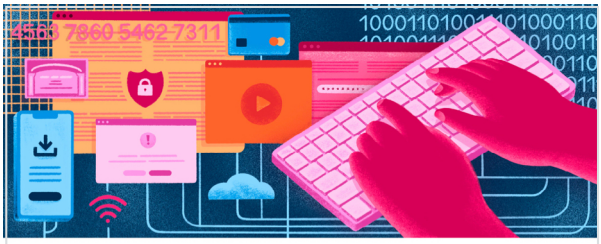
According to the FBI, seniors lose over $3 billion dollars every year to scams. We'll discuss how you can protect yourself from those who want to steal your money.



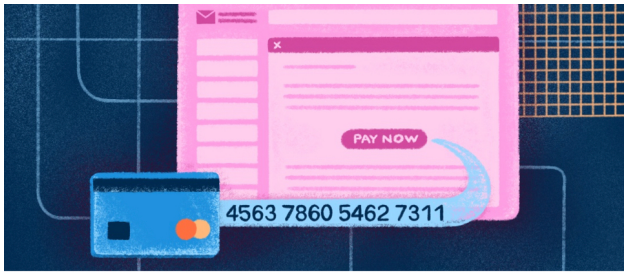
Scams Targeting Seniors

Banzai!

Here are some reasons that scammers may target senior citizens.

- Many seniors have access to a significant amount of money due to retirement funds, owning their home, or a lifetime of accrued savings.
- Some seniors are inexperienced with technology. Scammers take advantage of that to trick them into downloading malware or viruses.
- Many seniors have large extended families. This can make it harder to account for everyone at all times. That means that if a scammer claims a family member is in trouble, a senior may be more willing to believe it.
- Some seniors feel isolated. They may feel that they don't get to see friends often enough, that their family should contact them more, or that their situation prevents them from finding a romantic partner. Scammers manipulate these feelings to gain a senior's trust and more easily take their money.

Scammers know that you'll see through the scam if you do your research. To prevent this, they'll pressure you to act quickly. That pressure could be positive (a prize, a deal) or negative (a warrant for your arrest, losing your account, a loved one is in trouble). Always confirm claims with an outside source before acting.



Red Flag: Pressure to Act Quickly

Example*: One senior citizen in Texas received a call from scammers claiming to be federal officers. The victim was instructed to send money via various shipping locations in order to clear their name. When they tried to hang up, the scammers became aggressive and threatened that officers would show up at the victim's house to arrest them if the money was not sent immediately.

RED FLAG

Red Flag: Requesting Money

You should be suspicious of anyone who reaches out to you requesting money, but even more so if they want you to send it in unusual ways. Scammers will usually ask for wire transfers, gift cards, or cash to prevent you or your financial institution from tracing or cancelling the transaction. Be extremely wary of someone who asks for money this way, no matter their reasons.

Example*: In Alabama, an elderly woman received a message from a friend's Facebook account, which she later learned had been hacked. The hacker claimed that they knew of an attorney giving away thousands of dollars. All you had to do was send them a picture of your driver's license and the numbers and pins of $500 worth of gift cards. The woman fell for the scam, lost the money, and gave up personal information.

Red Flag: Asking for Sensitive Information

Scammers try to collect sensitive information so that they can steal your identity or access your accounts. Be wary of anyone who asks for passwords or social security and account numbers. Legitimate companies will almost never ask for this data and, if they do, should give you a secure way to send it.

Example*: Tons of new scams accompanied the COVID-19 pandemic. One version targeted those looking to ensure that they got their stimulus checks. Using official looking sites, victims were prompted to sign up for their check or validate their identity by entering sensitive information. This was not required in order to receive a stimulus check.

Phishing: A scammer pretends to be someone they aren't, usually a familiar company or personal friend. They ask the victim for sensitive information or tell them to click a link that downloads a virus to their device. Phishing can take many forms, including emails, texts, and even fake websites—scammers take great care to make their message seem legitimate.

- Always ask these questions before responding to unprompted messages: Are there misspelled words or strange links? Is the person acting like themself?

Malware or Ransomware: Hidden viruses show up in popups, ads, posts on social media, emails, or messages from the accounts of friends or family that have been hacked. When downloaded, the virus steals the victim's information or forces them to pay money.

- Be suspicious of any links someone sends you unprompted, particularly if they use extremely generic language. Don't click on links unless you are sure they are legitimate.

Tech Support or Antivirus Scams: The victim is told there's a virus on their device, usually via popup, text, or email. The scammer says they can fix it by accessing the device or installing antivirus software. Instead, the scammer steals the victim's sensitive data or downloads actual viruses to their device.

- Don't trust anything that pops up or reaches out to tell you that your device has a virus. Always use a well reviewed antivirus software to scan for problems or take the device to a certified professional.

Lottery or Prize Scams: The victim receives an email, call, or text that says they won a prize, often a cash award or luxurious vacation, and that they only need to pay taxes or a processing fee in order to receive it. This scam may even come with a check that will eventually bounce once the victim deposits it but, by then, the scammer is long gone with the victim's money.

Lucky Day Scams

- Lottery or prize scams
- Investment scams

- If something sounds too good to be true, it probably is. If you didn't enter for a giveaway, there's no way you won. And even if you did, are you sure that giveaway is legitimate?

Investment Scams: Scammers offer investment opportunities that are far more risky than they let on. Thieves may also claim to be financial advisors and, once they have access to the victim's account, steal their money rather than investing it.

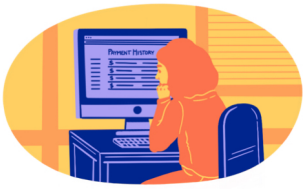
- Only seek out legitimate, verified advisors or do research into stocks yourself. Don't trust someone who approaches you claiming to have a deal.

Debt Collector or IRS Scams: A scammer claims to be a debt collector or representative of the IRS. They may even reach out to the family members of someone who recently passed away and say that they are now liable for debts.

- The IRS will never call you to collect. Situations where someone else is held liable for a family member's debt are very rare. You can send a debt validation letter to find out.

Representative Scams

- Debt Collector or IRS Scams
- Medicare Scams
- Affinity Fraud



Medicare Scams: A fraudster claims to represent Medicare, asks for the victim's sensitive information, and uses it to bill Medicare for services never provided. In a similar scam, deceitful people will provide medical services that are fraudulent and then bill Medicare to cover it.

- Medicare will only call you if you are a member of a drug plan and already agreed to be called, the original agent who helped you needs something, or you left them a message.

Affinity Fraud: A dishonest person plays on someone's affiliation with a group, such as a religious congregation or alumni association, as a way to get money or information. The scammer may be an actual member of the group (even someone the intended victim knows or likes) or just pretend to be.

- No matter who the person on the other end of the line is or claims to be, practice caution when giving up money or information. It's best to support groups through official channels.

REVITY CREDIT UNION

Relationship Scams

- Grandparent Scams
- Romantic Scams

Grandparent Scams: The victim receives a call, email, or message on social media from someone impersonating a loved one, usually a grandchild. The imposter claims that they're in some kind of trouble and asks for money.

- Always contact the person asking for help in another way or reach out to another family member to confirm. Even if the person claims they are embarrassed or don't want anyone to know, it's better to be sure you aren't getting scammed.

Romantic Scams: A con-artist deceitfully forms a relationship online—often to the point that the victim considers them to be a romantic partner. The scammer then asks for money in a lump sum or smaller amounts over a longer period of time. Usually they claim this money will be used to support them, cover an emergency expense, or pay for them to travel.

- While the internet can be a great way to meet new people, it's also extremely easy for people to claim to be someone they're not. You should do all you can to confirm a person's identity when talking with them and talk to friends or family if you're suspicious.

If you're contacted by a scammer:

- Ignore
- Report

If you're contacted by a scammer, the best thing you can do is ignore them—don't answer their calls, delete their emails, and navigate away from a site that doesn't look legitimate. You can also report them to the **FTC** or **FBI** to help stop them from reaching out to you or others again. Navigate through one or both of the sites linked above to show how exactly to report scammers.

If you've sent money to someone you believe is a scammer, it's best to act as soon as possible. Cancel the card, tell your financial institution you believe your account information has been stolen, explain the situation to an administrator, and call the police. If the scammer has your sensitive information, such as your social security number, go to **identitytheft.gov** to learn what to do next.

MEMBER OF REVITY CREDIT UNION? CALL US IF YOU HAVE ANY QUESTIONS 618.797.7993 OR VISIT US ONLINE AT REVITYCU.COM