LEARN, PREVENT, & PROTECT

yourself with tips to spot scams and keep you safe.

www.IowaFraudFighters.gov

IOWA | Department of Insurance and Financial Services

INTRODUCTION

The Iowa Department of Insurance & Financial Services is here to help you learn and empower yourself against con artists.

This booklet provides ways to protect yourself with expert fraud prevention tips, reporting resources, and more to help you stay a step ahead of fraudsters.

TABLE OF CONTENTS

ABOUT US

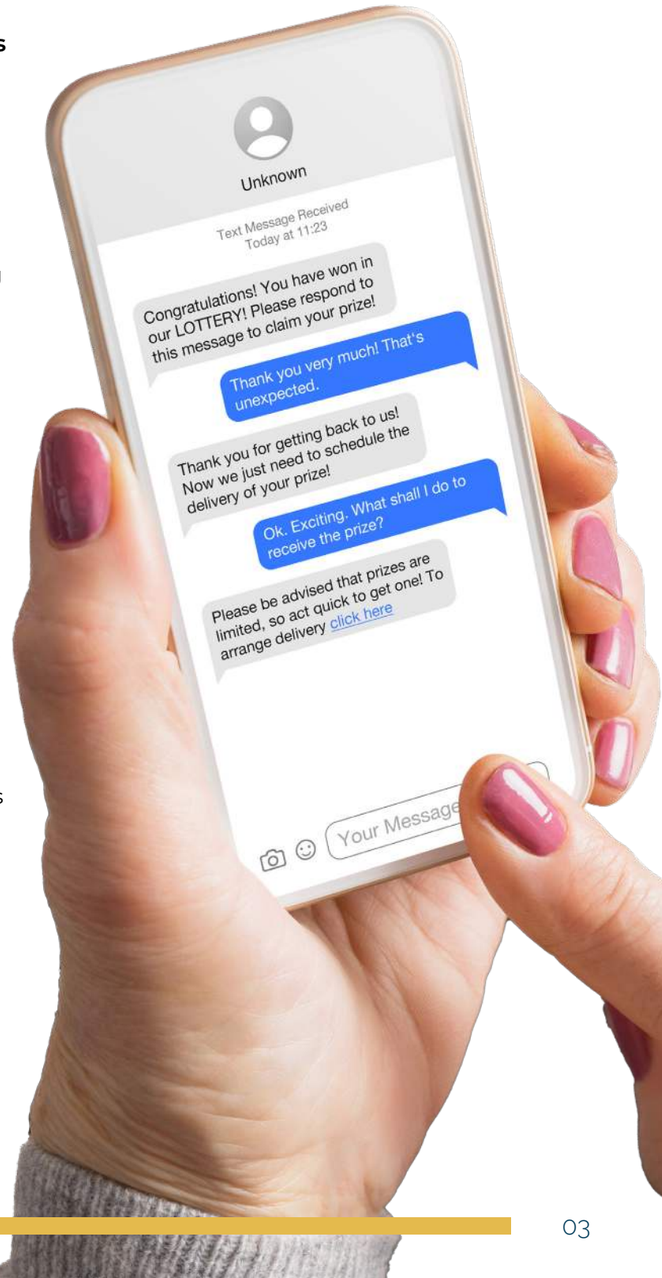
Did you know there is a whole team dedicated to helping Iowans learn more about scams and ways to prevent fraud? The Iowa Department of Insurance & Financial Services is here to help Iowans identify and avoid scammers' latest tactics.

About Fraud Fighters, a program of the Iowa Department of Insurance & Financial Services

Iowa Fraud Fighters are Iowans who have pledged to be informed and careful investors. Iowa Fraud Fighters shield their savings from scammers and fraudulent investment, consumer, and Medicare insurance offers. Arm yourself with expert fraud prevention tips and learn how to avoid scams. It's time to take a stand and shield your savings. You can become an Iowa Fraud Fighter by empowering yourself to fight and report fraud. The Iowa Department of Insurance and Financial Services and other state agencies are here to help you. You can see more about us by visiting https://iowafraudfighters.gov.

About Senior Health Insurance Information Program (SHIIP) and the Senior Medicare Patrol (SMP)

According to the World Economic Forum, cybersecurity attacks are on the rise, costing U.S. taxpayers $8.8 million per data breach (2022). Medicare and Medicaid fraud, errors, and waste cost taxpayers over $100 billion per year. The Senior Health Insurance Information Program (SHIIP) and the Senior Medicare Patrol (SMP) help Medicare beneficiaries, their families, and their caregivers prevent, detect, and report fraud by encouraging monitoring of Medicare statements; being cautious of emails and links online requesting personal and health information; and reporting any suspicious calls requesting your Medicare number to 1-800-MEDICARE, or SHIIP-SMP at 1-800-351-4664



INVESTMENT SCAMS

Ponzi or pyramid schemes promise high returns, often "guaranteed" for investors, but collapse when new investors can't be found. These schemes use funds from new investors to pay off the initial investors. Each group of new investors is used to pay off an earlier, smaller group of investors, while the majority of the money disappears into the scammer's pocket at the top of the pyramid.

Promissory notes are used by companies to raise money by selling debt, typically paying a high interest rate, to an investor. Con artists often sell promissory notes for companies that do not exist, so always check that a company is legitimate before purchasing these.

Affinity fraud targets groups, such as religious or ethnic communities, by using trusting relationships with influential or respected members of the group to attract more investors in a pyramid-type scheme.

Private placement offerings, or Regulation D, Rule 506 offerings can be used by small companies to raise funds. These offerings are unregulated and are often very risky investments or scams.

Oil and gas drilling programs are always high risk and should be researched carefully to avoid scams, especially those claiming a particular well is guaranteed to produce high returns or have attractive tax advantages.

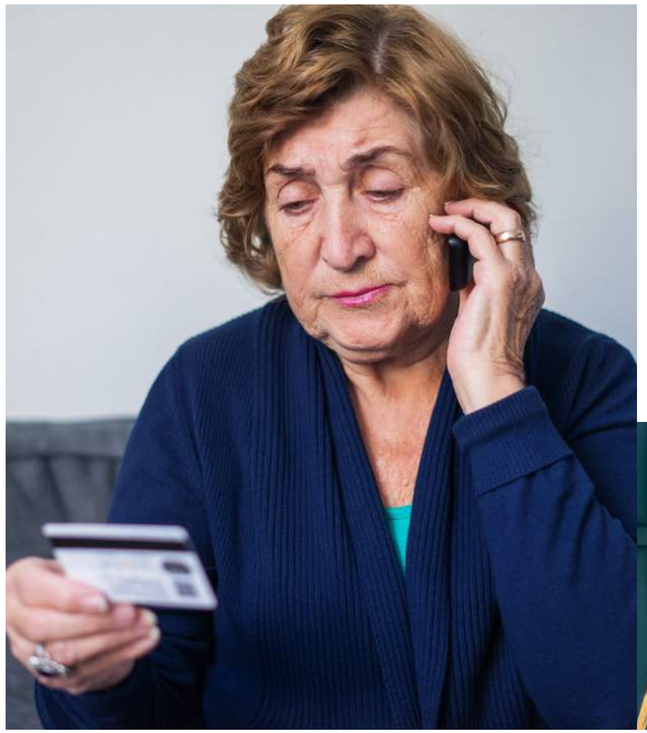
Gold and precious metals are always risky investments. It may be a scam if the seller wants you to invest in gold mining or to purchase gold or other precious metals that will be delivered to a secured facility. Be sure the company is genuine and ensure the gold or precious metal you purchase does exist.

Free dinner seminars are often advertised in local newspapers, on websites, or through mass-mailed invitations or emails. Many of these seminars are used to sell investment products at the seminar or through later communications. Be wary if guilt, fear, or high-pressure tactics are used to try to sell products.

Self-directed IRA fraud often occurs when a scammer misrepresents the responsibilities of self-directed IRA custodians by falsely suggesting that your investment is protected or that your self-directed IRA custodian will investigate the investment offer for you.

High-yield investment products are peddled by scammers claiming to have access to the world's leading financial institutions or banks. The scammers promise high returns at little or no risk to you by enrolling you in an elite or secret investment venture, often called a prime bank investment.

Cryptocurrency is a digital or virtual currency not regulated by a bank or financial institution and may be used for purchases or investments. Many cryptocurrency investment opportunities are promoted through popular social media sites by individuals claiming to be experts. Often, legitimate cryptocurrency purchases are made by victims and transferred, unknowingly, to the scammers.



MOST COMMON SCAMS

In the digital age, scammers have adapted to use many different ways to reach us, including phone, email, texts, online, and in-person. Here are some of the most common scams:

CONSUMER SCAMS

Investment schemes shouldn't be the only thing you need to guard yourself against. Fraudsters are always looking for ways to get access to your personal or financial information and money.

Computer tech support scams occur when con artists pose as technical support employees calling to request remote access to your computer to fix a virus or download software to improve your computer. They use the access to steal personal information or cause damage. They then can charge you a fee for "fixing" your computer.

Grandparent scams are used to coerce money from older Iowans by con artists who pretend to be a grandchild calling from a foreign country in desperate need of money to get out of jail or some other urgent trouble.

Romance scams occur when con artists strike up romantic relationships, often through social media or online dating sites, to coerce money from victims, often for travel expenses to visit the victim or for hardships the perpetrators claim they are going through.

Home repair scams are common when there has been a damaging weather event, such as a flood or tornado. Scammers pretending to be contractors or home repair specialists selling home evaluations and repairs in affected areas before disappearing without providing the services that were paid for.

Identity theft occurs when someone uses your personal information to open accounts, file taxes, or make purchases. As of July 2018, you can now freeze your credit. Refer to iowa.gov/difs for more information.

Imposter calls are robocalls that claim the IRS, other government entity, or a business is filing suit against you for owed taxes or threatening to send police to your residence if you don't pay a specific amount using prepaid cards. Remember, the IRS and other government entities will notify you by mail if it is transferring an outstanding debt to a private collection agency.

Lottery and sweepstakes scams occur when fraudsters charge an entry fee for sweepstakes or contests, or con artists sell international or out-of-state lottery tickets to Iowans. They typically seek advance payment of taxes or fees before they send a prize that never arrives or a check that bounces. If you have to pay a fee to receive your winnings, it's a scam.

Counterfeit check scams occur when con artists send you a check and ask you to cash it and wire the money back to them. Often referred to as Nigerian check scams, the scammer might offer to let you keep some of the money from cashing the check. These checks bounce because they are fake, and you're held responsible for the funds withdrawn.

SCAM TACTICS:

How They Try to Convince Us

Criminals use a variety of persuasion tactics to convince us of an untruth to steal our money or sensitive information – and they are good at it. Scammers may try to go after our money through cash, wire transfers, money transfer apps, cryptocurrency, and gift cards. Here are some of the tactics common to today's scams:

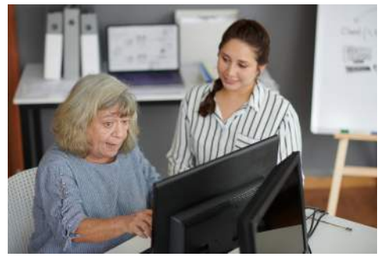
Phantom Riches
The prospect of wealth is behind many common scams, and the criminal's goal is to pressure the target into believing that a large bounty awaits. Fake lottery winnings and surefire investment schemes commonly use the phantom riches technique to coerce targets. Criminals create legitimate-looking shopping sites online and even create faux versions of the online stores of well-known retailers. If you are told you've won a sweepstakes or a lottery, but you just need to pay some fees upfront to claim your winnings, it is a scam.

Profiling
The profiling tactic involves the criminal gathering key pieces of information about the target and using that information to establish credibility and elicit an emotional response. The goal is to get the target to act quickly to address an "urgent" situation. For example, today's scammer may peruse social media accounts to gather enough information to impersonate a family member in trouble. Be careful what you are sharing on social media and don't give out any personal information to someone you don't know!

Fear and Intimidation
Criminals commonly use fear and intimidation to get their targets. Many cases we hear about begin with inducing immediate fear, such as telling you your grandson is in danger, the police have a warrant for your arrest, or your computer has a deadly virus. And we've heard from victims that criminals will harass them, calling dozens of times a day and leaving threats on their voicemails.

Scarcity
Criminals use the human impulse to stockpile limited supplies, alleging scarcity to convince us to act before it's too late. The early months of the coronavirus pandemic were replete with fake ads for much-desired personal protective equipment, while later it was about jumping the line to get the vaccine or quick access to in-demand testing.

Source Credibility
Impostor scams rely on getting the target to believe the contact is coming from a credible source — often a government agency, bank, or major business. Common social media scams involve fake profiles that appear to be celebrities, or new "friends" with profiles that are a mix of invented and stolen information.



FRAUD PREVENTION TIPS

Now that we know some of the most common scams and ways scammers try to reach us, let's take a look at some fraud prevention tips.

Tips to Prevent Consumer Fraud

- Don't respond to urgent pleas for money by phone, even if the caller sounds like a family member. Call that relative at a number you know to verify his or her situation.
- Be wary of people who show up at your door and seek upfront payment.
- Don't send money to someone you've never met in person, no matter how well you think you know him or her.
- Don't give unsolicited "support representatives" access to your computer. Always contact a known computer expert first.

Tips to Prevent Investment Fraud

- Always double check that the person selling you investments is licensed and the product they are selling is a registered investment product.
- Do your research! Use an open source to check on the seller, the product, and any related companies associated with the investment.
- Consult with your current financial advisor and/or talk to a trusted family member or friend about the investment opportunity.
- Document everything you're told regarding the investment and any transactional history if you decide to invest.

Tips to Prevent Medicare Fraud

- Stay informed about enrollment – Get the enrollment dates and plan information from an official source, make an appointment with a SHIIP representative to review plan options, and remember that Medicare plans cannot be sold door-to-door.
- Don't carry your Medicare card – Unless you're going to the doctor's office, it is best to leave your card at home in a safe place.
- Protect your personal information – Medicare will never call to ask for your personal financial information or Medicare number because they already have it.
- Review your statements – Check your statements each month for unfamiliar charges or charges for services/products you did not receive.
- Confirm suspicious mailings – If a Medicare mailing looks suspicious, SHIIP and Senior Medicare Patrol can review it and confirm if it is an official mailing or a scam.

If you need assistance to report Medicare fraud, learn more about your Medicare coverage options, or review your statements, please contact a SHIIP representative or your local Senior Medicare Patrol.

SHIIP IOWA'S MEDICARE RESOURCE

SMP Senior Medicare Patrol Preventing Medicare Fraud

OUR TOP 10

Fraud Prevention Tips

1. Don't be a courtesy victim. It's OK to just say no and hang up.
2. Check out anyone you don't recognize. Always contact the Department of Insurance and Financial Services at 877-955-1212 to double check that the financial professional and the investment offer are legitimate.
3. Monitor your money. Insist on receiving regular reports on your investments and financial accounts, check your credit score reports every year, and freeze your credit.
4. Never judge a person's integrity by the sound of his or her voice. Scammers know how to sound professional and friendly to gain your trust.
5. Watch out for salespeople who prey on your fears or other emotions. Scammers know you worry about your savings, but don't let fear cloud your judgment when you invest.
6. Take your time. Take the time you need to research, get advice, and learn more about investing.
7. Be wary of unsolicited offers. Be careful if you can't find current information about their company. If it sounds too good to be true, it is probably neither good nor true.
8. Always ask questions. Question everything. Your financial advisor or stockbroker is required to explain any restrictions before you invest.
9. Watch out for "reload" scams. If you lost money once, don't let scammers trick you into trying to recoup it.
10. Don't be embarrassed to report fraud. Reporting fraud is a responsible step in handling your finances, so don't be afraid or embarrassed to report it if you are victimized. You can save another person from becoming a victim.

DOUBLE-CHECK BEFORE YOU INVEST

Use this form to collect the information you will need to verify any investment seller or company before you make an investment. (Additional copies can be downloaded from www.IowaFraudFighters.gov.)

Seller/Agent and Company Information

Seller/Agent Name_____

Company/Business Name_____

Company/Business Address_____

Phone Number _____ Email _____

What Services Are Being Offered?

Investment:

☐ Stocks and Bonds
☐ Mutual Funds
☐ IRAs
☐ Private Placements
☐ Oil & Gas/Minerals

Insurance:

☐ Life
☐ Annuities
☐ Viaticals

Financial Planning:

☐ Investment Advice
☐ Financial Planning
☐ Wealth Creation

What written information will be provided? _____

Is seller/agent required to act in my best interest? Yes____ No____

Potential conflicts of interest _____

Explain commissions or fees charged _____

Licensing Information

(Call to check names and/or license numbers with Iowa Insurance Division at 877-955-1212.)

Insurance License No:_____ State _____

Securities License CRD No:_____

Other License: _____ No: _____

Always request a CRD report to learn of disciplinary actions taken against the company/business, criminal convictions, settlements, bankruptcies, civil proceedings and customer complaints.

FREEZE!

AND STOP IDENTITY THEFT

With daily reports of credit data breaches and identity theft, it may seem like criminals have the upper hand. There is something you can do to protect yourself, though. Freeze your credit! A credit freeze prevents the sensitive data in your credit files from being accessed without your consent, and that prevents identity thieves from opening fraudulent accounts in your name. It costs nothing to place or lift a credit freeze, and it doesn't affect your credit score.

Who Should Do This?

Everyone, regardless of age, income or credit history. A credit freeze provides maximum protection for your credit files. And it's free.

How to Freeze Your Credit

To freeze your credit, you must contact each of the three major credit bureaus.

Equifax
www.Equifax.com/personal/credit-report-services
1-800-685-1111

Experian
www.Experian.com/help
1-888-EXPERIAN (1-888-397-3742)

Transunion
www.TransUnion.com/credit-help
1-888-909-8872

Provide your name, address, date of birth, Social Security number and other requested information. Each credit bureau will give you a password or personal identification number (PIN).

IMPORTANT: Keep the PIN or password in a safe place where you can access it. You cannot lift the freeze without it. If you lose this information, the credit bureaus cannot look it up for you.

How to Lift a Credit Freeze

If you need to lift a credit freeze – when you're taking out a bank loan, for example, or financing a car – ask your creditor which bureau they use for credit applications. Then contact only that credit bureau to arrange a lift on the credit freeze. There's no need to unfreeze all three credit bureaus.

Select a temporary lift of the freeze, and at the end of a time limit you choose, your credit is automatically frozen again. Or you may choose to unfreeze your credit without a time limit. Just don't forget to freeze your credit again once your credit application is reviewed.

If you make the request by phone or online, the freeze must be lifted within an hour. If the request is made by mail, the credit bureau has three business days after receiving the request.

A Credit Freeze Won't ...

- Prevent you from getting a free annual credit report.
- Prevent you from opening a new account. (Follow the steps to unfreeze your credit, above.)
- Prevent a thief from making changes to your existing accounts. Keep monitoring all bank, credit card and insurance statements for fraudulent transactions.

Don't give out personal information

- For help with questions or concerns about freezing your credit, visit the Iowa Insurance Division at iid.iowa.gov/consumers/advocacy-education/security-freeze-credit-reports.
- To report a suspected theft of your identity, contact the Federal Trade Commission (FTC) at www.IdentityTheft.gov
- For more information on identity theft, visit the FTC at www.consumer.ftc.gov/topics/identity-theft

FREQUENTLY ASKED QUESTIONS

(FAQ)

How can I avoid telemarketing calls?

Don't answer your phone to unknown numbers, let them leave a voicemail. The more you answer your phone to telemarketers and scammers the more calls you will receive. Add your number to the National Do Not Call Registry. Register your phone number by calling 888-382-1222 or visiting www.DoNotCall.gov.

How can I deal with pushy telemarketers?

Don't feel that you have to be nice or polite. You don't have to talk to these people. You can just say no and hang up, or better yet, don't answer your phone to unknown callers.

What if I'm asked for personal information?

Never send money, give out credit card numbers and expiration dates, bank account numbers, dates of birth, personal identification numbers, or Social Security numbers to unfamiliar companies or people you don't know, or if you have not initiated the conversation.

What terms should raise concern about a proposed investment?

Be wary of these terms: high rate of return, risk-free investment, or guaranteed or insured against loss. High rates of return are usually accompanied by high risk and legitimate investments are not guaranteed against loss. If it's too good to be true, it is!

What if I'm pressured into making an immediate decision?

Don't let a salesperson pressure you into a quick decision. Do your own research and call the Department of Insurance and Financial Services at 877-955-1212 and consult with someone you trust before making any purchase or investment.

What protects me from losses associated with my investment?

Securities regulators make sure companies abide by securities laws and rules, but they do not insure investments. You should determine what degree of risk you are willing to take and be prepared to experience possible losses.

Can I trust that professional promotional materials and websites are reliable indicators of legitimate investment opportunities?

Promotional materials, websites, company addresses, and testimonials from investors can all be part of a fraudulent scheme to lure you into a scam. Do your homework before you part with your money.

How can I make sure the people trying to sell me investments or insurance are reliable?

One way is to ask for written materials and then verify the information they provide with the Department of Insurance and Financial Services.

Should I report fraud?

Yes. Don't let embarrassment over your investment stop you from reporting fraud or suspicious activity and protecting others from the same scheme. It is a brave and responsible step to report fraud. Use the contact information in this booklet if you need assistance in reporting fraud.

Still have more questions?

Check out iowafraudfighters.gov or you may also call 515-654-6600, and we will help you answer any questions you may have!

TEST YOUR KNOWLEDGE

Take the test below to check in and see what you have learned.

1. **What state program through the Iowa Department of Insurance and Financial Services is dedicated to helping Iowans prevent and learn more about fraud and scams?**

2. **How might scammers try to contact you?**
   A. Phone.
   B. Email.
   C. Text.
   D. Online.
   E. In-person.
   F. All of the above.

3. **True or False: an investment scam occurs when a fraudster tries to get you to purchase an item.**

4. **If you feel uncomfortable or pressured into sharing personal or financial information over the phone, what should you do?**
   A. Give them the information they are asking for.
   B. Don't be a courtesy victim. It's OK to just say no and hang up.

5. **What should I do if I suspect I am a victim of fraud?**
   A. Do nothing.
   B. Wait a couple of weeks, then talk to someone about what happened.
   C. Only post about it on social media.
   D. File a complaint with the Iowa Attorney General's Office, report the incident to the Iowa Department of Insurance and Financial Services.

Answer Key

(1) Fraud Fighters (2) F (3) False: Investment fraud occurs when someone tries to deceive you into investing money. (4) B (5) D

NOTES

REPORT SUSPICIOUS ACTIVITY

If you or a loved one has fallen victim to scams or fraud, you are not alone. Thankfully, you have a whole team of people who are here to help you report and learn more about fraud. Reporting scams can help prevent fraud for others in the future. Call or visit the below organization's websites to report fraudulent activity and learn more.

Iowa Attorney General
You can file a complaint with the Iowa Attorney General.
(888) 777–4590 / www.iowaattorneygeneral.gov

Senior Medicare Patrol
If you suspect Medicare fraud or to schedule a presentation,
call Senior Medicare Patrol (SMP).
(800) 351–4664 / www.shiip.iowa.gov

Iowa Department of Insurance and Financial Services
Check with the Iowa Department of Insurance and Financial Services
if you suspect investment fraud.
(877) 955-1212 / www.iowa.gov/difs

Division of Aging
If you suspect a dependent adult is being abused, call the Abuse hotline.
If the Adult is in imminent danger, call 911.
800-362-2178 / www.hhs.iowa.gov

IOWA | Department of Insurance and Financial Services

SHIIP IOWA'S MEDICARE RESOURCE