

S.A.F.E.

Senior **A**nti-**F**raud **E**ducation

Recognize a scam before you become a victim of fraud



**Division of
Consumer Protection**

Advocating for and empowering New York consumers

A Division of the New York Department of State

Andrew M. Cuomo, Governor

Rossana Rosado, Secretary of State

Become a savvy senior

Senior citizens are too often the targets of consumer fraud scams. Scammers prey on older adults, who are viewed as vulnerable and lonely easy prey with readily available cash. It's important to familiarize yourself with this kind of fraudulent activity to protect against becoming a victim. Here are six of the most common senior scams out there and some tips to help you stay safe.

* * * * *

• **Medical Device Scam**

Seniors have reported receiving unsolicited prerecorded messages, known as "robocalls," offering free medical alert devices, along with money saving coupons. When answered, the message urges consumers to press 1 to receive a free device by providing an address and credit card information. Pressing 1 puts the consumer through to a live operator, who uses scare tactics to elicit personal and financial information from the consumer. The message also offers the option of pressing another number to opt out of future calls. Pressing that number, however, alerts the scammers to a working phone number, which can be used for future scam calls.

• **Grandparent Scam**

These scammers call or email seniors asking for money. They impersonate loved ones who are in some kind of trouble and need cash. Often, the calls are made in the middle of the night, so the adult answering the phone may be disoriented. These con artists seem credible because they have become sophisticated in finding and using personal information from social media and Internet searches. In some cases, the scammer impersonates a police officer, a lawyer, or a doctor who is calling on behalf of the relative in trouble. In all cases, the scammers request that money be sent immediately and usually through a wire transfer.

• **Ghosting Scam**

“Ghosting” is a form of identity theft. Identity thieves obtain personal information about deceased persons from obituaries, funeral homes, hospitals, stolen death certificates, and online web sites. Once they have the information, especially Social Security numbers, they use it to establish credit and open accounts, take out loans, receive benefits, or even collect tax refunds filed under the stolen identity. Family members of the deceased are not responsible for charges resulting from this kind of identity theft as long as their names are not on the stolen accounts. Remember, it’s important to inform the Social Security Administration of a death.

• **Jury Duty Scam**

These scammers, pretending to be law enforcement officers or court officials, contact individuals to inform them that they have failed to report to jury duty. As a consequence, victims are told to pay a fine by credit card to avoid arrest. In many cases, when the victims inform the callers that they didn’t receive any jury duty information, callers emphasize citizen responsibility to appear for jury duty whether or not a notice has been received. These scammers also coerce victims into providing personal information, such as social security numbers and date of birth, which can then be used for identity theft or other fraudulent activity.

• **Funeral Notification Scam**

The “funeral notifications” scam involves emails, which include the subject line “funeral notification,” to deceptively inform recipients of an upcoming farewell ceremony in remembrance of a friend or loved one. These emails appear to be sent from legitimate funeral homes and instruct recipients to click on a link for “more detailed information.” The link sends victims to a third party web site where malware, or “malicious software,” is downloaded. This software causes computer havoc and allows scammers to gain access to the user’s computer information, which can then be used in fraudulent activity. If you receive such an email, delete it immediately.

• **Sweepstakes Scam**

Many sweepstakes, unfortunately, are run by con artists who are looking to access your personal information or tap into your accounts. These scammers entice consumers with various prize offers and then ask that you share personal information or that you pay a fee to enter the sweepstakes. The most common of these scams targets seniors, who pay the supposed fee and receive fake prize winning checks, which are deposited into consumer bank accounts. Unfortunately, the checks are then rejected as counterfeit. The con artists, meanwhile, have pocketed the money collected for fees or taxes on the prizes. Remember, you never have to pay fees to participate in legitimate sweepstakes.

• **IRS Imposter Scam**

Be alert to this “phishing” scam, one of the most sophisticated telephone scams to date. In fact, according to the Internal Revenue Service (IRS), at least 20,000 taxpayers have been targeted. By impersonating IRS agents, these phone scammers demand immediate payment of overdue taxes from victims via debit card or wire transfer

to avoid being arrested. These scammers may even know the last four digits of a victim's Social Security number. In addition, victims report that scammers follow up with emails after a call. If you receive an unexpected call from the IRS, it is most likely a scam. Many times it's difficult to determine if the call is a scam, but remember the IRS generally sends out prior notification of any action in the mail and never requires immediate payment over the phone. When in doubt, hang up and call back using a number that the IRS advertises on a government web site or in the phonebook: 1-800-829-1040.

- **Free Grant Scam**

Beware of fraudulent grants promised in print or over the phone. In one instance, free grants are advertised in the classified sections of newspapers and magazines. The advertisement claims that readers qualify to receive free grants to pay for anything from home repairs, college expenses, unpaid bills, or home business expenses. In other instances, people report receiving phone calls from someone impersonating a representative of a government agency or organization. These callers use official sounding names and promise free grants because taxes have been paid on time or because they can be used for debt relief. They all follow the same script – congratulating you for your eligibility and then asking for personal and financial information. They confirm name, mailing address, and then ask for the name of your bank, account numbers, and routing numbers, to be used only to withdraw money for a processing fee. Regardless of the method used, the claim is the same – guaranteed acceptance of your application and the promise that you do not have to repay the money. Remember, the grant offer is a fraud. The scammers only want access to the funds in your accounts.

Scam Prevention Tips

- Hang up without pressing a key if you receive an unsolicited phone call. If you do take the call, be sure to identify the caller and the company represented. Also always get a phone number for the business.
- Never provide personal or financial information over the phone. This includes your name, date of birth, Social Security number, address, and Medicare number.
- Contact your telephone provider to block “robocall” numbers. Avoid paying for blocking services since robocall numbers displayed on caller IDs change frequently.
- Install a firewall and anti-virus/anti-spyware software to protect your email account from being used by scammers. Also keep all of your software updated.
- Do not open attachments from strangers or any emails that seem suspicious. Attachments sometimes contain programs that allow scammers to gain access to your computer.
- Avoid listing birth date, maiden name, or other personal identifiers of loved ones in obituaries as such information is useful to identity thieves.
- Do not click or open files in unfamiliar emails to avoid downloading unwanted malware.
- Do not respond to guaranteed sweepstakes winnings in exchange for a contribution.

- The IRS usually initiates first contact about unpaid taxes through U.S. mail, never by phone or email.
- The IRS never asks for payment using a wire transfer or a pre-paid debit card.
- Call the IRS directly at 800-829-1040 if you think that you may owe taxes.
- Protect your personal information by storing it in a safe and secure place. Do not keep important account numbers or data in purses, wallets, or smartphones.
- Remember that phone calls can be deceiving. Scammers now use sophisticated technology to manipulate their area code in caller ID systems.
- Do not pay money for a “free” government grant. Anytime you are asked to make a payment to receive a government grant, it is a scam.
- Never wire funds or pay for a product or service using a money order. If the business is legitimate, it will accept a credit card or bank check. This will allow you the option to stop payment.
- Never pay cash or give full payment for home improvement work prior to completion. A legitimate contractor will accept a small down payment to proceed with any home improvement project and not demand full payment upfront.

S.A.F.E.

Senior Anti-Fraud Education

Recognize a scam before you become a victim of fraud

If you are a victim of a scam:

- Call your local police or sheriff's office to report the crime.
- Alert neighbors and community organizations to the presence of scam artists in your area.
- Contact the Division of Consumer Protection at www.dos.ny.gov, the Attorney General's Office at www.ag.ny.gov and/or your local consumer protection agency so they can warn others and offer assistance.
- Keep a record of your financial losses in case there is a prosecution and restitution is ordered.



Division of Consumer Protection

Advocating for and empowering New York consumers

A Division of the New York Department of State

1-800-697-1220 www.dos.ny.gov



@nysconsumer



/nysconsumer