Personal Cybersecurity Tips for Seniors*

Excerpted from the National Council on Aging

The web can be a rich source of information, connection, and community. Still, as with any public space, it's important to be aware of your surroundings. Online scams that target older adults are shockingly common—and their number and sophistication continue to grow. "Cyber criminals target older adults for a simple reason," explained Jessica Johnston, NCOA Senior Strategist for Economic Well-Being. "They believe that people in their 60s, 70s, 80s, and beyond are more likely to have money, earned and saved during a lifetime of employment." Scammers also buy into stereotypes that paint older adults as forgetful, overly trusting, and uncomfortable around technology. Whether or not any of this is true is beside the point, Johnston said. Once their victims are in sight, these criminals won't be deterred by facts. Sadly, they're so good at their game that anyone can fall for it—no matter their age or computer savvy.

But you don't have to resign yourself to becoming a victim. Scammers may be sophisticated—but there are smart ways to safeguard against them. Think of the internet as a freeway: you have to navigate it defensively. Just like fastening your seatbelt, using some basic cybersecurity best practices can help ensure that your online experience is safe and enjoyable.

Tip #1: Don't click on links in emails from unfamiliar senders

Be wary of any strange or unexpected messages, even if it's from someone you know. Emails, text messages (or SMS), and social media posts can all contain malicious links. Spam or malicious emails are by far the most common method attackers use to deliver malware or phishing links. Phishing links take you to sites that gather your personal and financial information. Malware, short for "malicious software," is software intentionally designed to damage or gain unauthorized access to a computer, server, or network. Malware has the power to destroy files and steal your personal information. It can even impact the performance of your computer.

How do you avoid malware attacks and phishing scams? Don't click on links sent through email, text, and social media from people you don't know. Be especially wary of emails that urge you to visit a website and provide personal details. And trust your instincts. Even if a message appears to be from a business or person you know, but you weren't expecting it or something feels "off," check with them first before you click any links. Go directly to the company's website (type it in yourself; don't click through to get there) and contact them that way. It's not rude—it's smart. It's also a good idea to install strong security software on your phone, laptop, or desktop computer.

Scammers often try to make you feel like you have to act immediately, using pressure to push you into rash decisions. If you ever feel urged to click a link or send money, take a step back and carefully assess the situation before responding.

Tip #2: Don't open any attachments unless you know the sender and were expecting them to send it

While many email attachments may appear to be harmless, they could contain malware designed to launch an attack on your device. These attachments can be disguised as run-of-the-mill Word

documents, PDFs, voicemail transcripts, invoices, and other e-files. Don't open any attachments you aren't expecting or that come from people or businesses you don't know. This is especially true if the attachments end in .exe or .zip. If it looks like a friend or family member sent the attachment, remember that someone else could be making unauthorized use of their email address. Always reach out to the person you know to make sure they've sent you something.

Even attachments that require a password should spark your suspicion. Having a password doesn't mean the attachment is safe to open, and the password won't protect you against malware. As always, check with the sender. This internet safety rule also applies to attachments sent via text messages (or SMS) and social media.

Speaking of social media, one more thing: Scammers often create duplicate (fake) accounts using the names and photos of people you know. Then they send a friend request. If you get one of these requests, reach out to your friend before accepting; chances are, it's not legitimate and you should delete it.

Tip #3: Ignore unsolicited phone calls and "robocalls"

Treat any unsolicited phone calls with skepticism—even if the phone number or name on your caller ID looks familiar.

"There is readily available technology that phone scammers use to 'spoof'—or mimic—numbers that don't belong to them," Johnston said. "These criminals might be calling you from another continent, but the number you see has your area code, or looks like it's from a local business. The person on the other end of the line is banking on the fact that you'll pick up because the call seems legitimate. And once that happens, you're immediately vulnerable to voice phishing."

What is voice phishing? It's a common method scammers use to defraud people.

Keep in mind that government departments, such as the IRS, will never call you and ask for sensitive information. And technology companies won't call you out of the blue to offer technical support or assistance, either. Avoid giving money to someone over the phone, especially if they ask for wire transfers, gift cards, or to pay fines or bail. The best thing to do is to pre-screen all your calls, even if you're pretty sure who's on the other end of the line. Any friend, family member, or organization with a legitimate need to call you will either leave a message or try again.

And if you do answer the phone and hear a recorded voice, the next best thing you can do is say nothing and hang up. Remember: this is not rude.

Tip #4: Don't respond to or click on pop-up windows on your phone or computer

Scammers also use screen pop-ups to target their victims. One common ploy is scareware. This malware scam uses bogus security alerts and other tricks to frighten you into downloading or paying for fake antivirus protection or other cybersecurity software. How does scareware work? An "urgent" pop-up window appears on your computer or phone, telling you that your device is

compromised and needs repairing. The message includes a number to dial for help. When you call it, the scammer may either ask for remote access to your computer or request a fee to fix it.

Tip #5: Don't conduct any transaction involving personal information while using a public (or unsecured) network

"This advice is less specifically about scams and more about online safety overall," Johnston said. "Public networks are crawling with scammers just waiting to intercept your passwords, bank account numbers, and other sensitive information so they can use it later to steal your money or identity. And it doesn't require them to fool you into giving it up. They just take it."
If you often rely on public WiFi and need to make purchases, log in to your financial institution, check your medical record, or other activity involving personal information, consider setting up a virtual private network (VPN) to protect yourself. Otherwise, wait to do these things until you know the internet access is firewalled (secure).

You can further safeguard your mobile device from intrusion by protecting it, and any apps on it, with a PIN number or biometric recognition (such as touch ID or facial recognition).

How can older adults avoid online scams?

Internet safety is important, but it doesn't have to be stressful. Awareness is a powerful first step in protecting yourself. Another thing to put on your personal cybersecurity checklist? Installing trusted antivirus software to protect you and your device. There are a number of reputable options available for free on the web.

Lastly, if you think you've been the victim of an online scam or cyber-attack, be vocal about your experience. You're not alone—and there's no reason to feel embarrassed about what happened. Immediately contact your local police and your financial institution if money has been taken from your account. You can also report the scam online to the Federal Trade Commission (FTC).

Read the full article here: https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security/

Cybersecurity and Seniors Links to More Resources

- FBI Elder Fraud Tools
- Internet Crime Complaint Center (IC3)
- Reporting Medicare Fraud & Abuse
- Social Security: Protect Yourself from Scams