacy settings for its iOS mobile operating systems here (choose your iOS version in the drop-down menu at the top of the page).
- **Android phones and tablets** – Go to **Settings > Privacy** and **Settings > Biometrics and security**.

On your computer or laptop

- **Macs** – Go to **Apple menu > System Preferences > Security & Privacy**. Apple has a guide for privacy settings on Mac OS here.
- **PCs** – Go to **Settings > Privacy** as well as the individual settings menus for any accounts you have linked to your computer, like Steam or Xbox accounts for gaming or email accounts attached to Microsoft Outlook.

If you haven't enabled it yet, **you can start by securing your devices with face recognition or a fingerprint scan**. That way you'll be able to unlock your computer or phone just by looking directly at the screen or placing a finger on the correct button.

These relatively new safety features provide tighter device security as they can't be stolen or guessed like your password or a PIN code. Face and fingerprint logins are now available on a range of devices, including Windows and Mac computers, smartphones, and tablets.

You can also customize internet browser settings. Firefox, Safari, Google Chrome, and others let you change your privacy settings from deciding what information websites can see to enabling more advanced protection.

How to Customize Internet Browser Settings

- **Safari** – Go to **Safari > Preferences > Privacy**. Check out Apple's guide here.
- **Firefox** – Firefox is a privacy-focused browser, so it has a bounty of privacy and security settings. This page has links to explainer articles for all of these features.
- **Chrome** – Go to **Settings > Auto-fill** and **Settings > Privacy and security**. You'll also want to check out the settings in your main Google account, as this is linked to the Chrome browser.

2. Detect and Avoid the Most Common Scams

As older people are online more often, they're exposing themselves to more risks. That's actually the case across the board, with online scams rising sharply in the last few years.

Phishing scams are the most common, cited as the cause of 80% of all internet security incidents.

People born between 1950 and 1965 are actually victims of online scams less often than younger generations. Recent research has found that only 9% of people in this age bracket have been caught out by a phishing scam in their lives, compared with around 20% for all other age groups.

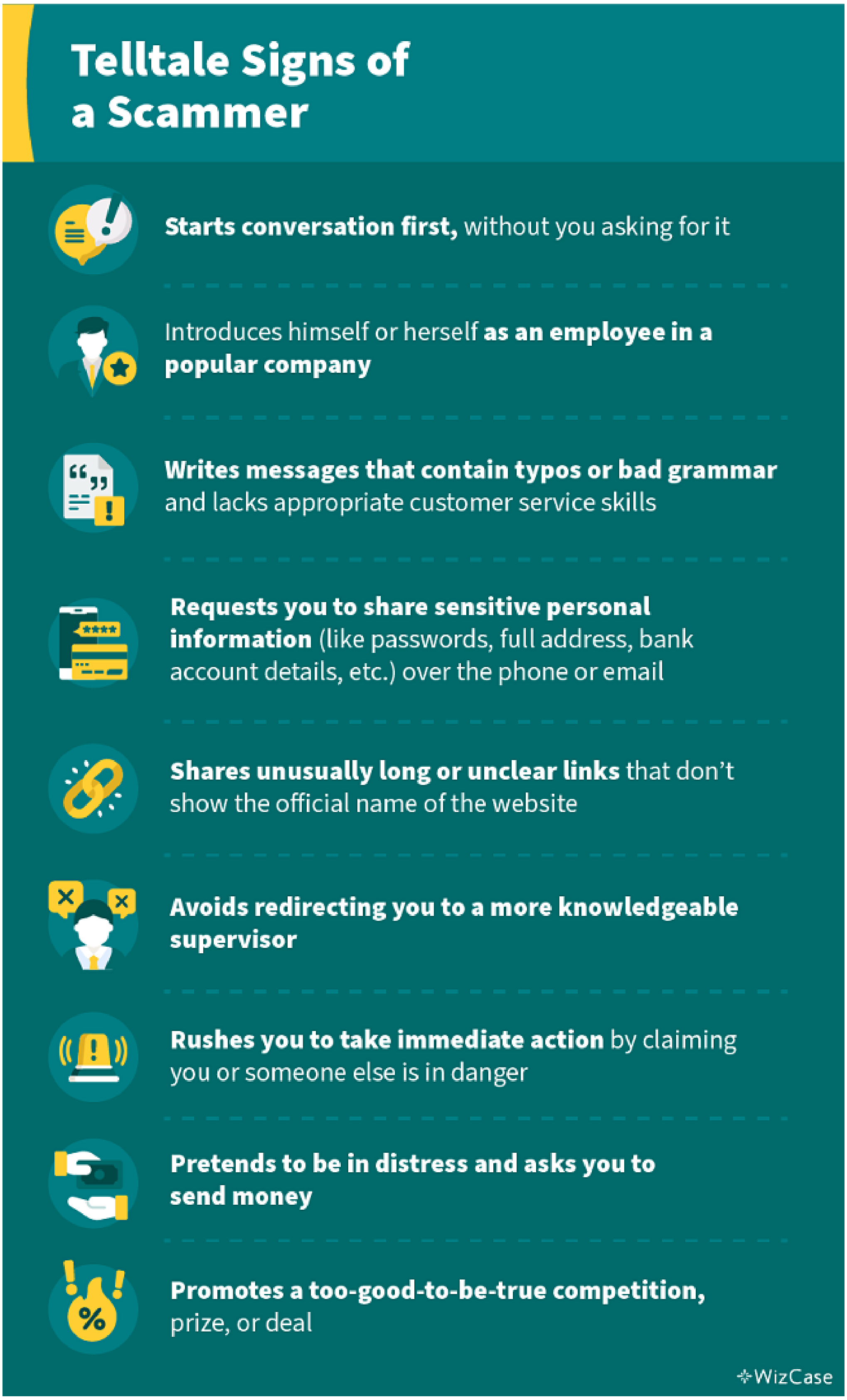
But these stats probably just show that younger people still use the internet more often – and in more ways, for more types of interaction – than older people.

And, as older people use the internet more, they're naturally going to become exposed to more online risks.

Everybody, including seniors, can protect themselves by understanding the most common online scams:

- Phishing emails, phone calls, and text messages: The most common scams are spread in the form of generic messages aimed to trick you into providing personal data like passwords, usernames, home addresses, and more.
- Bogus lotteries or competitions: These present too-good-to-be-true prizes or claim that you've won without entering any competitions. They usually include a link you have to click to claim your prize which automatically steals your data.
- Online dating scams: Fake dating websites collect all of your personal data when you create your profile. Predators may also scam you through catfishing.
- Fraudulent pharmacy sites: Fake sites offer you medication at a significantly lower price to encourage you to buy it. They never send you the order, but take over your bank account and transfer large sums of money out of it.
- Personal emergency scams: Sent out via email or text, the message appears to come from a distressed relative. They're often filled with a lot of emotional descriptions to persuade you to transfer money.

The first step you need to take to protect yourself is to learn to recognize the main signs of scams.



Telltale Signs of a Scammer

- **Starts conversation first,** without you asking for it
- Introduces himself or herself **as an employee in a popular company**
- **Writes messages that contain typos or bad grammar** and lacks appropriate customer service skills
- **Requests you to share sensitive personal information** (like passwords, full address, bank account details, etc.) over the phone or email
- **Shares unusually long or unclear links** that don’t show the official name of the website
- **Avoids redirecting you to a more knowledgeable supervisor**
- **Rushes you to take immediate action** by claiming you or someone else is in danger
- **Pretends to be in distress and asks you to send money**
- **Promotes a too-good-to-be-true competition,** prize, or deal

WizCase

What to Do If You Think You’re Being Phished

Don’t trust somebody who contacts you online or on the phone just because they know a few specific details about you. Cybercriminals spend hours trying to find the smallest bits of information, like which bank you use, where you live, and a shop you last visited. They then carefully craft each scam to create a convincing message or a phone call script.

If you don’t feel comfortable ignoring the email or phone call you received, you can **confirm the scammer’s identity by reaching out to the company or a person they claimed to be**.

It's the easiest way to check if you actually need to take any action and it'll give you peace of mind. When you have verified whether the call or email is legitimate, you can safely block any numbers, email addresses, and websites that tried to con you.

3. Stay Safe While Socializing on Social Media

Social media platforms are great for allowing you to talk to your friends and keep in touch with family, but they also come with a set of rules you should follow to stay safe. It's been found that over 50% of people over 50 are now utilizing Facebook to communicate with others.

Socializing Safely
Think twice before posting
Change default privacy settings
Treat online games like any social media
WizCase

Socializing online comes with its own, sometimes non-intuitive risks. These tips can help you stay safe while you use these platforms to "hang out" on the internet.

Think Twice Before You Post or Respond to a Message

Every bit of information you share online can be used by cybercriminals to gather more data about you and create more successful identity theft attempts.

Some details can even be used by real-life criminals to plan break-ins and other assaults. For example, it may be better to avoid posting your relationship status as it could indicate that you live on your own and make you an easy target. Similarly, sharing the names of your family members or your favorite color, cuisine, and restaurants could help hackers crack your passwords by using various combinations of this information.

Often, quizzes that get shared on sites like Facebook are only designed to harvest personal information about people that cybercriminals can leverage to their advantage.

Remember that nothing you post online can ever be fully erased from the internet.

While you can delete certain posts or messages, their digital footprint remains on the platform's database. You'll also never be sure who had already seen what you posted (or even downloaded it) before you deleted it. As a general rule, if you wouldn't want someone to bring it up in a few years' time, it's probably best to avoid sharing it.

Talking about your birthday, address, or specific locations you go to regularly on social media puts that information out for everybody to see. The same goes for your family and friends – don't put other people at risk!

Change Your Default Privacy Settings

How to Change Privacy Settings on Popular Social Media Platforms

- **Facebook** – Click your profile picture, go to *Settings & Privacy* > *Settings* > *Privacy*. You can also read about other ways to protect your privacy on Facebook here.
- **Facebook Messenger** – Go to *Chats*, tap your profile picture, then go to *Privacy*. Facebook's explainer is here.
- **WhatsApp** – Go to *Menu* > *Settings* > *Account* > *Privacy, > Security*, and *Two-step verification*.
- **Instagram** – Click or tap your profile picture, and go to *Settings* > *Privacy and security*.

- **LinkedIn** – Go to *Me > Settings & Privacy*.
- **TikTok** – Go to *Profile > Menu > Settings and privacy > Privacy and > Security*. Read TikTok's privacy settings explainer **here**.
- **Twitter** – Go to *Menu > More > Settings and Support > Settings and privacy > Security and account access* and *> Privacy and safety*. Twitter's protection guide is here.

Every account you set up on the internet, including social media, comes with automatically applied security settings. These are often not the most secure and you should change them as soon as you create your profile.

Adjust your privacy settings to add an extra layer of security to your social media profiles.

There are a few main security settings that should be your priority, like who can see your profile, whether strangers can search for you, and even if your location is displayed online. These pose major security concerns, and you should always limit your viewable information to your closest friends and family.

Your privacy settings can be altered according to your needs in your profile settings (the button is usually accompanied by a little cog icon). Some platforms offer you more freedom when it comes to changing them, while others let you alter only a couple of them.

Most social media platforms let you set your profile to "private", and some offer even more granular privacy tools.

For example, you can usually control who can see individual posts or photos you put online. This is a good way to share fun memories and photographs with family and friends – away from the prying eyes of the entire public internet.

Enjoy Online Gaming Safely

If you play online computer games, whether you play on a PC or a console, you can follow a lot of the same advice I've shared for staying safe on social media platforms.

Your in-game and lobby chats can be seen by anyone: any user in the game can record and screenshot your conversations, download shared files, and spread this information around the public internet.

Keep personal information personal in online games.

It's great to play online with people you know well, and in these environments where you know everybody you're playing with it's fine to be open. But when you're playing against strangers, it's best to maintain anonymity by not revealing any details about your personal life.

4. Be Aware of Catfishing on Online Dating Sites

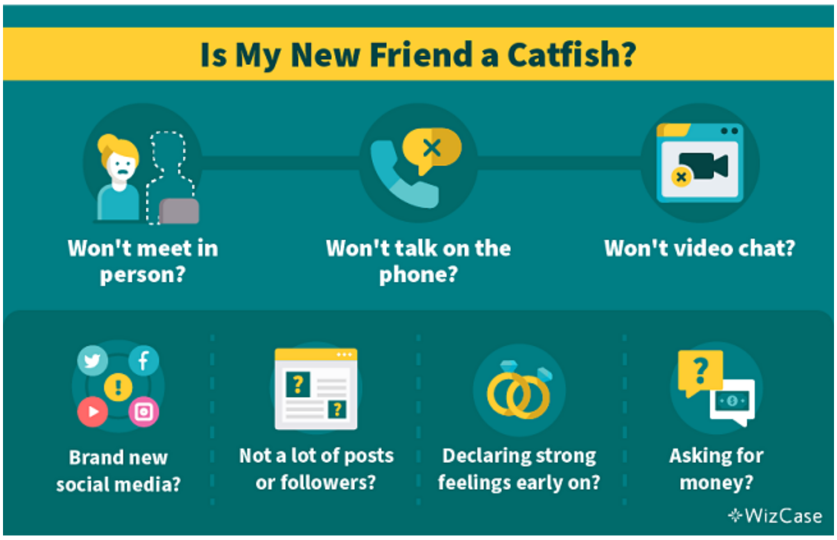
Senior citizens are dating more than ever, and many of them are using online dating sites and dating apps to do so. A recent survey found that a third of seniors are using dating apps today.

But this puts them at risk of catfishing scams.

Catfishing can affect users of all ages, but scammers intentionally target seniors. A catfish is someone who creates a fake online persona and pretends to be interested in starting a relationship (or friendship) with you. The scammer takes their time to build your trust and form a close relationship they can then exploit by asking for money.

While it does make online dating trickier to navigate, it doesn't mean you have to give up on love altogether.

There are many signs you can look out for to spot a potential catfish.



If your online partner refuses to meet, talk on the phone, or video chat, this is a red flag. They usually avoid this type of contact because they don't look or sound like the person they pretend to be.

You should also check their social media profiles. If they have limited posts and photos (or their accounts have just been created), then your partner may be fake.

A catfish is also likely to proclaim their strong feelings for you in a very short period of time. If you're suspicious already, and somebody asks you for money, gifts, or favors — it's probably a good time to walk away from the relationship.

5. Enjoy Online Shopping Without Compromising Your Security

Going to a physical shop is no longer a requirement when you run out of milk or bread. Now, you can order anything you need (including food, medication, furniture, cooked meals, or clothes) on the internet and have it delivered straight to your house. Doing so reduces the need to drive to multiple locations and spend hours in queues, so it's not surprising that almost 50% of seniors like to shop online.

Unfortunately, online shopping creates a whole new area of possible vulnerabilities, such as leaking your payment details or becoming a scam victim. These dangers can be greatly reduced by making sure you're following a few extra precautions.

Safe Shopping
Use legitimate sites
Use a credit card
Consider a virtual card
Don't save payment details
Use secure WiFi
WizCase

Make Purchases Only Through Legitimate Sites

The rise of online shopping demand has encouraged hackers to duplicate hundreds of e-commerce websites that mimic the look and functionality of their legitimate versions. In fact, they're almost identical which makes it very difficult to differentiate which site is secure.

There's just one detail that you need to look for — if a shopping site you're on has a little lock sign next to its link that means it's legitimate and can be used to check out safely. That small sign means the website is secure from hackers.

You should only visit and use e-commerce websites if they have the small lock sign by their URL.

If you notice a website doesn't have the lock, refrain from making any purchases until you confirm it isn't a scam. You can check a site's legitimacy on websites known for reviewing online security, like TrustPilot.

That way you can access an independent expert review and a site's safety score, as well as read about other people's experiences shopping there.

Protect Your Money by Using a Credit Card

Buying items with your credit card is the safest method as you aren't taking the funds directly from your bank account. That way if you happen to get scammed, you'll be able to dispute your transaction with a credit card issuer.

These kinds of disputes are usually approved without any issues which means you won't be required to actually pay for your order, so you won't lose any money.

If you don't feel comfortable using a credit card, create a PayPal account and use it as a payment method instead. While it's directly linked to your bank account (which means it'll take your money automatically once the payment is processed), PayPal is also known for being good at disputing transactions.

As soon as you report a scam, the company will stop the payment process and your money won't be taken from your account or you'll be refunded the full amount you already paid.

I use PayPal for online purchases to make sure my payments are secure and refundable

Consider Getting a Virtual Credit Card for Online Shopping

A virtual credit card is only designed for one-off uses. It masks the numbers of your real credit card, so you're not giving any information to e-commerce sites that can be linked back to you or to your accounts.

Virtual cards create another layer of security for online shoppers.

Even reputable e-commerce sites can be hacked, and stored credit card information is a lucrative bounty for cybercriminals. If you use a virtual credit card when you're shopping online, your details won't be exposed in the event of this kind of security breach.

Virtual cards are now offered by most major card providers and banks. American Express, Visa, MasterCard, Capital One, and Citibank all support virtual cards now.

Never Save Your Payment Details

Your internet browser or shopping site may encourage you to save your payment details for quicker use in the future. However tempting, it also means that anyone who accesses that website on your device will be able to make a purchase with your card without your knowledge. It's particularly dangerous if a hacker breaks into your system or if your device is stolen.

So to be extra safe, it's worth spending a few more minutes to enter your card number and billing info if it means your bank account stays protected from unauthorized use.

It's tempting to save your card details for faster checkout, but it can put your card at risk of theft.

Use Only Secure WiFi Connections to Buy Anything

Public internet connections (in cafes, restaurants, shopping centers, etc.) aren't secure as anyone can easily connect to them without any authentication required.

Cybercriminals are known to utilize this effortless connection to upload malicious code and intercept your online communications. This means that they can see exactly what details you input online, including your payment details and billing address.

To avoid compromising your details, shop online only when you're connecting to a private WiFi — like the one in your home. This will reduce the likelihood of hackers breaking through your online security and stealing your credit card numbers, PayPal logins, and other data you share.

6. Recognize False and Misleading Information Online

Nowadays, anyone can set up a basic website and share any information they want there. Just because something can be found on the internet, doesn't automatically mean you can take it as a fact without questioning its integrity.

The most common misinformation spread online includes health advice, news or political information, and fake official government requests (like phony tax refunds, social security, and medical care advice).

In a survey investigating online behaviors in the run-up to the 2016 US presidential election, over-65s were found to be more likely than any other age group to visit fake news websites and share links on Facebook.

Fortunately, everybody can use the following practices to make sure you're getting your information from trustworthy real experts.

Don't Fall for Fake News
Fact check news and political info
Use sites like Snopes and Politifact
Make sure you're on the official website for government services
Be wary of unsolicited calls or emails
WizCase

Fact Check News and Political Information

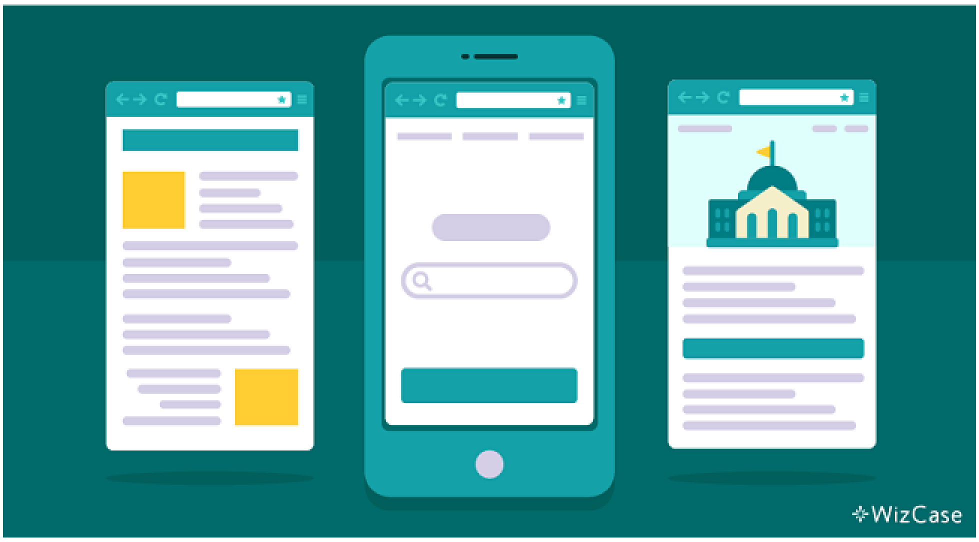
As anyone can create a website that looks legitimate, it's become increasingly more difficult to differentiate between fact and fiction in news and politics. Due to the polarization of opinions, many people falsify the information they post online to manipulate readers.

When you're checking any information online, first check if the article you're reading has a list of reputable sources to back up its claims.

Strong claims need unquestionable proof backed by science or highly-qualified professionals. You should also see if the article has a specific publishing date and a writer who created the piece. Many illegitimate sites avoid posting such specific information to avoid personal repercussions and fines.

Next, you can briefly scan the article for signs of any endorsements which could indicate the company was paid to take a certain angle on the story. These advertisements are usually disclosed at the bottom of the screen or even page notes, so pay great to details.

I also use multiple fact-checking online tools, like Politifact and Snopes which debunk false claims by presenting well-researched facts.



Sometimes just Googling suspicious information is enough to bring up reliable sources that set the record straight.

Use Official Government Sites to Deal With Tax, Medical Care, Retirement, and Social Security

Most official organizations (like Medicare, Social Security, and HM Revenue and Customs), now let you access their services online. Unfortunately, many scammers and fraudsters take advantage of it and create fake websites that imitate legitimate versions to gather your sensitive data.

They also use these companies to carry out phishing. If you think the government has contacted you, you're more likely to be duped into providing your details.

Keep in mind an official organization would never contact you over the phone or email asking to confirm your tax refunds, social security numbers, or other data.

Instead, they often send you an old-fashioned paper letter that you can send back or ask you to come in and fill in certain documents in person. If anyone tries to contact you claiming to be a healthcare provider, social worker, or insurance expert, pause and call your provider directly to confirm their request.

7. Protect Your Health

There is a lot of health misinformation and downright dangerous medical advice online.

Often, the motivation for publishing this type of content is to scandalize readers and get lots of people to share and visit the page. This boosts ad revenue for the website publishing the information.

Get Your Health Information From Trusted Sources

There are thousands of health websites available and not all of them can be used as trustworthy sources of information.

As a general rule, you should check who manages the website you're on. If it belongs to an established medical company (like WebMD and Mayo Clinic) or to a trustworthy government organization (like the CDC), the information you view is unbiased and well-researched.

However, many well-meaning but ill-informed people create websites to spread their beliefs about medicine and health (even if they're not based on reality). Others create websites with misleading information to promote useless or dangerous products.

Speak to a healthcare professional about any medical advice you find on the internet.

Even when you use the most trusted online sources, you should still confirm with your doctor or pharmacist before you take any action. Trusted healthcare sites are great as a source of information, but they're not a substitute for professional medical attention.

8. Follow These Simple Steps If You Become Involved in a Data Breach

Even when you follow all of the precautions, you may still find yourself affected by a data breach. As companies of any size are likely to experience a hacker attack at least once a year, your data may become compromised through no fault of your own.

Of course, you may also have become a victim of cybercrime or hacking personally. If that happens, you're far from being alone! People of all ages and all levels of internet experience get hacked all the time.

But following a few simple steps as soon as you become aware of a potential security breach can help you protect yourself from further harm.

What to Do When Your Data Is Compromised
****
Check for malware
Change passwords
Contact your bank
Make a report
WizCase

Check Your Devices for Malware

Data breaches, particularly those that involve software companies with direct access to your device, may lead to your computer or phone becoming infected with various malicious files. If you suspect you've become a victim, run a virus check as soon as possible by launching your antivirus software. Should any malware be found, the software will immediately block and remove it from your device.

Change All of Your Passwords

Though only one of your accounts may have been compromised, any information may aid hackers in guessing your other passwords. Changing your passwords regularly is one of the best ways to protect yourself.

Contact Your Bank and Check for Suspicious Activity

If you lost your credit or debit card, it's a good idea to inform your bank to be on the lookout for any suspicious activity. This will instruct experts to monitor your outgoing payments and take action if they notice anything unusual.

Most banks will have trained professionals on hand to help you protect yourself from the impacts of financial fraud, so let them know as soon as you find out your accounts have been compromised.

Report Any Theft or Fraud to Your Local Police

Finding the hackers who are responsible for breaking into a system or stealing your credentials and money is extremely difficult. However, you should still file a police report to document the crime and have it as proof of your innocence. It'll help you claim any insurance or liaise with lenders and creditors.

9. When in Doubt, Always Ask for Help

Even tech experts sometimes need help navigating their devices' constant updates and changes. Asking for help will provide you with additional information you may not have initially thought about.

Where to Go for Help
Family and friends
IT support at work
Help centers for big tech companies like Google and Facebook
In-store, for example at Apple Genius Bars
Community centers and libraries
Online courses
WizCase

Tech-savvy family members can help, but don't be afraid to reach out to real IT experts. All popular technology companies employ and train multiple specialists to help you with any of your queries.

I usually reach out to tech support through online live chat services, but sometimes that option isn't available. If that's the case, I tend to write a descriptive email or simply make a phone call — you can find the contact details needed on the company's website.

Apple also provides face-to-face support through the "Genius Bar" which you can find in all of its retail stores. You'll have to make an appointment through the company's online website and a specially trained "genius" will help you with any issue you may have. You can also ask someone at your local electronics store or repair shop, they may be able to help with any problems you might have.

Local community centers and libraries often organize computer training classes appropriate for seniors and folks new to technology. These courses are designed to teach you system maintenance, online safety, and computer skills in an easy-to-understand format. These are often funded by banks or government authorities to help protect customers and citizens.

Finally, you can use online courses to learn about online safety and computer skills. They allow you to learn about any topic related to digital life without even leaving your house. You don't have to spend any money on them either as many sites for seniors offer hundreds of courses for free.

TechBoomers has classes that cover the basics of every internet platform and what you can use it for. GCFGlobal can teach you all about email, internet safety, different operating systems, and even the actual build of a computer.

Don't Wait for Hackers to Find You — Protect Yourself Today!

With more hackers targeting seniors online, it's crucial to learn how to stay safe on the internet. The good news is that you can take simple steps to protect yourself.

As new online threats emerge with the constant development of technology, you can rely on the recommendations and expert resources recommended in this article to stay safe. Remembering all the security tips can be overwhelming as there are so many of them. But with a bit of practice, you'll be able to enjoy the internet safely!