As the state’s consumer protection agency, the Minnesota Department of Commerce is committed to empowering older adults and their families to protect themselves against financial fraud.

In recent years, we have strengthened our efforts to protect Minnesota’s older adults by working closely with law enforcement, prosecutors, financial professionals, consumer advocates and community organizations.

We know that, every day across Minnesota, older adults are targeted by fraudsters and scam artists. It can happen to anyone, whoever they may be and wherever they may live.

Fraud against older adults takes many forms – from classic Ponzi schemes with phantom investments promising “guaranteed” profits to fake sweepstakes and lottery scams. It can even involve a family member, friend or caregiver who abuses their trust and exploits an older adult’s vulnerability to steal from them.

The common denominator among all these predatory practices is that they aim to take older adults’ hard-earned savings.

The best line of defense is prevention through education, because knowledge is power.

Each of us has the power to stop fraud before it starts. We need to know how to identify the red flags which signal that an older adult’s savings and financial well-being may be in danger. That is what this financial fraud prevention toolkit is all about.

We want every Minnesotan to know that Commerce is here to help. We encourage you to contact us whenever you have a question or concern about a potential financial fraud or scam at 651-539-1600 or 800-657-3602 (Greater Minnesota).
Trust ... but verify. Most frauds and scams are based on exploiting people’s trust. It’s okay to say “NO!”

It’s not that you should never trust anyone. You should always be wary of a stranger or an acquaintance who is trying to get your money. However, even if it is a family member or a financial professional you have known for a long time, you should still verify what they are doing with your money. Get a second opinion and closely monitor your finances.
Phone Scams

Hang Up on Fraud!
Financial Fraud Prevention for Older Adults and Their Caregivers

Telephone scams are an increasingly prevalent form of fraud. The ordinary telephone is today’s weapon of choice for criminals.

One of the most common complaints reported by seniors and their loved ones is how often they encounter scams and fraudulent schemes over the phone. Common examples of fraud:

- “I’m calling from Microsoft and it appears you have a computer virus...”
- “You’ve won a foreign lottery and you just need to send money to claim your winnings...”
- “This investment is low risk and high return.”
- “This offer is good for today only.”
- “This is your grandson and I’m in jail and need bail money.”
- “You owe money and face serious consequences.”
**Scammers use public information to find out your name and phone number.**

They often use scare tactics to get you to send money, provide personal information or gain access to your computer. If someone calls and wants you to hand over money, be very suspicious. Remember, if it sounds too good to be true, it probably is.

**End the call:** Don’t be a “courtesy victim.” When it comes to protecting yourself, there is no such thing as being rude. Just end the conversation and hang up the phone.

- Never give out your personal or financial information over the phone.
- Be suspicious of any call from a stranger asking you to give them money, even if they claim to be with a law enforcement or government agency.
- If you get a call from someone who claims to be a law enforcement official and is making an unusual request, ask for their name and agency. Call the agency directly (not the phone number they might give you) to confirm that they are who they say they are.
- Don’t trust caller ID, because it can be easily “spoofed” to show a fake name or number.
- Use common sense. If something doesn’t sound or feel right, it probably isn’t

**Phone a friend:** If you are confused or concerned by a phone call, contact a trusted friend or family member for advice. Don’t let a caller rush you into making a decision.

**Report the fraud:** We can’t stop fraud that we don’t know about. Call us and report the fraud so that other don’t become victims. You can contact the Minnesota Department of Commerce Consumer Services Center at 651-539-1600 or 1-800-657-3602 (Greater Minnesota) or by email at consumer.protection@state.mn.us.
If you are thinking of selling a timeshare, be wary if you receive a phone call unexpectedly from someone who claims to be an eager buyer or an agent who promises they can sell the property at a good price – sometimes for more than the property is worth. Timeshare properties can be difficult to sell and scammers take advantage of this through various schemes.

The scam happens when the timeshare owner is asked to make an upfront payment, allegedly for closing costs, taxes or other fees. The scammer instructs the owner to wire funds to an offshore bank account with a promise that the money will be held in escrow until the sale is finalized.

Many times, the scammer will then disappear with the owner’s money. Sometimes, however, they will ask for yet more money for fees that have suddenly “come up.” Either way, the owner rarely sees their money again.

The Commerce Department offers Minnesotans the following tips to avoid timeshare resale scams:

- **Don’t pay upfront fees.** Legitimate fees should be paid as part of the closing or deducted from the sale price.

- **Don’t wire money or send a money order or cashier’s check.** It is almost impossible to recover these funds if you have been scammed.

- **Be wary of an overeager buyer.** Scammers identify timeshare owners through public databases and real estate records. They will cold call or mail materials, offering purchase terms that are often too good to be true. These tactics are a red flag that the offer could be a scam.
• **Do some homework.** Check the would-be buyer or agent’s name, phone number and address on the internet. If you have trouble finding information, or if what you find looks suspicious, the offer could be a scam.

• **Contact the home timeshare resort where you own your timeshare.** See if they have any information on the reseller who contacted you. Often, a resort will have its own buy-back or resale program, or it can provide a list of reputable agents.

• **Do not provide personal information,** bank account information or credit card information over the phone to a reseller. Remember, these scammers are also out to steal your personal information for identity theft.

• **Watch out for imposters:** A sophisticated update of the timeshare resale scam is where a con artist impersonates a legitimate business with an offer to sell your timeshare to an eager buyer. However, after you turn over money for “fees,” the supposed reseller disappears along with the fictitious buyer. All the more reason to never pay upfront fees until closing.
If you are concerned by reports of a widespread data breach or believe your personal financial information has been compromised, the Commerce Department recommends the following actions as potential safeguards.

Request a credit freeze on your credit report

A freeze restricts access to your credit report, which makes it nearly impossible for someone to open a new account or line of credit in your name.

If you have been a victim of identity theft, Minnesota law allows you to place a freeze on your credit report for free. Minnesotans can also request a credit freeze for any reason as a preventive measure for a $5 fee. Credit reporting agencies must place the freeze within three days of receiving a request and provide a unique PIN to you within 10 days of the request.

To request a credit freeze, contact each of the nationwide reporting companies:

- Equifax: 1-800-349-9960
- Experian: 1-888-397-3742
- TransUnion: 1-888-909-8872

Be prepared to provide your name, address, date of birth and Social Security number.

If you want someone (such as an insurer or landlord) to have access to your credit report, you will need to temporarily lift or remove the freeze. Check with each credit reporting company on the cost and how much advance notice they will need to lift the freeze. You will also need to continue monitoring your credit cards and bank accounts for fraudulent transactions.
Place a fraud alert on your credit report

If you have been a victim of fraud or identity theft, you can request a fraud alert at no charge by contacting each of the three credit reporting companies. You must prove your identity and the alert is active for 90 days and can be renewed.

A fraud alert tells potential lenders or creditors that you are a victim of fraud and they should take steps to verify the identity of anyone trying to open an account or borrow money in your name.

With a fraud alert in place, you can also request a free copy of your credit report from each of the three credit reporting companies.

Paying for services to protect your identity

You may have seen advertisements for services that claim to protect you from identify theft, but you should consider if it is worth the cost. These services often charge a monthly fee for actions you can do yourself for free, such as monitoring your accounts and requesting a credit freeze.

Check for suspicious or unauthorized activities

Review your credit report and if you find accounts fraudulently opened in your name, close them and contact your credit card companies to reissue new cards if any legitimate accounts have been compromised.

Closely monitor your accounts with creditors including credit cards companies, banks, credit unions and other lenders during the months following any breach.

Consider filing your tax returns early

To prevent someone from fraudulently filing a tax return with your information and getting your tax refund, file as soon as you have all the needed information.

Beware of “asset recovery” scams

These scams pack a “double whammy” by targeting individuals who have already been victims of fraud. They will lure victims with the promise of getting your money back for an upfront fee and it’s unlikely they will deliver on their promise.
The financial well-being and long-term care needs of aging parents can be among the most sensitive, difficult issues for families to discuss. While it may be an uncomfortable topic, it is important that adult children have these discussions with their aging parents ahead of time to prevent potential problems and misunderstandings down the road.

We encourage Minnesotans to take the time to talk with their loved ones about their financial commitments and long-term care wishes. To get the conversation started, Minnesotans can start with these four questions:

Do you and your parents know the red flags of a scam?

According to the Investor Protection Trust, one out of every five persons over the age of 65 has been the victim of a financial swindle. One recent study estimated that older Americans are defrauded out of nearly three billion dollars each year.

Be sure that your parents know how they can protect themselves from fraud. For example, they should avoid giving out personal information to strangers in response to texts, emails or calls, regardless of who they claim to be or from where they claim to be calling. Be alert for behaviors that may indicate your parent is a victim of financial exploitation, such as unpaid bills, an unexplained lack of money or the sudden appearance of a new “friend.”
What is the plan in case of cognitive issues or other health problems where your parents may not be able to take care of their own finances?

Encourage your parent to officially ask someone to serve as their medical and financial proxy or power of attorney. It is best if your parent chooses someone who they trust to make their financial decisions. If possible, there should be agreement within the family about the responsible person. This person should also maintain clear communication with all family members.

Where do your parents keep their accounts, records, insurance policies and other important financial documents in case they are needed?

If an elderly parent’s health suddenly deteriorates, out-of-pocket expenses can add up quickly. Discuss all sources of income and insurance coverage to determine how and if your parent might cover unanticipated medical treatment. If your parents agree, familiarize yourself with their insurance coverage and financial assets such as savings, pension plans, stocks, IRAs and 401(k) plans. Income, assets and insurance affect Medicaid eligibility and Medicare options.

What are your parents’ wishes for their assets, estate and future quality of life?

Ask your parents whether they have created a will and where it is located. Know your parents’ views on end-of-life care as well, and make sure you, or someone else, records their preferences in an official document such as a living will or advanced health care directive long before they no longer are capable of expressing informed consent.

Is your parent comfortable with the prospect of living in a nursing home, or do they have plans to move in with a family member or friend should special care be required? Be open and direct about your ability to honor these wishes. If your parents need nursing home care, it is important to know if their monthly income meets state eligibility requirements for Medicaid.
Protect Yourself Online

Hang Up on Fraud!

Financial Fraud Prevention for Older Adults and Their Caregivers

There are some simple steps you can take to help keep your personal financial information secure when using the internet and accessing your online accounts.

**Protect your online accounts:** Create a strong password with at least 10 characters and a combination of letters, numbers and symbols. Use different passwords for different accounts. Otherwise, if one password is compromised, all of your accounts using that same password would be vulnerable, too. Remember to change your passwords every few months.

**Access your accounts safely:** Make sure your computer’s anti-virus, firewall and other security software are up-to-date. Avoid using public wireless networks that don’t require a password. Check for the padlock icon in the upper left corner of your internet browser, which signals the website you are using is encrypted. Be sure to log out of your account and close your browser when you are finished.

**Monitor accounts for suspicious activity:** Regularly monitor your online bank and credit card accounts. Consider making it a quick Saturday morning routine. Keep track of your transactions so that you can spot suspicious activity and report it immediately to your bank or credit card company.

**Protect your devices with a password:** Restrict access to your smart phone or computer tablet with a password that will protect your information in case the device is lost or stolen. A device that is unlocked without a password is vulnerable. Anyone who comes across your device could gain access to your email, text messages, social media and any financial accounts that you are logged into.

**Limit where you save your information:** Saving credit card, bank or contact information on a retail website may be convenient when it comes time to check out online, but it increases the risk of your information being compromised. If an online retailer is hacked, your information could fall into the wrong hands.
**Just delete it:** Don’t click on a link or open an attachment in an email unless you are absolutely certain who the sender is and the link or attachment is safe. Malicious links and attachments can secretly download software to steal information from your computer. To be better safe than sorry, call the sender and confirm that they actually sent you the email with the link or attachment.

**Ask questions:** You should also hold your investment and financial professionals accountable for cybersecurity. Talk with your investment professionals about what steps they take to safeguard client information.

**Using social media safely**

Social media is a great way to stay connected, but you need to be careful how much information you share.

- **Use social media wisely.** Posting personal information such as your birthday or where you went to school can provide cybercriminals with enough clues to steal your identity and open fraudulent accounts in your name.

- **Adjust your privacy settings:** Your privacy settings on social media might broadcast your posts and personal information to a wider audience than you may realize. Check to see who can view your information and posts.

- **Keep your guard up:** Social media can connect you with people who share your common interests. However, there are cybercriminals who may target you online in the hopes of gaining your trust. Once your guard is down, they will try to get you to reveal personal information to steal your identity or even convince you to send them money.
Pension Advance Scams

Hang Up on Fraud!
Financial Fraud Prevention for Older Adults and Their Caregivers

Pension scams prey on older adults under financial stress. Avoid products that promise fast cash for your pension and read the fine print before signing over control of your benefits.

Pension advance scams often target government retirees or former military service members. The scam involves investors who offer cash advances to pensioners who are willing to turn over future pension payments in exchange for an immediate lump-sum cash payment. The upfront cash comes with a cost in the form of high fees and interest rates.

The Commerce Department offers retirees and former service members the following guidance to protect their pensions.

Retirees: Questions to ask before you sell your pension rights

- How financially secure is the company that is offering to buy your entitlement? Check the background of the principals before entering into the agreement.

- How does the company make its money? The company typically takes commissions and other fees that may result in the cash payout being lower than the future benefits you are assigning. Do these costs outweigh the convenience of a lump-sum payment?

- Do you know what restrictions, if any, apply to your ability to assign your pension benefits? Check with your pension administrator to determine what restrictions apply. The transaction could be illegal and therefore void.

- Does the company require you to purchase life insurance that names it as the beneficiary? If so, you should consider this increased cost when considering whether the payout is worth it.

- Did you consider the tax consequences? The lump-sum payment you receive may be taxable as income.
Protect your pension

If you are considering a pension advance to meet your immediate financial needs, consider your alternatives:

- **Understand your options:** Work with a financial counselor affiliated with the National Foundation for Credit Counseling or the Association of Independent Consumer Credit Counseling Agencies. Affiliation with these organizations ensures that the member agencies meet certain quality and ethical standards and that the credit counselors receive proper training.

  - Choose an agency that offers free face-to-face counseling sessions to discuss your spending habits, arrange a budget and help you handle your personal finances. Signing up for consumer credit services or a debt reduction plan over the phone or the internet puts you at risk for losing money to a fraudulent enterprise.

- **Read the fine print:** Predatory lenders will rush you into signing away your rights and may mislead you when it comes to fees and interest rates or may mischaracterize the product so it seems like it is not a loan. Look for hidden fees and make sure you understand how much you will be paying for the loan in added fees and interest rates. In Minnesota, victims of predatory pension advance scams were misled into getting loans with illegal and excessive interest rates.

- **Be wary of offers that come over the phone or online:** If you get a call or find a loan through the internet, check that the business is licensed with the Minnesota Department of Commerce. The Commerce website has a License Lookup tool to search whether a lender is licensed. Contact the Commerce Consumer Services Center at 651-539-1600 or 800-657-3602 (Greater Minnesota) or consumer.protection@state.mn.us if you have a question or concern.
Tips for Smart Investing

Hang Up on Fraud!
Financial Fraud Prevention for Older Adults and Their Caregivers

• Check the registration and background of the individual selling the investment. Anyone selling a security must register with the Minnesota Department of Commerce, unless they qualify for an exemption. Check the status of a registration using the License Lookup tool on the Commerce website at mn.gov/commerce. To check the registration of a specific investment product, call the Minnesota Department of Commerce Securities Unit at 651-539-1638.

• Develop a personal financial plan that meets your needs. Be sure recommendations you receive are consistent with your financial needs, risk profile and investment objectives.

• Beware of promises promoting high or unrealistic returns in a short period of time.

• Diversify everything – Your assets, money managers, accounts and financial institutions. Spreading money around will limit your exposure to risk.

• Beware of investments promoting no downside or risk. All investments have some degree of risk.

• Do your homework. Ask questions and do your research about investments and those who sell them. Get clear and direct answers before investing. Don’t rely on reputation or word of mouth alone.

• Beware of vague or overcomplicated explanations of how a business runs and how money is made. If you don’t understand how it works, do not buy it.
• **Understand the cost.** Ask about risks, obligations and costs before investing. Keep in mind commissions, sales charges, maintenance or service charges, transaction fees and penalties associated with the investment.

• **Understand how to access your funds in a timely manner.** Before you invest, ask about restrictions or limitations on accessing your money. Don’t tie up your money in a restricted investment if you may need it on short notice.

• **Ask questions about cybersecurity.** Before you make an investment, be sure the firm or individual selling you the product has a satisfactory plan in place to protect your private data from cybersecurity threats.

• **Report investment fraud or securities violations to the Minnesota Commerce Department.** Your call may help prevent others from being victimized.

---

### Confused by titles?

The following are types of financial professionals that may provide securities-related advice:

• **Investment Advisers** (and investment adviser representatives) make specific investment recommendations based on your needs and owe a fiduciary duty to make those recommendations in your best interest. The investment adviser is paid a fee for the service they provide or may charge a percentage of the market value of the securities in your portfolio.

• **Financial Planners** are not licensed under Minnesota laws and rules. Any person may call themself a “financial planner.” If a financial planner provides investment advice for a fee, they must be registered as an investment adviser (investment adviser representative). If someone presents themselves as a financial planner, you should ask them about the licenses they hold and the services they provide.

• **Brokers** (and broker agents) buy and sell securities on your behalf and may provide investment recommendations. When making a recommendation, the agent is required to make suitable recommendations based on your investment objectives and risk tolerance.
Buying and Selling Bullion Products

Hang Up on Fraud!
Financial Fraud Prevention for Older Adults and Their Caregivers

You may see an advertisement or receive a telemarketing call promoting gold or other bullion products as an investment opportunity. As with any investment, you should first do careful research to make sure you fully understand the product and the risks. It is also important to know who you are dealing with in order to avoid scams.

Bullion products are defined by Minnesota law as any coin, round, bar or ingot containing silver, gold, platinum, palladium or other precious metal. Bullion product dealers and their representatives who do business with Minnesota consumers must be registered with the Minnesota Department of Commerce. If you are thinking about buying or selling bullion products, the Commerce Department offers tips to recognize red flags that could mean trouble, as well as questions to ask before you make a decision.

Red flags

When someone is trying to sell you bullion products, watch out for these red flags of potential fraud.

- **Cold calls.** While legitimate salespeople may call you uninvited, the phone also remains the weapon of choice for fraudsters. Don’t feel you have to stay on the line and be “Minnesota Nice” – just hang up.

- **Fear tactics.** Scammers exploit fears of a big economic downturn and claim that “rare coins” will provide financial protection. Don’t let fear distract you from making a sound decision.

- **“Act now.”** Don’t fall for a sales pitch that creates a false sense of urgency. You should always take time to make an informed decision.

- **“Double your money.”** Avoid investments that are pitched as having no risk or offering unrealistic returns. If a deal sounds too good to be true, it probably is.

- **Bait and switch.** Unscrupulous dealers try to entice you with artificially low prices and then use high-pressure sales tactics to get you to buy more expensive products or products that might not exist at all.
• **Inappropriate investment advice.** You may be pushed to put your “paper investments” into precious metals. Be suspicious of any salesperson who offers specific investment advice or recommends what you should do with your stocks, bonds, retirement accounts or savings.

During the sales transaction itself, watch out for these red flags.

• **The dealer will only accept a check or wire transfer.** These transactions are more difficult to cancel or get your money back. While you should always be cautious about giving out your credit card information, credit card transactions generally have more consumer protections.

• **No documentation.** Missing documentation about the product you bought or incomplete information on the invoice you receive could mean you are not getting what you paid for.

• **Delayed delivery or payment.** If you do not receive the purchased product or the payment on a product you sold in 30 days, contact the Minnesota Commerce Department for assistance at 651-539-1600 or 800-657-3602 (Greater Minnesota only).

**Do your homework**

Always ask hard questions before you put your money in any investment. Here are some key considerations to help you make an informed decision about investing in bullion products.

• **Evaluate your goals.** Carefully assess whether bullion products, including their risks, fit with your financial goals. Talk it over with family members, a trusted friend or an independent financial adviser.

• **Fully understand what you are buying.** Avoid investing in products that are unfamiliar to you. For example, numismatics and collectible coins cost substantially more than bullion coins or products sold only for their precious metal content.

• **Check if the dealer is registered.** Make sure the dealer is registered with the Commerce Department and see if there have been any disciplinary actions. Search the internet for any complaints against the company.

• **Ask how the dealer is paid.** A reputable dealer will not hide from you the commission they receive from a transaction.

• **Verify the product’s authenticity.** Ask for information on the authenticity of a product’s precious metal content. Don’t stop there. Make sure the information is not fake by researching the company that provided it.

• **Check the product’s “melt” value.** This is widely available and represents the actual, “intrinsic” value of the product.

• **Comparison shop prices.** You should always shop around for up-to-date price information. For collectible and rare coins that contain precious metals, you can look up approximate values in coin publications available at the library or a bookstore. For bullion products, it is best to check the internet for the current spot prices of precious metals.
As an older investor, you may be a top target for con artists. Don’t be cheated out of savings, windfall insurance payments or even the equity in your home.

You can avoid becoming a victim by following these self-defense tips, developed by the Minnesota Department of Commerce and the North American Securities Administrators Association (NASAA).

- **Don’t be a courtesy victim.** Con artists will not hesitate to exploit your good manners. Save your politeness for friends and family members, not strangers looking for a quick buck!

- **Trust, but verify.** Say “no” to anyone who presses you to make a quick decision. Take time to research the salesperson, firm and investment opportunity.

- **You can check the status of an individual’s ability to offer investments** using the License Lookup tool at the Commerce website: [mn.gov/commerce](http://mn.gov/commerce) or if an investment is registered with the Commerce Department by calling 651-539-1638.

- **Stay in control.** Be wary of anyone who suggests investing your money in something you don’t understand, or who urges you to leave everything in their hands.

- **Don’t judge a book by its cover.** Successful con artists sound and look extremely professional and can make even the riskiest investment deal sound safe. Don’t be fooled by the sound of their voice on the phone because it has no bearing on the soundness of the investment opportunity.

- **Don’t make decisions out of fear.** Fear can cloud your good judgment and cause rushed decisions. An investment that is right for you will make sense because you understand it and feel comfortable with the risk involved.
• **Monitor your investments and ask tough questions.** Don’t add to the mistake of trusting a fraudulent investment professional or con artist by failing to keep an eye on the progress of your investment. Insist on regular written reports, and look for signs of excessive or unauthorized trading of your funds.

• **Ask questions about cybersecurity.** Make sure the firm or individual selling you a product has a plan in place to protect your private data from cyber threats.

• **Look for trouble withdrawing your principal or cashing out profits.** Some investments do have certain periods when you cannot withdraw your funds, but you must be notified of these restrictions before you invest.

• **Don’t let embarrassment or fear keep you from reporting investment fraud or abuse.** Every day you delay reporting fraud or abuse is another day the con artist is spending your money and finding new victims.

• **Beware of “asset recovery” scams.** These scams pack a “double whammy” by targeting individuals who have already been victims of fraud. They will lure victims with the promise of getting your money back for an upfront fee and its unlikely they will deliver on their promise.

• **Beware of “Senior Specialists.”** Fraudsters may imply a certain level of training on issues important to people 55 and older to give you a false sense of security. However, this “training” may be nothing more than a sales tactic. They often recommend liquidating assets to purchase other, more risky products like indexed or variable annuities.

---

**Report suspected fraud, scams, or financial abuse to the Minnesota Department of Commerce. Your call may prevent others from being victimized.**