The Ultimate Internet Safety Guide for Seniors in 2024 by Katarine Glamoslija

Malware. Software designed to damage a computer, steal data, or financially exploit unsuspecting users. Common malware types include ransomware, trojans, and spyware

Data breaches. The release of personal information (such as email addresses, usernames, passwords, and even credit card numbers and social security numbers) to the general public and dark web servers. Recent high-profile data breaches have affected millions of Facebook and LinkedIn users.

Scams. Hackers are constantly coming up with new ways to deceive users into giving away their personal information and money, including scam emails, text messages, websites, social media accounts, and online dating profiles.

Identity theft. Using another person's personal information (e.g. name, social security number, credit card, etc.) without permission

How to Best Protect Yourself (& Your Personal Info) Online

Use a good antivirus software on your computers like Emsisoft

Hackers use deceptive pop-up windows, email links, text messages, websites, phone calls, and more to try and rush and pressure users into bad decisions.

Only go on secure websites. A website is considered secure if the address starts with "http***s***://"

Avoid pirate sites

Consider a VPN (Virtual Private Network) VPN hides your actual IP and prevents your internet service provider from monitoring your online activity. I use ExpressVPN

Use a variety of passwords and always include capital letters, small letters, numbers and special characters and a minimum of 8 charcters

Keep your system updated

Don't be afraid to ask for help! Make sure you have a trusted family member or human to speak with.

How to Spot Online Scams

Romance scams. Criminals pose as interested romantic partners on dating websites or social media, and exploit seniors for money.

Lottery and charity scams. Hackers appear to represent legitimate charities, lotteries, or sweepstakes and then convince seniors that they have won a contest or persuade them to make a donation.

Tech support scams. Criminals claim to be tech support and flag a fake computer or mobile device issue. They offer to solve the problem by using a program to take over a device to gain personal information.

Grandchild scam. Criminals pose as grandchildren who ask for financial assistance.

Government impersonation scam. Criminals claim to be government employees and demand payment or personal information regarding taxes, social security, pensions, etc.

Most of the time, online scammers will be very insistent and demand that you act quickly, whether it's giving them access to your device, giving them personal information, or sending them money. It's important that you resist the pressure to act out of urgency and take the time to assess the situation properly. Here's a few techniques you can use to determine if you're communicating with a legitimate person or a scammer:

Don't click on links and don't download anything. If you're even slightly suspicious about the communications you're receiving, don't follow any links or download any files. Unsafe links and files can steal your data, damage your devices, and much more. Good internet security software can block unsafe links and suspicious downloads in real time.

Go to the source. Google the charity, lottery, tech department, or even government office potentially being impersonated. You can usually contact these organizations via phone or email and verify if you're being contacted by a scammer or an honest person.

Ask yourself clarifying questions. Ask yourself, "Why would a tech support person need you to download a file? Or, "How did you win a sweepstake that you never entered in the first place?" By asking yourself these types of questions, it will likely expose whether the message is from a legitimate source or not.

Use Google. Most scammers aren't very creative. There's a good chance the scam being run on you has been used before — copy-paste text from an email, or just type in a few words describing your situation, followed by the word "scam", and see if the same scam has been attempted on other people.

Phishing

Scammers reach out to users via phone call, text message, email, and even plain-old snail mail. But one of the most common and dangerous techniques is called phishing.

Phishing is the act of creating fake websites, phone numbers, or email addresses that mimic legitimate sources for the purpose of getting information, stealing money, or deploying malicious programs on user devices.

Identifying phishing attacks can be tricky, as phishing messages can look very official and will often link to websites that are pretty convincing copies of legitimate sites. Banking websites and online retailers are very commonly imitated for phishing attacks.

Don't click on links. Phishing messages and smishing messages frequently contain links that can lead you to unsafe sites.

Check the email address and not just the sender name. It's really easy to deceive someone with a fake sender name when sending emails. When this happens, the sender name may be familiar, but the email address doesn't match the sender name.

Look for typos. Phishing attacks frequently use similar spellings as the brands they are trying to spoof, for example "amazn.com", or "support@micr0soft.com" to fool users.

Use Google. Look up the organization being imitated on Google, and compare the legitimate website to the potential phishing site.

Phishing pop-up ads that appear while you're browsing the internet are also very common. Some ads will ask you to claim a prize, or you may even receive a fake notification from Microsoft or Apple claiming something is wrong with your device. It's best to not click on any pop-up ads that appear on your screen and simply click on the X in the corner to close the window — legitimate Windows notifications don't pop up in the middle of your browser screen.

Don't assume that only strangers can send you phishing messages. Real accounts can be hacked and it's possible to receive phishing messages from your friends. Look out for impersonal, vague, or out of character language in the message. And if you do receive a message or email from a friend asking you to click on a link, follow the steps above to try and determine if you're being phished. Also, if possible, simply reach out to your friend with a phone call or text to determine if they sent you the message.

How to Respond to Identity Theft

Notify your bank. Your bank will immediately freeze your accounts, preventing any further losses, and it will also begin the process of reimbursement for the funds stolen from your account.

Run an antivirus scan. It will detect and remove any surveillance malware from your device that could be used to steal future financial information and prolong the identity theft attack. Make sure you're using a reputable antivirus program.

Change your passwords. Once your system is free of malware, change your passwords. I recommend using a high-quality password manager for this process.

Data Breaches

Data breaches occur when a hacker breaks into a company's servers, steals the company's data, and publishes the private data stored by that company — this information can include millions of usernames, passwords, personal information, and even financial information. Sometimes, the data from these breaches is exposed publicly, with everyone on the internet simultaneously gaining access to this information, while others breaches are secretive, with the information being shared among hackers in the dark web for weeks or months until the breach is discovered.

data breaches are scary, but what can you do about them? There's nothing an average user can do to prevent Facebook from getting hacked, but there's a lot you can do to keep yourself safe in the event that your information has been breached:

Use unique passwords. If you have a different password for each of your online accounts, then a data breach won't result in a devastating privacy violation when hackers get their hands on one of your account passwords. If you have the same password for most of your accounts, hackers can use that password for multiple sites to gain access to your accounts.

Change your passwords regularly. Many breaches go unreported for months before being found, so it's smart to be proactive and constantly change your passwords. It's quick and easy to update your passwords with a password.

Use a breach monitoring tool. You can manually enter your emails and usernames into haveibeenpwned.com, which is a massive public registry of all of the publicly available breached account information. Many password managers have data breach monitoring and alert you if your email was involved in a breach.

How to Keep Your Passwords & Online Accounts Secure

Password security is incredibly important, and it can actually be pretty easy to maintain good password hygiene with the right tools. Simple passwords like birthdays or your pet's name and a zip code can be cracked by hackers in under a minute. And if you use the same password for every account, once that password is found, all of your accounts are compromised.

How to Use Emails Safely

To begin with, always check the sender's email address to make sure it's coming from a legitimate source. Look out for addresses that look similar to a known brand but with slight variations (for instance, @costco-special-offers.com rather than @costco.com). And always be wary of clicking on any links promising you cheap products or asking you to fill out a random survey to receive free services. Your friends can also be hacked — you should be very suspicious of any downloads or links that your friends send you. Always confirm with them directly through a trusted medium (e.g. telephone) that they sent you a file or link.

How to Protect Your Privacy and Stay Safe on Facebook

ll of your activity on Facebook is being tracked, analyzed, and sold to advertisers and businesses, but all of your browsing outside of Facebook is also being logged.

Cyber criminals are also able to take advantage of Facebook users by creating fake Facebook accounts and exploiting unaware individuals. If you receive any unsolicited communication or interaction from someone you don't know on Facebook, whether it's a message or a friend request, consider the following:

The profile picture. Is there a picture that looks unique and confirms their identity, or are they using what looks like a random stock photo?

Personal details. Check out how much information they've provided about themselves on their profile. Typically real profiles will have some personal details, while a cyber criminal won't have any work history, family members, or life events listed.

Followers/Friends. Look at how many friends/followers they have and if they're interacting with them. A real person on social media will usually have a few friends or family interacting with them. A criminal will have very few or zero comments or posts from friends on their Timeline.

Mutual friends. If you don't have any mutual friends with someone, and you don't recognize them, it's probably a spam account.

How to Use Online Banking & Online Shopping Safely

Banking and shopping online through legitimate channels is very secure, but there are a few common mistakes that can cost you a lot of money.

How to Stay Safe When Banking Online

First, make sure you're using your bank's official website or mobile app.

Setting up your online bank account will require you to have access to your routing number and account number. You will also need to use a strong password that is unique to that account.

If possible, don't log into your online banking on a public network (like a coffee shop or a library) — only use a secure Wi-Fi network (like your home network) to access the account. By using an unsecure network, you may be vulnerable to hackers accessing your personal information.

Another major threat for users accessing banking information online is keylogging. Keylogging is a dangerous type of malware that allows cyber criminals the ability to record everything that you type into your keyboard. The best way to combat keylogging and screenlogging is to use a good antivirus that can detect this type of malware.

How to Stay Safe When Shopping Online

Don't click on ads.

Use an online payment company account.

Stick with trusted brands.

Read reviews.

Avoid TEMU, a China based scam company. You may get an item but not what you ordered.

How to Protect Your Privacy Online

How to Prevent Malware & Viruses from Infecting Your Device

Here are some of the most common types of malware:

Virus. A malicious program that repeatedly copies itself, taking up space on your hard drive and causing your computer to crash.

Trojan. Pretends to be a legitimate file to gain unauthorized access to your device in order to steal data, install other malware, or even give hackers remote access to your computer.

Spyware. Allows hackers to quite literally spy on your computer and track your browsing history online.

Adware. Clutters your desktop with pop-up ads, inserts unwanted results in your search bar, and even redirects your browser while you're online.

Ransomware. Encrypts and locks your device unless you pay a ransom to recover your account.

Rootkit. Gains extremely deep access to your system, allowing it to hide from antivirus scanners and make changes to the operating system and other essential components.

Cryptojacker. Uses your computer as part of a larger network to mine cryptocurrency. This can put a ton of strain on your computer, causing slowdown, crashing, and even permanent damage to your hard drive.

How to Stay Safe on Your Smartphone & Tablet

Mobile Malware

Privacy-Invading Apps & Fleeceware

Public Wi-Fi Networks

Smishing

Staying Safe

Some good features to look out for in mobile antivirus programs are:

Real-time malware protection.

App privacy detection.

Wi-Fi monitoring.

Parental controls.

Anti-phishing protection.

VPN.

Anti-theft protection.

Bottom Line

Use common sense. If it sounds to good to be true it probably is