# **Types of Scams**

This is just a sampling of the scams out there. Scammers want your personal information or money, so guard both fiercely. Never, ever give either your personal information or money to a stranger – over the phone, via email, or someone who knocks on your door. Only trust people you know. Scammers are very, very good at what they do. They don't want you to think; they want you to act fast and say yes, and they will manipulate or trick you to get what they want. This is not the time to be polite. Don't answer the door, hang up, or delete messages.

#### **Advance Fee Loans**

Scammers trick you into paying money to qualify for a loan or credit card. They may "guarantee" a line of credit or promise to deposit money in your bank account once you pay an initial fee. Despite these claims, you will not receive a loan, credit card or any money. Never pay in advance to qualify for a loan or credit card.

### **Bogus Job Opportunities**

Scammers post bogus job offers on various employment websites. The scammer uses or sells the personal information you provided in the job application.

#### **Credit Repair Scams**

These scams involve false promises that bad credit can be erased, interest rates can be lowered, and debts can be consolidated. Many of these companies charge hundreds or thousands of dollars but do little or nothing to improve your credit. The reality is that they cannot erase accurate negative information from your credit report. With certain exceptions, negative information will remain on your credit report for up to seven years. If you want to improve your credit, contact a nonprofit credit counseling agency or your creditor directly. You may be able to arrange a payment plan yourself – at no or very little cost.

## **Disaster-Related Charity Fraud**

After a major natural disaster, scammers send emails and/or texts to raise money for the victims of the disaster.

#### **Extended Car Warranties**

Scammers find out what kind of car you drive, and when you bought it so they can urge you to buy overpriced or worthless plans.

#### **Fake Checks**

You are sent a check or money order and asked to deposit it in your bank account and wire transfer the sender a portion of the money, minus a nice bonus for you as a "thank you" for helping out. The check or money order you received will be counterfeit, and it will be returned to your bank unpaid and the full amount will be deducted from your account, usually with an additional bank fee. Never wire transfer money to a stranger.

This scam also preys on people trying to sell merchandise on Craiglist or eBay. They will offer to pay you more than you are asking for an item with a cashier's check; then ask you to pay a

portion of it back as a handling fee. The check will be no good, leaving you without your merchandise and having paid a fee.

## Family and Caregiver Financial Exploitation

In the majority of financial abuse cases involving the elderly, family members, caregivers and friends are the offenders. They might use the seniors' credit cards without permission, pressure them to sign over their power of attorney, or forge their signature. Signs of financial exploitation include a senior's bills going unpaid, a new "best friend," exclusion from other family members or friends, unusual bank activities, or missing belongings.

#### **Foreclosure Rescue Scams**

These scams target homeowners who are having trouble making their house payments. A phony foreclosure rescue company might contact you and promise to negotiate with your lender. You pay thousands of dollars, but the company makes little or no contact with your lender. Never pay an advance fee for a loan modification.

In some cases, a phony "investor" offers to buy your house and lease it back to you until you can afford your mortgage payments. The investor takes your money, but does not transfer the mortgage loan or pay your lender. As a result, you risk losing your equity and your home. Help is available for free. Call Save the Dream Ohio toll-free at 888-404-4674.

## **Foreign Lottery Scams**

You receive a letter, email, or phone call telling you that you may have won a foreign lottery. All you have to do to collect your winnings is to wire money to the caller for taxes or a "processing fee." Foreign lotteries are illegal and it's impossible to win a lottery you have never entered. Never wire money to a stranger.

#### **Free Lunch**

The scammer invites a hundred people to a seminar, where he or she presents an unbeatable investment opportunity. You must sign up right now. You can't sign up later because he or she is leaving town in two hours, and so will your money.

#### **Free Trial Offers**

Some companies use free trials to sign you up for products – sometimes lots of products – which can cost you lots of money because they bill you every month until you cancel.

#### **Gold Coin Scams**

Scammers call you and offer you a fabulous deal on gold coins, promising you that they will double in value in the next one to two years. Or the scammers take out an ad – on the radio, on TV, or on a billboard – describing how the world economy is shaky and the only thing you can really rely on during periods of economic uncertainty is precious metals. You call a toll-free number and are pitched on buying gold and silver coins that will absolutely go up in value. The coins are being sold at a 300-500% mark up and you will lose money the minute you buy them.

# Government Agency: IRS, Medicare, Affordable Care Act, US Treasury, etc. Scam

First, you may receive a call from someone claiming to be with the IRS or US Treasury. They assert that you failed to pay a correct amount in taxes for a previous year, or a petition has been filed against you for tax fraud. Then they demand immediate payment. The demand is coupled with a threat. Usually people are told that they will be arrested in the next couple of hours. Others threaten a costly lawsuit and imminent action by the IRS to seize assets. To avert this consumers are told to pay immediately. Charges are typically \$2000 or so.

Second, many of these calls are now coming in the form of robocalls. If you don't answer the call they will leave a voicemail message providing a call back number. Consumers are told that this is their "final notice," and the IRS is filing suit against them.

The IRS stresses that it never makes telephone calls to collect taxes. The IRS never takes payment through Western Union, MoneyGram, stored value cards or gift cards. Call the IRS to check it out at: IRS at 800-829-1040.

The caller may claim to be from Medicare or from "Obamacare" to offer you medical coverage or insurance. Medicare never makes calls, and you do not sign up for the Affordable Care Act over the phone, and no one in the insurance industry would call it Obamacare.

## **Grandparent Scam**

The caller pretends to be your grandson or granddaughter and says that they have been arrested for drunken driving or they are being detained for some other reason, often in another city or country, and they need you to wire them money to get them out of trouble. They may have gotten your granddaughter's name from social media, or they may have waited for you to say, "Is this Katie?" and then they continue the ruse. Sometimes, they will even put a "lawyer" on the phone to talk to you. When in doubt, ask the caller a question only your family members would know how to answer and call your son or daughter to confirm the location of your grandchild. Never wire money to a stranger.

## **Home Improvement Fraud**

This occurs when contractors or companies do little or no work they were paid to do. Door-to-door contractors may offer to repair your roof, pave your driveway, or trim your trees for a good price. Scammers may say they will give you a discount or that they have leftover supplies from repairing another house in the neighborhood. After you pay, however, the contractor disappears without doing any work or after doing a poor job.

To avoid home improvement scams:

- Beware of contractors who show up at your door. Ohio law requires that sellers give you a three-day right to cancel most door-to-door sales, and no work should begin before the three days.
- Don't make large down payments or pay in full until the work is complete.
- Get the exact cost in writing. Don't accept verbal estimates.
- Research a contractor by calling the Ohio Attorney General's Office and Better Business Bureau.

## **Identity Theft**

Identity thieves steal your personal information and use it without your permission. They use information, such as your Social Security number, to obtain credit, take out a loan, receive medical treatment, get identification, open new accounts, and purchase products. Identity theft can disrupt your finances, credit history, and reputation, and take time, money and patience to resolve.

#### To avoid identity theft:

- Never, ever give your Social Security number or Medicare number to anyone you don't know or trust. Don't give it to someone over the phone or in an email.
- Do not carry your Social Security card or Medicare card with you.
- Read your bank, credit card, and account statements, and the explanation of medical services.
- Shred all documents that show personal, financial, and medical information.
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the messages.
- Create long and strong passwords: use a minimum of 8 characters and mix upper and lowercase letters, numbers and symbols. Don't use the same password for more than one account, and store it in a safe place away from your computer.
- If you shop or bank online, use websites that protect your information. The web address will start with "https"; "s" is for secure.
- Set your computer's operating system, web browser, and security system to update automatically.

#### **Investment Fraud**

A scammer will offer you a "risk-free" investment in any number of items: real estate, coins, precious metals, or oil, for example, promising you astronomical returns. They promise the investment will make you rich, or absolutely double in value. They use something you want — money and economic security — to get your emotion up, in the hopes of triggering an impulsive decision. All investments involve risk, and you should research a company and only invest with people you know or trust.

## **Living Trust Scams**

A living trust is a legal arrangement in which assets are transferred into a trust while the consumer is still alive, which keeps the assets from going through probate court when the consumer dies. Trusts can be useful estate planning devices, but scammers use high-pressure sales tactics to scare seniors into buying a living trust, making exaggerated or false claims about probate costs or the tax advantages of living trusts. Never buy legal services from door-to-door salespeople or telemarketers. Call Pro Seniors to discuss your estate planning options.

#### Oil and Gas Scams

The caller tells you that they are drilling for oil, often off the Gulf Coast or in Mississippi, and they have new technology that allows them to find oil where no one else has ever been able to

drill. The caller will claim to be a registered broker and claim that the investment is registered with the SEC. Never invest with someone you don't know or trust.

#### **Phishing**

Scammers "phish" for your personal information using emails, social media sites, and the Internet.

- 1. Email: They pretend to be from your bank, government agency, or store (i.e. Target or Sears) and ask you to update or verify the account, often because there is a problem. They ask you to submit a Social Security number, bank routing number, or birth date. Never respond to unexpected requests for your personal information.
- 2. Impostor customer care: Cybercrooks create fake customer service accounts, via slight keyboard tweaks (say, an extra underscore or character), to intercept messages tweeted to banks, e-commerce or video game producers and phish for log-in and financial account information. "The consumer poses a question to a support site and within minutes receives a response (from an impostor account) providing a link to a solution, which, of course, is also a fake," notes Devin Redmond, vice president of social media security and compliance at Proofpoint. "The customer not only expects the response, he or she welcomes it and has incentive to follow the link." If you choose to use social media customer care, be sure to look for the "verified" logo in all communications.
- 3. Live-stream lures: The bait is phony comments and promises of live video streams of popular events, such as a big football game or boxing match available only in certain markets or on pay-per-view. The hook? Links that lead to scammer-run websites, where there's no sneak peek, only an attempt to get personal and credit card details, often under the guise of a fake free trial.
- 4. Fake freebies and discounts: Con artists set up legitimate-looking social media accounts that claim to offer free or dirt-cheap products and services. It's easy pickings for swindlers to collect names, addresses, phone numbers, emails and other information that they can use for identity theft or to sell on the black market, along with credit cards "required" for shipping and handling charges.
- 5. Contest cons and survey swindles: In this oldie but goodie, fraudsters post promises of a prize for completing a survey, but the goal is to mine personal information. Crooks' posts and links appear authentic with URL shorteners.
- 6. Gossip gotchas: Search terms of celebrity names, coupled with terms such as "video" and "picture," have long been among the internet's most typed and most dangerous for malware. The latest celeb-centric scheme: links that promise illicit videos of Hollywood elite, sports superstars and other household names. Along with malware, many phish for credit card info.

#### **Phony Charities**

Someone pretending to represent a charity calls or sends you a letter asking you to make a charitable donation.

## **Prizes/Sweepstakes Scams**

The scammer claims that you have won a contest, lottery, or prize that you never signed up to win. To collect your winnings, you'll be asked to pay a fee. Often you'll be instructed to send money via wire transfer or money order, typically to a foreign country, or give your credit card number. They'll tell you to expect your winning once you pay, but the prize never arrives. Remember that legitimate sweepstakes are free and require no up-front payment.

## **Reverse Mortgage Abuse**

A reverse mortgage is a loan accruing interest that allows older consumers to convert home equity into cash. Unscrupulous salespeople will pressure you into taking out a reverse mortgage that has very high fees. Others pressure you to use the money from the loan to buy annuities or investments that may not benefit you. Do not take out a reverse mortgage unless you fully understand all the costs, terms, and conditions. Keep in mind that reverse mortgages substantially reduce your home equity, and the total amount you owe will grow over time.

#### Sale of Unbeneficial Annuities

When you buy an annuity, you give a large sum of money to an insurance company, and it pays you back on a regular basis, usually for as long as you live or for a specific period of time. There are many different kinds of annuities, and buyers should clearly understand which type of annuity they are buying, what it will cost them, when the company will be paying the money back, the amount of early withdrawal penalties, and the risk factors involved. Scammers, using high-pressure sales tactics, will charge high fees and sell deferred annuities that often are not suitable for the consumer's current age and financial situation. Read all the terms and conditions and seek advice from people you trust before making a major financial investment.

## **Stealing Mail or Sensitive Documents**

Personal information is taken from your trash, your office, or from social media and used to steal your identity. Shred all documents that show personal, financial and medical information, and be careful not to post personal information – bank account information, Medicare number, Social Security number, address, or even birthday – on social media.

#### **Sweetheart Scams**

Scammers create personas on dating websites and express an interest in you. They build an emotional bond with you and then start asking you for money.

## **Tech Support Scams**

You receive an email or phone call claiming to be Microsoft, telling you there is a problem with your computer and they need to install an anti-virus program for \$99, or some other fix for a cost. You are led to a website where the scammer "proves" there is a problem. Afraid of the consequences of inaction, you allow the con to take remote control of your computer and they

actually install a virus and charge you for it. They can essentially hold your computer hostage until you pay.

After you pay, another scammer will call and offer to "fix" your computer, demanding more money to restore your computer, except that they won't fix it. Instead they will ask for more and more money.

#### **Travel Scams**

These scammers promise free or discounted trips, post phony rental listings, deep discounts if you join a travel club, or tell timeshare sellers they've got a buyer lined up.

#### Signs it is a scam:

- You "won a free vacation" but you have to pay some fees first
- The prize company wants your credit card number
- They cold-call, cold-text, or email you out of the blue
- They don't or can't give you specifics
- You're pressured to sign up for a travel club for great deals on future vacations
- You get a robocall about it

The key to planning a good trip is making sure you're buying from travel businesses you know and trust:

- Get recommendations
- Call to verify your reservations and arrangements
- Get a copy of the company's cancellation and refund policies before you pay for the trip, and ask "What if...?"
- Pay by credit card
- Ask about mandatory hotel "resort fees"

#### **Veterans' Scams**

Veterans, particularly those who are over 65, are at particular risk from imposters, caregivers, and family members because they often have benefits through the US Department of Veteran Affairs, making them targets for a scam that involves "poaching" your pension.

Dishonest advisers claim to offer free help with paperwork for pension claims. The scheme involves attorneys, financial planners, and insurance agents trying to persuade veterans over 65 to make decisions about their pensions without giving them the whole truth about the long-term consequences.

Specifically, these unscrupulous brokers try to convince veterans to transfer their assets to a trust - or to invest in insurance products - so they can qualify for Aid and Attendance benefits. What they don't reveal is that these transactions could mean that the veteran loses eligibility for Medicaid services or loses the use of their money for a long time. Adding insult to injury, the advisers are charging fees that range from hundreds to thousands of dollars for their services.

Furthermore, this type of scam is often directed toward veterans and family members who do not actually qualify for VA pension. You could be required to repay these benefits to the government.

Examples of possible pension poaching scams:

- Organizations that cold call veterans, charge money for assisting with a VA pension claim, and take credit card information from veterans over the telephone.
- People who charge as much as \$6,000 upfront to represent claimants before VA, with a percentage of any eventual back payment from VA as a portion of the ultimate fee

For more information about VA pension eligibility requirements—which include special monthly pension benefits—go to www.benefits.va.gov/pension or call 1-800-827-1000.

Other types of scams targeting veterans involve imposters claiming to be from the VA. If you are contacted by someone claiming to be from TRICARE or the VA, do not share any personal information.

Other Types of Veteran Scams

- "Special Deals" for Veterans
- Imposter scams: claim to be from the VA and need to "confirm" or "update" their records
- Investment advisors posing as "Veteran Advocates"
- Charging for access to your military records
- Sweetheart scams & "lucky winner" scams
- Charity fundraising
- Online auctions claiming to be active duty military, getting ready for deployment.

#### **Work-at-Home and Business Opportunity Ploys**

These scams claim that you can make good money working from home or getting involved in a business opportunity. You will be asked to pay in advance for materials, or start-up costs, or training. You should never pay to have a job. Research any business by contacting the Ohio Attorney General or Better Business Bureau. And remember, if it sounds too good to be true, it is.

Information gathered from: The Ohio Attorney General's Elder Fraud Brochure, the Federal Trade Commission's Phone Scams booklet, the AARP Fraud Watch Network, and "Top Phishing Scams on Social Media" from AARP.