

Ten Common Scams Targeting Older Coloradans—

And How to Avoid Them




Colorado Attorney General's
Senior Fraud Handbook Series, Vol. 1

AARP Foundation

ElderWatch

Helping older consumers recognize, refuse and report fraud in partnership with the Colorado Attorney General



The information contained within this booklet is for educational purposes only and should not be substituted for the advice of an attorney licensed to practice law in Colorado.

Publication Date: July 2018

Consumer Protection is our Mission

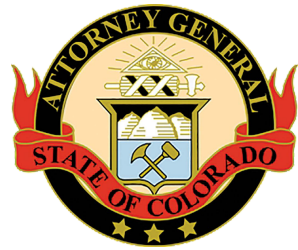
Fellow Coloradans:

Our office has for many years fought hard to educate our citizens facing a deluge of phony telephone calls, letters, and emails—all designed to trick them into believing that they have won a lottery or sweepstakes, that they owe back taxes or have a computer virus, or any one of dozens of other scams.

We have prepared this fraud handbook for you to explore and understand ten of the most common scams directed at older Coloradans, to provide some simple steps to identify these scams and, most importantly, some tips to avoid them.

But, reading this handbook is just the first step to protect yourself and others. To succeed in preventing fraud, we urge you to form your own fraud-fighting team. Include your spouse, siblings, children or grandchildren, or trusted friends and advisors. Discuss any and all suspicious solicitations you receive—in whatever form—before you send away your hard-earned money to strangers. You'll be surprised to learn that you are not alone in this fight, and that sharing these experiences will empower you, your family, and your friends to make smart decisions.

We also urge you to visit our fraud-fighting website at www.stopfraudcolorado.gov where you can sign up to receive my fraud alert newsletters, report suspicious activity, and research hundreds of other frauds and scams.



AARP Foundation

ElderWatch

Helping older consumers recognize,
refuse and report fraud in partnership
with the Colorado Attorney General

Table of Contents

1: IRS Tax Scams	3
2: Grandparent Scams	4
3: Tech Support Scams	5
4: Federal Government Grants	6
5: Home Repair Scams	7
6: Foreign Lotteries and Sweepstakes	8
7: Magazine Sales	9
8: Timeshare Resale Scams	10
9: Charity Fraud	11
10: Identity Theft	12
Contacts	13

1 IRS Tax Scams

The Scam:

You get a call from someone claiming to be a federal IRS agent and seeking immediate payment of taxes they claim you owe. The phony agents try to intimidate you with threats of arrest, liens on property, deportation, or driver's license revocation to scare you into making payments or disclosing personal information. The imposters often have just enough personal information to convince a taxpayer they are legitimate.

Authorities believe that many of these phony calls originate in India and other foreign countries. Consumers may see official looking numbers on their caller ID, and the callers may provide badge numbers or other official-sounding identification.

How to Avoid It:

According to the IRS, it will **NEVER:**

- Call you to demand immediate payment;
- Demand that you pay taxes without allowing you to question or challenge the amount you may owe;
- Require that you pay your taxes a certain way, such as with a wire transfer or prepaid money card or gift card;
- Ask for your credit or debit card numbers, or other personal information over the phone; or
- Threaten you with arrest, liens, deportation or license revocation.

Debt Collectors: The IRS does use private debt collectors to pursue outstanding inactive tax debt. Before you may be contacted, you will first receive a letter from the IRS telling you that your account has been turned over to a specific collection agency, and a second letter from that collection agency advising you of the amount due and providing a taxpayer identification unique to you. **Private collection agencies will not ask for payment on a prepaid debit, iTunes or gift card.**

To make a complaint about a private collection agency or report misconduct by its employee, call the U.S. Treasury Inspector General for Tax Administration (TIGTA) hotline at 800-366-4484 or visit www.tigta.gov.

If you receive one of these calls, or a similarly threatening email, **immediately hang up the phone or delete the email message without responding.** If you are concerned that you may owe back taxes, you can go to www.irs.gov/balancedue to check your account balance, or call the IRS directly at 800-829-1010.

2 Grandparent Scams

The Scam:

You receive a call or an email, often in the middle of the night, from someone claiming to be your grandchild, other relative, or close friend. There will be some story of an emergency: they've been in an accident; arrested; or trapped in a foreign country without money or a passport. The call may involve another person saying they are a doctor, lawyer, law enforcement official, or even a kidnapper. No matter what the alleged emergency, this scam always involves a desperate plea for immediate payment.

Sometimes the caller will know a surprising amount about you and your family. These scammers may search public records, or obtain information you posted on social media sites like Facebook and Twitter. Or, they will just call randomly and say, "Grandma," and hope that you will respond "Is this Mike?"

These fraudsters will ask you to send funds via a wire transfer, prepaid card, or they will ask for your bank account and routing number. Wanting to protect their family or friend, grandparents will impulsively send the money—only to learn later on that their loved one is safe and there was never any kind of emergency.



How to Avoid it:

Here are some important tips:

- Beware of any urgent plea for money to pay doctor's or lawyer fees, bail or fines, or even customs fees to get out of some foreign country.
- Before doing anything else, contact other relevant family members to verify the situation.
- Be suspicious of any demand that funds be sent by wire transfer or prepaid cards.
- Never give out personal or financial information, such as bank account information or credit card numbers.
- Be aware that fraudsters attempting this scam may call late at night to confuse potential victims.
- Agree on a family "password" and make sure everyone in your family knows it. You can then ask any caller to recite the password as proof that they are who they say they are. It's important not to share the family password with others or online and to change it after it's been used.

3 Tech Support Scams

The Scam:

You're working on your computer when suddenly a message appears and warns that your computer may be infected with a virus. You are directed to click on a link in the message or to call a specific number to get assistance in checking for viruses and removing them. You will likely be asked to make a payment in advance for these services. Or even worse, you may unknowingly give the scammer remote access to your computer where they can secretly install software that will track your computer strokes (including to online accounts and passwords) or steal personal and financial information off of your computer.

The first question you should ask yourself is "Could anyone—even Microsoft—know whether my computer has been infected with a virus?"

How to Avoid it:

Here are a few basic things you should know and some tips for avoiding tech support scams:

- The minute a stranger calls or emails you, or a pop-up message appears on your computer with a "WARNING!" about a virus detected on your computer, you should know that it is a LIE. Large computer or software companies—including companies that provide legitimate security and anti-virus software—have no way of knowing whether your particular computer has been infected. NOTE: If you have antivirus software installed and operating on your computer, that software may send you an alert about a possible virus.
- Legitimate companies will NEVER call you out of the blue or send you a pop-up message with claims that they have detected a virus or other problem with your computer.
- If you receive a call from someone who offers technical support, or claims your computer has been hacked or infected with a virus, hang up immediately. Delete any pop-up messages without responding.
- NEVER allow a stranger to gain remote access to your computer—for any reason. Once they are inside, they can steal personal or financial information or install their own virus to steal this information for them.
- If you suspect that you actually have a virus or other problem with your computer, contact the help number that comes from the manufacturer, or reputable local computer repair company.
- Keep all security software installed on your computer up-to-date and turned on.
- Make sure your device's firewall and pop-up blocker are turned on. This will help prevent intrusions and unsafe pop-ups.

4 Federal Government Grants

The Scam:

You receive a call, email, or even a Facebook message informing you that you have been selected by the federal government to receive a grant. Government grant scams have been around for years and always involve the same basic premise: somehow (even though you never even applied for a grant!), and for some reason (sometimes the caller claims it's because you paid your taxes on time!) the government has selected you to receive "free" grant moneys—to be used for no particular purpose—and you never have to pay it back.

Of course there is a significant catch: you usually have to pay large sums of money to claim your "free" grant. As with most scams, they want your money immediately, usually by wire transfer or pre-paid card.

How to Avoid it:

Here are a few basic tips for recognizing and avoiding government grant scams:

- The call, email, text message, or Facebook message is completely unsolicited and is not in response to a formal grant application you actually submitted.
- The solicitation refers to some vague and non-existent government organization ("Federal Grants Administration," "Federal Bureau of Grant Awards," US Government Grant Department," etc.).
- REMEMBER, no government agency (state or federal) will ever call you or message you on social media about a grant award.
- The scam artist speaks with a heavy foreign accent, uses poor grammar, or appears to be in a large room with a lot of other telephone calls that can be heard in the background.
- The solicitation comes in the form of an online "friend" request that appears to be from someone you know and offers to introduce you to an elected official, such as your Attorney General, who can get you the grant.
- NEVER give out personal identifying information (address, date of birth, Social Security Number) or financial information (bank account or credit card numbers) in response to unsolicited calls, emails, texts or advertisements.
- NEVER agree to pay any fee in order to claim these phony grants.
- NEVER agree to send a wire transfer, transfer money through a social media site like Facebook, or use pre-paid cards.
- NEVER pay for a list of grants that you might be eligible to receive.

5 Home Repair Scams

The Scam:

From shoddy workmanship to “fly-by-night” unlicensed contractors, many people are scammed by roving con artists who knock on doors and offer unnecessary repairs. A typical scenario involves an uninvited door-to-door solicitation from a contractor claiming to have a “special price” on roofing, siding, windows, asphalt, etc. Of course, the price is only good “right now” and the contractor will need all or most of the price paid “up front.” Once they get your money they usually disappear having done little or none of the promised work. The work that is done is usually of poor quality.

How to Avoid it:

It is important to follow some basic tips to avoid home repair scams:

- Be suspicious of anyone coming to your home uninvited claiming to be a roofing or home repair contractor.
- If they claim to be a public insurance adjuster, demand to see a current license from the Colorado Division of Insurance.
- Don't fall for high pressure sales tactics, promises of special, limited-time deals or demands for immediate payment before the work is started and completed.
- Before you spend any significant amount of money on a new roof or other home repairs, contact your insurance company yourself and arrange to have an authorized adjuster come to your home.
- Obtain bids from at least three different contractors, and check each one with organizations like your local Better Business Bureau.

It is also important to know:

- Colorado law requires that a roofing contractor **MUST** provide a written contract that includes: the approximate dates of service, the approximate costs of the services, the roofing contractor's contact information, identification of the roofing contractor's surety and liability coverage insurer, and information regarding your right to rescind the contract within seventy-two hours if your insurance company denies your claim.
- A roofing contractor **MUST** include, on the face of the contract, in bold-faced type, a statement indicating that the roofing contractor shall hold in trust any payment from the property owner until the roofing contractor has delivered roofing materials at the residential property site or has performed a majority of the roofing work on the residential property.

6 Foreign Lotteries and Sweepstakes

The Scam:

A letter comes in the mail, a notification in your email, or you receive a phone call, with incredible news—you have just been announced as the winner of a HUGE lottery or sweepstakes prize! All you have to do to claim your prize is to pay some money (they may call it an entry fee, judge's fee, import or customs fee, taxes, etc.). But, what's a couple thousand dollars when you're set to receive millions?



Avoid it:

Here are some signs that you are being solicited by a phony sweepstakes or foreign lottery:

- The call, letter, or electronic message comes from a sweepstakes or lottery you don't remember entering.
- The so-called "prize notice" contains vague and confusing terms, or bad grammar, that leaves you confused about whether you have actually won a prize or are just being asked to enter into the sweepstakes or lottery.
- You are required to submit some form of payment in order to claim a prize or award—it might be as little as \$20 as an "entry fee" or "judges fee" or thousands of dollars for taxes or insurance.
- The notice creates a sense of urgency imploring you to "act immediately" or using terms like "final notice" or "last chance to claim your prize."
- You are required to make an immediate payment using a wire transfer or pre-paid money card.
- You are required to provide personal identifying information, such as your social security number, birth date, or bank account information.

REMEMBER, it is ILLEGAL to sell or promote a foreign lottery or sweepstakes in the United States, so anyone claiming that you have won such a lottery is breaking the law. Any solicitation through the mail, by telephone, or electronically (email or text message) that requires the purchase of any product, or the payment of any fee as a condition to entering or winning a lottery or sweepstakes is illegal.

7 Magazine Sales

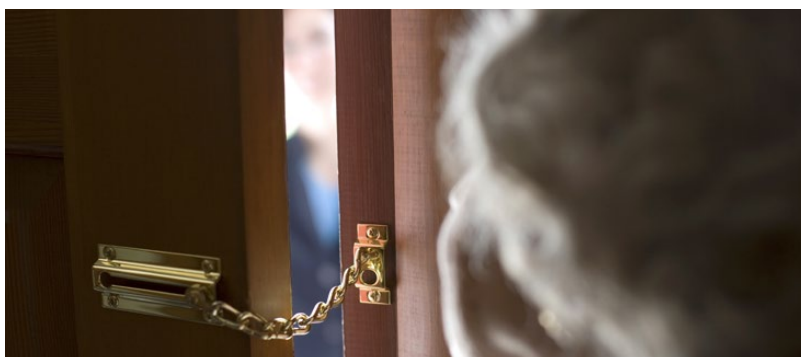
The Scam:

The scam may begin with an unwanted telephone call offering to renew your magazine subscription, a knock at the door from a “student” claiming they are raising money for some good cause, or a direct mail solicitation that may appear to be an invoice for a current subscription or a renewal offer. None of these offers come from the actual magazine publisher and, if you ever get the magazines you ordered, it will likely to be much more expensive than if you dealt directly with the publisher.

How to Avoid it:

Here are some simple ways to recognize a magazine sales scam and to avoid paying exorbitant prices for unwanted subscriptions:

- The solicitation looks like a bill, comes in an “official” envelope, but contains fine print that says “this is not a bill.”
- Door-to-door or telephone solicitation demands immediate payment or uses emotional pleas to get you to subscribe.
- Solicitation promises large savings over “cover price” or similar terms.
- The scam artist claims to be from the actual publisher or to have authority to act for the publisher.
- If you have an existing subscription, any renewal notices should come only from the actual publisher or the company that has been mailing your magazines (called a fulfillment house). Check the mailing label on your current subscription.
- It is easy to check what an actual subscription should cost by checking out the magazine online or at your local grocery or book store.
- Don't get persuaded by high-pressure or confusing solicitations that are designed to get you to act quickly and without thinking. You can ALWAYS close your door, hang up the phone, or throw the mail away!



8 Timeshare Resale Scams

The Scam:

As consumers age, have a decline in their financial situation, or simply change their vacation preferences and habits, they may tire of the burden of regular timeshare fees and assessments. Efforts to sell your timeshare on Craigslist or other Internet sites, or through a timeshare transfer company, end up costing you thousands of dollars in processing, application, or transfer fees, only to see the promised buyers disappear at the last moment. And, of course, you then learn that all of those fees you paid up front are non-refundable.

How to Avoid it:

BEFORE you contract with any timeshare reseller or transfer company:

- Contact your resort or condominium management company or homeowner's association and find out whether they offer re-purchase or reselling programs and whether they have any experience with the reseller or transfer company you are considering.
- Do your homework—review the company's business report and complaint history from the Better Business Bureau. Search for the company or individual on the Internet to see what kind of experience and reputation they have.
- Timeshare interests in Colorado are considered to be interests in real property and any person offering to sell, exchange, buy or rent a timeshare interest, or offering to list a timeshare interest for sale must be a licensed real estate broker by the Colorado Division of Real Estate. Ask whether the reseller or transfer company is properly licensed, in which state they are licensed, and their license number. Then, check them out with that state's licensing agency (many states allow you to do this online).

Here are some basic warning signs and tips to help protect you from these scams:

- You receive unsolicited offers or sales pitches, especially when they include promises like "we have a buyer waiting for your timeshare," "we guarantee you will make a large profit on the sale," or similar statements.
- The reseller or transfer company only uses a PO box or other mail forwarding service and won't give you an actual physical address (independently check any address out on the Internet to make sure it's not a vacant lot or other phony address).
- You are asked to make an immediate payment by wire transfer, money order, or prepaid gift or money card.
- The offer suggests that you are about to be hit with an historic increase in resort or condominium fees or assessments, or similar appeals to scare you into acting quickly.

9 Charity Fraud

The Scam:

Typical charity fraud includes fundraising for non-existent charities, donated dollars being spent for non-charitable purposes or personal expenses, and misrepresentations about an organization's charitable or tax-exempt status. Charity fraud costs billions of dollars each year in lost donations to legitimate charities doing important work to benefit the public. Charity scams often take advantage of natural disasters or national tragedies and tug on your heart strings, patriotism, and emotions.

Avoid it:

Red Flags of a Charity Scam:

- Won't provide proof that a contribution is tax deductible.
- Thanks you for a pledge you don't remember making.
- Uses high-pressure tactics like trying to get you to donate immediately, without giving you time to think about it and research the charity.
- Asks for donations in cash or asks you to wire money.
- Offers to send a courier or overnight delivery service to collect the donation immediately.

Important questions to ask or research BEFORE making a donation:

- Confirm that the solicitation is from the charity, and not an imposter, by contacting the charity or visiting its website.
- Check out the charity before you give to learn more about it through www.checkthecharity.com.
- If a solicitor calls you: ask for their registration number and the registration number of the charity they are representing. This will help you investigate the charity with the Secretary of State.
- Ask every solicitor how much of your donation will actually go to the charitable organization. If you think the amount is too low, tell them, "No thank you."
- Ask every solicitor and charity: "Is my contribution tax deductible?" Charities must indicate their tax-exempt status in their registration statements. Tax exempt does not necessarily mean that contributions are tax deductible.



10 Identity Theft

The Scam:

Identity theft occurs when someone fraudulently uses your personal identifying information to obtain credit, take out a loan, apply for government benefits, employment, credit cards, loans, and even medical services, or any other activity in which a criminal uses your information in a fraudulent way. Identity theft is about more than the loss of money—it is about the loss of security, independence and self-worth. Your identity can be stolen through the theft of a purse or wallet, phony email and websites that trick you into revealing personal and financial information, computer hacking, or even going through your trash.

Avoid it:

Here are some practical steps you can take to minimize your risk of identity theft:

- NEVER give out personal identifying information (address, date of birth, Social Security Number) or financial information (bank or credit card numbers) in response to unsolicited calls, emails, texts or advertisements.
- Never provide personal identifying or financial information over the telephone if you did not initiate the call.
- Never respond to e-mail or “pop-up” messages on your computer claiming some problem with a credit card, Internet, or other account. Promptly contact your real credit card company or Internet Service Provider to verify that there are no problems with your account.
- Use a “cross-cut” shredder, and get in the habit of shredding all personal or financial documents before placing them in the trash.
- Be careful with your incoming and outgoing mail. If you don’t have a secure, locked mailbox, mail your bills from a curbside public mailbox or directly at your local post office. Never leave outgoing mail in an unsecured mailbox overnight.
- Consider placing a “security freeze” on your credit reports. It’s free and it won’t allow anyone else to apply for credit in your name.
- Have current and active anti-virus software installed and running on your home computer.
- If you’re using a public Wi-Fi network on a computer, tablet, or phone, do not visit any password protected site (such as a bank, credit card company or health or insurance site).
- Use secure passwords for all of your accounts. Do not use common numbers or personal information (like birth dates or part of your social security number) or commonly chosen words (such as a child’s, a spouse’s, or pet’s name) for passwords.

Contacts

Colorado Attorney General's Office

<http://coag.gov> <http://www.stopfraudcolorado.gov/>
<http://www.stopfraudcolorado.gov/seniors>
<http://www.stopfraudcolorado/fraud-center/identitytheft>

Ralph L. Carr Colorado Judicial Center
1300 Broadway, 10th Floor
Denver, CO 80203
(720) 508-6000
Consumer Line: 1-800-222-4444

Federal Trade Commission (FTC)

<https://ftccomplaintassistant.gov>
<https://identitytheft.gov>

Major Credit Bureaus

Equifax: www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285

Experian: www.experian.com
P.O. Box 9532
Allen, TX 75013
1-888-EXPERIAN (397-3742)

TransUnion: www.transunion.com
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289

A free copy of your credit report is available from the website
www.annualcreditreport.com

Social Security Administration

<http://www.ssa.gov/myaccount>

AARP Foundation ElderWatch

1-800-222-4444, selection 2

We Are Here To Help You!



www.coag.gov
www.stopfraudcolorado.gov
Consumer Line 1.800.222.4444

Colorado Attorney General's Office
Ralph L. Carr Colorado Judicial Center
1300 Broadway, 10th Floor
Denver, CO 80203

