PROTECT YOURSELF

Help Avoid Scams Aimed at People Over 60

Fraudsters target seniors more than any other group. Here are examples of the top scams, and tips to help keep seniors safe.

The FBI reports that scams targeting individuals aged 60 and older recently caused over $3.4 billion in losses*. Scams are built around topics that make people nervous, so you act more emotionally than rationally: your health, your Social Security or Medicare, or the recent death of a relative. Likewise, scammers try to confuse seniors and rely on them being polite and trusting. Combating senior fraud takes not only good cyber hygiene, but also requires habits and behaviors that will help make you a bad target for criminals.

If you do fall victim to any of the scams below—and lose money from an account—don't feel ashamed. These scammers are really good at what they do. The best counterattack is to report the incident right away. The sooner you let your financial institution know, the better chance you have of stopping future thefts, and maybe even recovering some of what you lost.

GRANDPARENT SCAM

How it works:

This fraud is usually done through a phone call. Someone poses as your grandchild (or a niece or nephew) and uses names or family details pulled from social media in a frantic tone. They'll disguise their voice and may hand the phone to a "lawyer" or "cop." They'll paint a dire scenario—they've been arrested or in a car accident—and need you to send cash or wire money right away.

What you can do:

- ☐ **Recognize urgency as a red flag.** Phrases like "right now" or "there's no time" can be a clue that something is not right. Scammers may also use artificial intelligence (AI) to imitate the voice of your loved one, so don't immediately trust a voice*. Remember, real life is rarely that urgent—take a moment to think critically about how likely the scenario is. Then hang up and call the relative directly.

SOCIAL SECURITY, MEDICARE, AND IRS SCAMS

How it works:

There are several variations but, typically, a caller says there is a problem with your account and they need to verify information. The goal isn't usually to take money directly from you, but to get personal data they can sell on the black market or use to file fake claims or refunds in your name. Don't underestimate how real these can seem—they may even have some of your personal information already.

What you can do:

- ☐ **Never give out personal information to a caller.** No matter how pressing they make it seem ("police will be there in an hour"), you can always take the time to hang up, look up an official number, and call to verify the situation.

- ☐ **Don't answer phone numbers you don't recognize.** Scammers may target odd times, like early in the morning or late at night, when you could make a decision without thinking clearly.

TECHNICAL SUPPORT SCAM

How it works:

A pop-up window on your computer claims you have a virus and offers to install an antivirus program if you click a link. Instead, the link installs malicious software (malware) to get your personal information. In another version of the scam, someone calls claiming to be from a software company and convinces you to give them access to your computer so they can provide support.

What you can do:

- ☐ **Don't click on pop-ups, ever.** Legitimate computer companies don't contact users via a phone call or pop-up window for unsolicited technical support.
- ☐ **Make sure your operating system is up to date, and consider installing antivirus software.** If those steps sound difficult, ask a family member or hire a local computer security professional.

FAKE FINANCIAL, INVESTMENT, OR SWEEPSTAKES EMAILS

How it works:

Sometimes these fake emails or text messages (also called phishing) promise a prize or opportunity. They often contain a threat or warning about a financial account. What they have in common is that they look like they're coming from a legitimate source and ask you to click a link.

What you can do:

- ☐ **Be very wary of clicking links in emails or text messages.** These messages are so sophisticated it may be almost impossible to tell that they are not real, or that the link is actually taking you to a fake web page designed to steal your login information. Get in the habit of opening a web browser and typing in the website address yourself, rather than clicking on the link.
- ☐ **Don't repeat passwords across accounts.** If you do get tricked into giving your username or password for a website, fraudsters may try using them to log into other accounts. But, if you're in the habit of creating a unique password for each site, they're less likely to get much further.

DECEASED DEBT SCAMS

How it works:

Scammers look through obituaries and target family members of the deceased, claiming there's an outstanding debt and convincing the grieving family member to pay.

What you can do:

- ☐ **Show it to someone you trust.** Scammers count on you being too emotional to think clearly. Always reach out to someone you trust—a relative or attorney—to get a second opinion.
- ☐ **Set up account alerts for your bank accounts.** You'll be notified when big withdrawals or charges occur. Consider letting family members get alerts as well. That way, if someone gets into your account or you get tricked into making a payment, you'll have another set of eyes on it.

Tools to help avoid fraud

Huntington has tools that can help mitigate some of these cyber risks, including alerts[¶] that can notify you of unusual or suspicious account activity, and the ability to lock a lost or stolen credit or debit card.

Contact Huntington

Call **(800) 480-2265** to report a lost or stolen card. If you're concerned about potential fraud or want more information, visit **huntington.com/Security**.

[¶]Message and data rates may apply.

† Federal Bureau of Investigation. Elder Fraud Report. April 2024.

‡ Federal Trade Commission. "Scammers use AI to enhance their family emergency schemes." March 2023.