CYBER SAFETY FOR SENIORS:

Essential Tips for Staying Protected Online

By Eric N. Peterson

Cyber Safety for Seniors

Essential Tips for Staying Protected Online

By Eric N. Peterson

For Dad

Table of Contents

Introduction 5
Why the Seniors and Elderly are a Cyber Target 5
Understanding the Threat Landscape 7
General Recommendations for Common Threats 9
Real-life Stories & Examples 12
Senior Specific Threat Recommendations & Solutions 14
About the Author 17

Introduction

In the digital world of today, which is changing quickly, seniors and the elderly stand out as an especially vulnerable group. Even though new technologies bring a lot of benefits, they also bring new problems and risks, especially for people who didn't grow up during the digital change. Many seniors are easy targets for scams and online threats because they are not very tech-savvy. Cybercriminals would love to get their hands on their life savings and assets.

Also, their risk is raised by things like memory loss, a natural trust in others because of how they were raised, and growing social isolation. Often, these people don't do their normal digital housekeeping, like checking their bank accounts or changing their passwords, because they forget or rely on others to do it for them. This makes them more vulnerable to deceit and fraud.

Additionally, digital contact, which is a main way for many families to talk to each other today, can sometimes be good and bad for older people. As they try to stay in touch with loved ones, they may unintentionally open themselves up to bad things happening online. Because of these risks, it is more important than ever to give our senior citizens the information and tools they need to navigate the digital world safely.

Also, I've called out some common misconceptions in large red boxes. There are numerous examples of these and limited space within this guide, but to get you thinking about security, start with these two:

1) If you receive a call from someone claiming to be a grandchild in trouble and needing money, always verify with another family member before taking any action
2) 2) Always research charities before donating, especially if they contact you unsolicited. Authentic charities won't pressure you into making a donation immediately.

Why the Seniors and Elderly are a Cyber Target

Here are ten reasons cybercriminals and bad actors target our seniors.

1. Limited Digital Literacy: Many seniors did not grow up with the technology available today. Their limited familiarity with the digital landscape can make them more

susceptible to scams and cyber threats. It's essential to educate and support the elderly in navigating the digital world safely, ensuring they have the knowledge and resources to protect themselves against cyber threats.

2. Wealth Accumulation: Over a lifetime, seniors often accumulate savings, assets, and pensions. Cybercriminals see this demographic as a lucrative target.
3. Cognitive Decline: Some elderly individuals may suffer from cognitive decline, making them less able to discern suspicious online activity or recognize a scam.
4. Trust in Others: Many seniors come from a generation where trust was more freely given, making them more likely to believe and act upon deceptive communications.
5. Isolation: The elderly are often more socially isolated, which can lead them to seek out interactions online. This can expose them to potential threats.
6. Less Frequent Monitoring: Some seniors may not regularly monitor their bank accounts, credit reports, or online profiles, allowing fraudulent activity to go unnoticed for longer periods.
7. Dependence on Caregivers: Relying on caregivers or others for assistance with online tasks can expose seniors to insider threats, where trusted individuals exploit their access.
8. Less Familiarity with Security Practices: Due to limited digital exposure, many seniors are unaware of best practices for passwords, software updates, and other security measures.
9. Fear and Anxiety: Cybercriminals exploit seniors' fears, often posing as government agencies, medical facilities, or banks to extract personal information.
10. Digital Communication with Family: As more families use digital tools to communicate, seniors may unintentionally click on malicious links or download harmful attachments thinking they're from loved ones.

Microsoft, Apple, or any other tech company will never call you unsolicited to tell you that your computer has a virus or is malfunctioning.

Understanding the Threat Landscape

Common cyber threats that impact everyone, including senior citizens include: Phishing,

malware, ransomware, and social engineering. Here are the definitions with examples. You may have even had these happen to you.

Phishing:

> Definition: Phishing is a cyber-attack where perpetrators attempt to trick individuals into divulging sensitive information, such as login credentials or credit card numbers, by masquerading as trustworthy entities in electronic communication.
>
> Example: An email that appears to come from a trusted bank asking users to "click on a link to verify their account details." Once the user clicks on the link, they are directed to a fraudulent website designed to look like the bank's authentic website, where they are prompted to enter account information, which is then stolen by the attackers.

Smishing:

> Definition: Smishing is a type of deception technique where attackers use SMS (Short Message Service) messages to deceive individuals into providing personal information, passwords, or financial information. It's a form of phishing but executed over text messages instead of email. Cybercriminals will often craft a message to induce panic, interest, or curiosity in the recipient, prompting them to click on a link, reply with personal information, or even call a specified number.
>
> Example of Smishing: A user receives a text (SMS) stating:
>
> "ALERT: Unusual activity detected on your BankXYZ account. Please confirm your identity immediately to prevent account suspension. Click here: [malicious link]"
>
> In this example, the attacker hopes the recipient will be concerned about their bank account's status and, without questioning the sender’s authenticity, click on the provided link. The link might lead to a fake login page designed to capture the user's bank login credentials. Alternatively, it might download malware onto the user's device.

Vishing:

Definition: Vishing is a form of deception technique where attackers use voice calls to deceive individuals into providing personal information, passwords, or financial information. The term "vishing" is derived from combining "voice" with "phishing." In vishing attacks, scammers often pretend to be from legitimate organizations, such as banks, government agencies, or service providers, to sound credible and manipulate victims into revealing sensitive data.

Example of Vishing: A user receives a call, and the person on the other end says:

"Hello, this is John from the Fraud Prevention Team at BankABC. We've noticed some suspicious transactions on your account. For your security, I need to verify your identity. Can you please confirm your account number and the last four digits of your social security number?"

In this example, the attacker is impersonating a bank representative, attempting to create a sense of urgency and concern. If the recipient provides the requested information, the scammer can then potentially access the victim's bank account or commit identity theft.

Malware:

Definition: Malware is a general term for malicious software that is specifically designed to disrupt, damage, or gain unauthorized access to computer systems. It encompasses various types of harmful software such as viruses, worms, trojans, and spyware.

Example: A user might download a seemingly harmless software from the internet, only to find out that it covertly installs a trojan, which then allows attackers to access and control the user's computer remotely.

Ransomware:

Definition: Ransomware is a type of malware that encrypts a victim's files or locks users out of their systems. The attacker then demands a ransom from the victim, promising to restore access or decrypt the files upon payment, although there's no guarantee they will do so.

Example: A user receives an email with an attached document claiming to be an invoice. Upon opening the attachment, the user's files are encrypted, and a screen displays a message demanding payment (usually in cryptocurrencies like Bitcoin) in exchange for the decryption key.

Social Engineering:

Definition: Social engineering refers to manipulative tactics that trick individuals into divulging confidential information or performing actions that compromise security. Unlike other cyber-attacks, which exploit software vulnerabilities, social engineering exploits human vulnerabilities.

Example: An attacker calls an employee posing as IT support, claiming they need the employee's password to perform a critical system update. Trusting the caller's supposed identity, the employee shares their password, inadvertently granting the attacker access.

In all these scenarios, the common theme is deception. Cyber attackers are constantly evolving their tactics, relying on both sophisticated technology and human psychology to achieve their malicious goals. Awareness and education remain crucial in recognizing and preventing such threats.

Your bank will never ask you for your password, PIN, or full account number over the phone or via email, nor send emails with direct links asking you to update or confirm your personal details.

General Recommendations for Common Threats

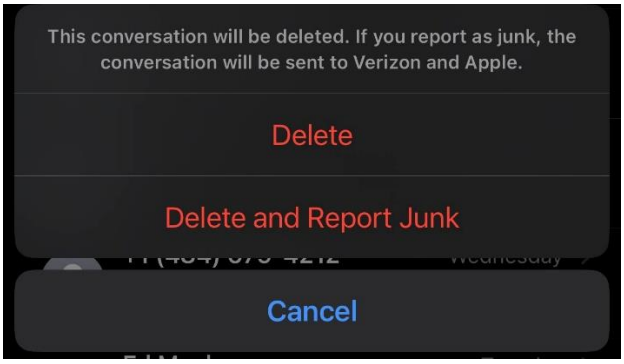
Phishing Attacks:

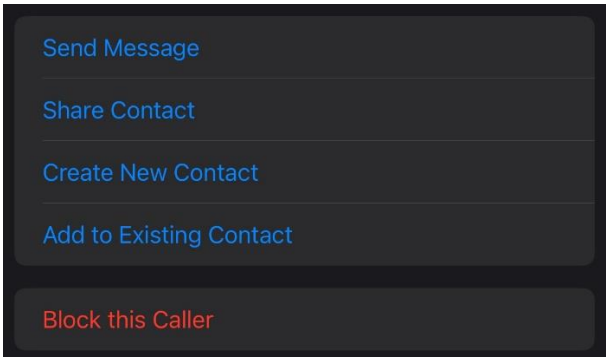
Solution: Always verify the sender's email address. Be wary of unsolicited communications, especially those urging immediate action or requesting personal details. Avoid clicking on links

or downloading attachments from unknown sources. Being wary of "too good to be true" deals and offers targeting seniors and the elderly. Universities usually have official channels to communicate critical information, so when in doubt, verify directly with the institution or organization.

Smishing Attacks:

Solution: Be wary of texts by new numbers or people you don't know and of any fitting the scam profile (sounding scary or threatening) and containing links. It's probably best to just delete and report them as junk and ignore them all together. See the following screenshots.





Vishing Attacks:

Solution: Bad actors hate to leave messages, so one way to circumvent their tactics is to ignore the phone call, let it go to voice mail. You can also block the call (depending on device and OS), by reviewing the info on the text/call and selling block this caller. You'll still get robo calls and others (hopefully you've added your phone numbers to the various block lists? If not, I've included them below.

National Do Not Call Registry (U.S.):

Managed by the Federal Trade Commission (FTC), this free service allows U.S. consumers to opt out of receiving telemarketing calls. Once registered, telemarketers are required to remove your number from their call lists - Website: donotcall.gov

State-specific Do Not Call Lists:

Some U.S. states have their own "Do Not Call" lists. It's worth checking with your state's regulatory office or consumer protection agency to see if there's a separate list to which you can add your number.

Carrier-specific Services:

Major phone carriers often offer services or features that help identify and block unwanted calls. For example, AT&T has "Call Protect," Verizon offers "Call Filter," T-Mobile provides "Scam Shield," and Sprint had "Premium Caller ID" (though Sprint has since merged with T-Mobile).

Ransomware:

Solution: Regularly back up all important files to an external drive or cloud storage, keeping them separate from your main system. This ensures that you can restore your data without paying a ransom. Additionally, avoid downloading software or opening attachments from unverified sources. Additionally, apply regular software updates and recognize and avoid malicious apps.

Public Wi-Fi / Eavesdropping:

Solution: Avoid accessing sensitive accounts or conducting financial transactions over public Wi-Fi. If necessary, use a Virtual Private Network (VPN) to encrypt your online activities, ensuring they remain private, even on open networks.

Identity Theft:

Solution: Use strong, unique passwords and enable 2FA/multifactor authentication for any accounts or applications that allow it. Utilize a password manager and never reuse passwords. Securely store any sensitive documents, especially those that contain personal information. Recognize secure e-commerce websites and monitor your bank statements and credit reports regularly for any suspicious activity. Be cautious about the personal information you share online, especially on social media.

Social Media Scams:

Solution: Be skeptical of too-good-to-be-true offers or sensational stories shared on social platforms. Verify the authenticity of any unexpected friend requests, as scammers sometimes impersonate acquaintances to spread malicious links or solicit information.

Adware and Spyware:

Solution: Install reputable antivirus and anti-malware software on your devices. Periodically run scans to detect and remove potential threats. Only download software or apps from verified, trusted sources.

Doxing:

Solution: Be cautious about the amount and type of personal information you share online. Adjust privacy settings on social media platforms to limit what is visible to the public. Consider using pseudonyms or usernames that don't link directly to your real name on non-essential platforms.

To wrap things up, having a general attitude of skepticism and caution online can go a long way. Cyber threats often rely on exploiting human error, so taking a moment to think before acting can make a significant difference.

The IRS, or any tax agency, will not call demanding immediate payment via gift cards, wire transfers, or cryptocurrency, nor will they threaten to arrest you over the phone for unpaid debts or fines.

Real-life Stories & Examples

Real-life stories involving our senior citizens and being targeted by cybercriminals are easy to find and very sad. Here are the senior-specific threats and examples to illustrate where cyber and security awareness training for our elders is needed.

Limited Digital Literacy

Example: Joan, a 70-year-old grandmother, received an email claiming she had won a prize. The email asked her to click on a link and enter her details to claim it. Unfamiliar with phishing scams, Joan provided her personal information, only to find out later that she had been scammed.

Wealth Accumulation

Example: Richard, a retired engineer, was contacted by someone claiming to be from an investment firm with a too-good-to-be-true opportunity. Enticed by the promise of high returns, Richard transferred a significant sum, only to find out it was a sham.

Cognitive Decline

Example: Ellen, suffering from early-stage Alzheimer's, was called repeatedly by a scammer posing as a tax agent. They convinced her she owed back taxes, leading her to make multiple payments over several weeks.

Trust in Others

Example: George, a war veteran, received a call from someone posing as a charity supporting veterans. Trusting the caller, he provided his credit card information, which was later misused.

Isolation

Example: Lucy, a widow who lives alone, started receiving friendly emails from a supposed overseas friend. Over time, the 'friend' manipulated Lucy into sending money to help with a fake emergency.

Less Frequent Monitoring

Example: Margaret, not accustomed to checking her bank statements regularly, didn't notice unauthorized withdrawals made over several months.

Dependence on Caregivers

Example: Mr. Thompson's caregiver accessed his personal computer, discovered his banking details, and made unauthorized purchases using his credit card.

Less Familiarity with Security Practices

Example: Harold, never having changed his online banking password, fell victim when his easily guessable password ("password123") was compromised.

Fear and Anxiety

Example: Sara received a call from someone claiming to be from the Social Security office, threatening to stop her benefits unless she provided her SSN and other personal details. Out of fear, she complied.

Digital Communication with Family

Example: Alex, trying to keep up with his grandchildren, clicked on a malicious link in a message that appeared to be from one of them, which resulted in malware being installed on his computer.

These examples underscore the importance of educating seniors about cyber risks and implementing preventive measures to protect them.

You cannot win a lottery or sweepstakes you did not enter. Be wary of emails or calls claiming you've won money, especially if they request payment to claim the prize.

Senior Specific Threat Recommendations & Solutions

Here are some recommendations to guard against cyber threats and scams.

Limited Digital Literacy

Solution: Seniors should enroll in basic computer and internet safety courses. Local community centers, libraries, or senior centers often offer classes tailored to their age group. This helps them understand the basics of safe online behavior.

Wealth Accumulation

Solution: Before making any significant investments, seniors should always consult with a trusted financial advisor or family member. It's also essential to be skeptical of offers that seem too good to be true.

Cognitive Decline

Solution: Family members and caregivers should regularly check in on seniors, especially those with cognitive impairments, to ensure they aren't making rash financial decisions or being manipulated.

Trust in Others

Solution: It's essential for seniors to verify the identity of anyone asking for money or personal details, whether through call-back methods, consulting with trusted individuals, or other means. Additionally, do not grant remote access to your computer unless you are 100% certain of the identity and trustworthiness of the individual on the other end.

Isolation

Solution: Encourage seniors to engage in community activities or senior centers where they can share experiences and learn from others. It can help them become aware of common scams targeting their age group.

Less Frequent Monitoring

Solution: Set up automatic alerts for bank accounts and credit cards to notify of any unusual activity. Regularly review financial statements and online profiles to catch unauthorized actions early.

Dependence on Caregivers

Solution: Ensure all caregivers undergo background checks. Monitor their internet and financial activities if they're responsible for them. Set up restricted user profiles or guest accounts on devices for caregivers to use.

Less Familiarity with Security Practices

Solution: Ensure that seniors are using strong, unique passwords for all their accounts. Consider setting them up with password managers and regularly update their software and security applications.

Fear and Anxiety

Solution: Educate seniors about common scam tactics, like impostors posing as government agencies. Let them know that legitimate organizations will never instill fear or demand immediate payment.

Digital Communication with Family

Solution: Teach seniors to verify unexpected links or attachments from family members by calling or texting the person directly before clicking. Install robust security software that can detect and block malicious links and downloads.

Proactive education, combined with supportive technologies and regular check-ins by friends, family and neighbors, can go a long way in ensuring that seniors stay safe in the digital age. We encourage continued learning in the ever-evolving field of cyber security and cyber safety and sharing where you can. Good luck!

Medicare will not call asking for your Social Security number or bank information. Be suspicious of unsolicited offers for "free" medical equipment or services.

About the Author

Eric Peterson is a cybersecurity expert from SLC, UT, working in CyberOps, directing and managing teams that monitor and respond to cyber threats and that help to keep companies' data and enterprises safe. He has over 20 years of experience in IT and Cybersecurity, an M.S. and B.S. in IT Security and assurance, and over 20 industry-recognized certifications, including CISSP, CISM, CRISC, and CISA. As a published author, he has written multiple eBooks, many on guitar instruction, and many cybersecurity technical blog posts and guides.

For more information, connect with Eric on LinkedIn or visit www.cybertipsguide.com for more eBooks and helpful cyber tips and guides.