PROTECT YOURSELF

Help Avoid Scams Aimed at People Over 60

Fraudsters target seniors more than any other group. Here are the top scams and how to help seniors stay safer.

A RECENT REPORT BY THE CONSUMER FINANCIAL PROTECTION BUREAU estimated the number of incidents of financial fraud against seniors quadrupled between 2013 and 2017†. Scams are built around topics to make you nervous so you act more emotionally than rationally: your health, your Social Security or Medicare, 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. The 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 and a frantic tone. They'll disguise their voice and maybe 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 are also careful to ask for small amounts that you can send quickly (the FTC says the median loss on this scam is $2,000‡). But remember, real life is rarely that urgent—take a moment to think critically about how likely this 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, it's to get personal data that 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**, especially early in the morning or late at night. Scammers count on your not being fully awake, so you'll make decisions without thinking§.

Member FDIC. ®, Huntington® and Huntington.Welcome.® are federally registered service marks of Huntington Bancshares Incorporated.
©2019 Huntington Bancshares Incorporated.

TECHNICAL SUPPORT SCAM

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

What you can do:

- ☐ **Don't click on pop-ups, ever.** Large, 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. Sometimes they 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 and 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 will use them to try to log into your other accounts. If your password is unique for each site, they'll probably get nowhere.

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** so you'll know when big withdrawals or charges occur, and 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[¶], which can let you know about unusual or suspicious account activity so you can catch fraud early, and the ability to lock your credit or debit card if it is lost or stolen.

Contact Huntington

If you think you may be a victim of fraud related to your Huntington credit or debit card, or your card has been lost or stolen, please call us at **(800) 480-2265**.

Visit **huntington.com/Security** for additional information.

[¶]Message and data rates may apply.

---

† Consumer Financial Protection Bureau. *Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends*, 3. February 2019.
‡ Fletcher, Emma. "New twist to grandparent scam: mail cash." Consumer Protection Data Spotlight, December 3, 2018. Accessed May 29, 2019.
§ Lavelle, Justin. Email to Mike Haney. May 28, 2019.
†† Fetterhoff, Mark. Email to Mike Haney. May 30, 2019.

Member FDIC. ®, Huntington® and Huntington.Welcome.® are federally registered service marks of Huntington Bancshares Incorporated.
©2019 Huntington Bancshares Incorporated.