IOWA FRAUD FIGHTERS

SHIELD YOUR SAVINGS

LEARN, PREVENT, & PROTECT

yourself with tips to spot scams and keep you safe.

Presented by

IOWA | Department of Insurance and Financial Services

www.IowaFraudFighters.gov

INTRODUCTION

SCAMMERS ARE GETTING SMARTER, BUT SO ARE YOU.

Whether you're buying online, scrolling Instagram, managing your family's finances, or planning for retirement, scammers are constantly evolving their tactics to target busy people like you. As someone juggling school, work, family, and financial responsibilities, you're particularly vulnerable to sophisticated scams that prey on time, pressure, and trust.

This comprehensive guide will help you recognize common scam tactics, protect your identity, and develop the skills to spot fraud before it impacts your financial security. You've worked hard to build your career and provide for yourself and your family. Let's make sure scammers don't undermine that hard work.

The financial impact of fraud on Iowa families is staggering. In 2023, Iowans lost over $45 million to various scams, with the average victim losing $2,847. For most, this can mean months of financial stress, damaged credit, and the emotional toll of feeling violated. But here's the good news: most scams are preventable when you know what to look for.

TABLE OF CONTENTS

ABOUT US

The Iowa Department of Insurance & Financial Services serves as your first line of defense against financial fraud and predatory practices. Our mission is to protect Iowa consumers from unscrupulous actors who target hardworking families through deceptive investment schemes, insurance fraud, and identity theft.

Iowa Fraud Fighters is our comprehensive public education program designed specifically for Iowans navigating complex financial decisions. Whether you're just starting to learn about money management, a parent teaching your teenagers about responsible financial decisions, a professional managing investments, or someone caring for aging parents, you face unique fraud risks that require specialized knowledge.

Anyone can be a Fraud Fighter! It just means you understand the tactics scammers use, know how to protect yourself and your family, and feel confident helping others recognize potential threats. Our program provides the tools and knowledge you need to make informed decisions and avoid costly mistakes.

Learn more, access additional resources, or join our community of informed consumers at www.IowaFraudFighters.gov.

SCAMS TO KNOW (AND AVOID)

Money Transfer & App Scams

Digital payment apps like Cash App, Zelle, and Venmo have revolutionized how we handle money, but they've also created new opportunities for scammers. The most common version involves fake overpayments: someone "accidentally" sends you too much money for an online purchase, freelance work, or even claims it was meant for someone else. They then ask you to "refund" the difference through a payment app.

Here's what actually happens: the original payment is made with a stolen credit card, fake check, or fraudulent bank transfer. While the money initially appears in your account, it will be reversed within days or weeks once the fraud is discovered. Meanwhile, the "refund" you sent through the payment app is real money from your account, and it's gone forever.

These scams often target people selling items online, freelancers, or anyone who regularly receives payments. The scammers create urgency by claiming they need the refund immediately for an emergency, or they may even threaten to report you for "stealing" their money.

Red flags to watch for:

- Payments larger than the agreed amount
- Requests to refund through a different payment method
- Pressure to send money quickly
- Buyers who seem overly eager or don't ask questions about the item

Fake Marketplace Listings

Online marketplaces like Facebook Marketplace, Craigslist, and OfferUp have made it easier than ever to buy and sell locally. Unfortunately, they've also become hunting grounds for scammers who post fake listings for high-demand items like gaming consoles, electronics, vehicles, and even rental properties.

These scams typically follow a pattern: the listing features stolen photos of the item, an attractive price that's just below market value (not so low as to seem obviously fake), and a seller who seems legitimate at first. Once you express interest, the scammer will create urgency by claiming multiple people are interested, or they'll make excuses for why you can't see the item in person.

The scammer then requests payment through methods that offer no protection: wire transfers, gift cards, cryptocurrency, or payment apps. Once you send the money, the scammer disappears, and you're left with nothing.

Vehicle scams are particularly costly, with some Iowa residents losing thousands of dollars on cars that never existed. Rental scams are also common, targeting people who need housing quickly and may not have time for thorough verification.

Protection strategies:

- Always insist on seeing items in person before paying
- Meet in safe, public locations for transactions
- Use payment methods that offer buyer protection
- Research the seller's profile and history
- Trust your instincts if something feels off

Job Offer Scams

Employment scams have become increasingly sophisticated, targeting professionals looking for remote work opportunities or better career prospects. With the rise of remote work, these scams have exploded, particularly targeting people between jobs or those seeking flexible work arrangements.

The most common version involves fake job postings for legitimate-sounding positions at real companies. The scammer conducts interviews via text or messaging apps, then offers you the job quickly, often without a phone or video interview. They claim you need to purchase equipment, software, or training materials upfront, or they ask for banking information for "direct deposit setup."

Check-cashing scams are another variant: you're hired for a "financial assistant" role and asked to deposit checks and transfer funds. The checks are fake, but by the time the bank discovers this, you're responsible for the money you transferred.

Some scammers target specific professions, creating fake opportunities for teachers, healthcare workers, or skilled trades. They may even use stolen LinkedIn profiles to make their outreach seem legitimate.

Warning signs:

- Job offers that require upfront payments
- Interviews conducted only through text or email
- Salaries that seem too good to be true
- Requests for personal financial information early in the process
- Pressure to start immediately without proper documentation

Subscription Traps

Free trials have become a standard marketing tactic, but many companies use them to trap consumers in unwanted subscriptions. While some legitimate businesses offer genuine free trials, scammers and unethical companies exploit this model to generate recurring revenue from consumers who forget to cancel or face deliberately complicated cancellation processes.

These traps often start with advertisements on social media promising free samples of health supplements, beauty products, or weight loss solutions. The fine print, often hidden or written in confusing language, reveals that you're actually signing up for automatic monthly shipments that can cost as much as $80-200 per month.

Some subscription traps are even more deceptive, offering "free" trials that require only shipping costs, then charging your credit card repeatedly for different products or services you never agreed to purchase. They may also sell your information to other companies, resulting in multiple unwanted subscriptions.

Common subscription trap categories:

- Health and beauty products
- Streaming services with hidden fees
- Credit monitoring services
- Software subscriptions with auto-renewal
- Membership programs with escalating fees

Romance & Online Dating Scams

Romance scams are among the most emotionally and financially devastating frauds, with victims losing an average of $4,400 according to recent FTC data. These scams target people on dating apps, social media, and even professional networking sites, exploiting the natural human desire for connection and companionship.

The scammer typically creates a fake profile using stolen photos and develops a detailed backstory. They may claim to be deployed military personnel, traveling professionals, or widowed individuals. The relationship develops quickly, with the scammer expressing deep feelings and discussing future plans together.

Once trust is established, the scammer creates a crisis requiring immediate financial assistance: a medical emergency, legal trouble, travel complications, or a business opportunity that requires quick funding. They may ask for money transfers, gift cards, or even cryptocurrency, always promising to pay back the money once their situation is resolved.

Some romance scammers operate long-term schemes, building relationships over months or years before making financial requests. Others may ask victims to receive and forward packages, unknowingly making them accomplices in money laundering schemes.

Protection strategies:

- Never send money to someone you haven't met in person
- Be suspicious of people who profess love very quickly
- Verify their identity through video calls and reverse image searches
- Be wary of anyone who repeatedly cancels plans to meet
- Trust friends and family who express concerns about your online relationship

Crypto & NFT Scams

Cryptocurrency and NFT investments have created new opportunities for both legitimate wealth building and sophisticated fraud. Scammers exploit the complexity and volatility of these markets, along with many people's limited understanding of how they work.

Common crypto scams include fake cryptocurrency exchanges, pump-and-dump schemes promoted on social media, and fake celebrity endorsements. Scammers may promise guaranteed returns, exclusive investment opportunities, or claim to have insider knowledge about the next big cryptocurrency.

NFT scams often involve fake marketplaces, stolen artwork, or projects that disappear after collecting investors' money. Some scammers create fake social media profiles of successful crypto investors to lend credibility to their schemes.

Warning signs in crypto investments:

- Promises of guarenteed profits
- Pressure to invest quickly
- Requests for personal wallet information
- Unverifiable claims about past performance
- Social media promotions from unverified accounts

Impersonation Scams

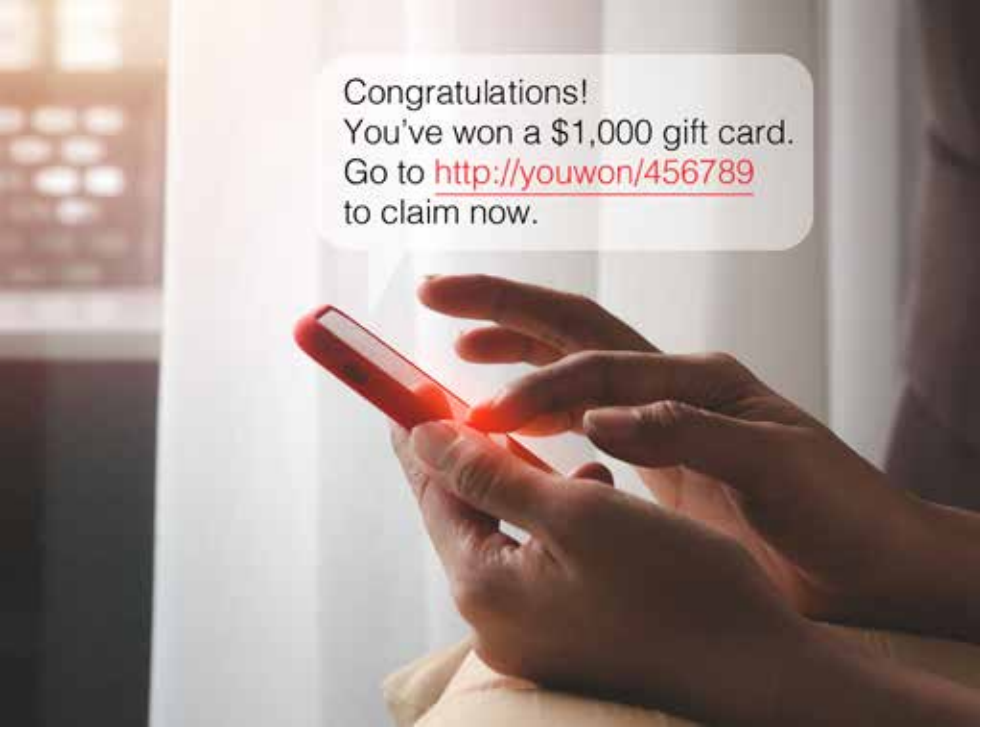
Impersonation scams have become increasingly sophisticated, with scammers using technology to make their communications appear legitimate. These scams involve criminals pretending to be trusted organizations, government agencies, or even people you know personally.

Technology has made these scams more convincing than ever. Scammers can spoof phone numbers to make calls appear to come from legitimate organizations, create fake websites that look identical to real company sites, and even use artificial intelligence to clone voices.

Common impersonation targets include:

- Government agencies (IRS, Social Security, Medicare)
- Banks and credit card companies
- Tech companies (Microsoft, Apple, Google)
- Utility companies
- Employers or coworkers
- Family member in crisis

The scammer typically creates urgency by claiming your account has been compromised, you owe money, or someone you care about needs immediate help. They may ask for personal information, payment through untraceable methods, or remote access to your computer.


Congratulations!
You've won a $1,000 gift card.
Go to http://youwon/456789
to claim now.

SCAM TACTICS:

How They Try to Convince Us

Understanding the psychology behind scams is crucial for protection. Scammers aren't just criminals, they're skilled manipulators who understand human psychology and exploit our natural tendencies to trust, help others, and seek opportunities for financial gain.

Social Profiling

Modern scammers are sophisticated researchers who use social media, public records, and data breaches to create detailed profiles of their targets. They know where you work, your family members' names, your hobbies, recent life events, and even your financial concerns based on what you share online.

This information allows them to craft personalized approaches that seem incredibly legitimate. They might reference your recent job change, your child's school, or your interest in a particular hobby. This personal touch makes their scam attempt seem like a genuine opportunity or legitimate contact.

Scammers also use this information to identify the best times to contact you, the most effective emotional appeals, and the types of scams most likely to succeed. For example, they might target new parents with work-from-home opportunities or recent retirees with investment schemes.

Limiting your vulnerability:

- Review your social media privacy settings regularly
- Be cautious about sharing personal information online
- Limit location sharing and check-ins
- Be aware of what information is visible to strangers
- Consider what your posts reveal about your financial situation

Fear Tactics

Fear is one of the most powerful tools scammers use to bypass your rational thinking. They create artificial crises that demand immediate action, preventing you from taking time to verify their claims or consult with others.

Common fear-based scenarios include claims that your bank account has been compromised, you're about to be arrested for tax evasion, your computer is infected with viruses, or a family member is in legal trouble. The scammer emphasizes that delay will result in serious consequences: financial loss, arrest, or harm to loved ones.

These tactics are particularly effective because they trigger our fight-or-flight response, making it difficult to think clearly. The scammer reinforces this by setting strict deadlines and discouraging you from discussing the situation with others.

Recognizing fear tactics:

- Threats of immediate arrest or legal action
- Claims that your account will be closed immediately
- Warnings about imminent financial loss
- Pressure to act before consulting others
- Emphasis on secrecy or confidentiality

Phantom Riches

The promise of easy money or incredible returns appeals to our natural desire for financial security and success. Scammers exploit this by offering investment opportunities, work-from-home schemes, or contest winnings that seem too good to pass up.

These schemes often target people facing financial stress, career transitions, or major life expenses. The scammer presents their offer as a limited-time opportunity that requires quick action to secure your spot or take advantage of favorable conditions.

Phantom riches scams are particularly dangerous because they often require upfront investments or personal information that can be used for identity theft. Even when victims realize they've been scammed, they may continue sending money in hopes of recovering their initial investment.

Common phantom riches promises:

- Guaranteed investment returns
- Work-from-home opportunities with minimal effort
- Contest winnings you never entered
- Inheritance from unknown relatives
- Government grants or rebates

Scarcity Pressure

Scammers create artificial scarcity to prevent you from taking time to research their offer or seek advice from others. They claim that only a limited number of people can participate, the offer expires soon, or someone else is competing for the same opportunity.

This tactic is particularly effective in online shopping scams, investment schemes, and job offers. The scammer may claim that hundreds of people have applied for the same position, only a few investment slots remain, or the sale price is only available for a few more hours.

Scarcity pressure often combines with other manipulation tactics, such as social proof (claiming others have already taken advantage of the offer) and authority (implying that important people endorse the opportunity).

Recognizing scarcity pressure:

- Countdown timers on websites
- Claims about limited availability
- Pressure to “act now” or “don’t miss out”
- Statements about competition from others
- Refusal to provide time for consideration

False Authority

Scammers frequently impersonate authority figures to gain compliance and trust. They may claim to represent government agencies, law enforcement, financial institutions, or technical support services. Some even impersonate employers, family members, or other trusted individuals.

The authority figure typically contacts you about a problem that requires immediate attention and cooperation. They may use official-sounding language, reference real procedures or policies, and even provide fake badge numbers or case references to seem legitimate.

Technology makes these impersonations more convincing than ever. Scammers can make phone calls appear to come from legitimate numbers, create fake websites that look identical to real organizations, and even use artificial intelligence to mimic familiar voices.

Verifying authority:

- Always verify contact independently through official channels
- Real authorities provide time for verification
- Legitimate organizations have established procedures for contact
- Be suspicious of authorities who demand immediate action
- Government agencies typically communicate through official mail first

SMART PREVENTION TIPS

DIGITAL SAFETY TIPS

Your digital footprint is your first line of defense against online fraud. Strong security practices not only protect your accounts but also make you a less attractive target for scammers who prefer easy victims.

Account Security: Two-factor authentication (2FA) is essential for all important accounts, especially banking, email, and social media. Even if scammers obtain your password, they can't access your account without the second authentication factor. Use authenticator apps rather than SMS when possible, as phone numbers can be compromised.

Create unique, complex passwords for every account using a password manager. Many people reuse passwords across multiple sites, which means a breach at one company can compromise all your accounts. Password managers generate strong passwords and remember them for you, making this process effortless.

Communication Security: Be extremely cautious about unsolicited communications requesting personal information, money, or urgent action. Legitimate organizations typically don't request sensitive information through email, text, or phone calls. When in doubt, contact the organization directly using official contact information.

Avoid clicking links in suspicious emails or text messages. Instead, navigate to the organization's website directly by typing the URL into your browser. This prevents you from accidentally visiting fake websites designed to steal your information.

Privacy Protection: Review your social media privacy settings regularly and limit what information is visible to strangers. Scammers use personal information to make their approaches seem legitimate, so sharing less publicly makes you a less attractive target.

Be cautious about what you share online, including photos that might reveal your location, financial status, or personal information. Even seemingly innocent posts can provide scammers with information they can use against you.

INVESTMENT SAFETY

Investment scams are particularly dangerous because they can result in significant financial losses and jeopardize your long-term financial security. These scams often target people during major life transitions, such as career changes, retirement planning, or inheritance management.

Verification is Essential: Before investing with anyone, verify their credentials through official channels. All investment professionals must be licensed, and you can check their status by calling **877-955-1212** or visiting the SEC's **investor.gov** website. This process takes just a few minutes but can save you thousands of dollars.

Research the investment product thoroughly, including the company offering it, the risks involved, and the track record of similar investments. Be particularly cautious of investments that are difficult to understand or explain to others.

Red Flags in Investment Offers: Legitimate investments involve risk, and anyone promising guaranteed returns or claiming investments are "risk-free" is likely running a scam. High-pressure tactics, limited-time offers, and claims about exclusive opportunities are also warning signs.

Be extremely wary of investment opportunities promoted through social media, especially those endorsed by celebrities or influencers. Many of these promotions are paid advertisements, and the endorser may not have actually invested in the product.

Documentation and Exit Strategies: Always require written documentation before investing, including clear information about fees, risks, and your ability to withdraw funds. Legitimate investments provide transparent information about costs and liquidity.

Understand how you can exit the investment if needed. Scammers often make it difficult or impossible to withdraw funds, requiring additional payments or fees to access your money.

FAMILY AWARENESS

Protecting your family from fraud requires open communication and coordinated planning. Scammers often target family relationships, impersonating relatives in crisis or exploiting family members' willingness to help each other.

Emergency Verification Procedures: Establish family protocols for verifying emergency requests for money or personal information. Create code words or security questions that only family members know and agree to always verify unusual requests through direct phone contact.

Discuss common scam scenarios with family members, especially those involving impersonation or crisis situations. When everyone understands these tactics, they're less likely to fall victim to them.

Protecting Vulnerable Family Members: Elderly family members and teenagers are particularly vulnerable to certain types of scams. Maintain regular contact with older relatives and discuss their financial activities. Consider setting up account alerts or involving trusted family members in major financial decisions.

Educate teenage family members about online safety, social media scams, and the importance of verifying job offers or investment opportunities. Young adults are often targeted with employment scams and fake scholarship opportunities.

Financial Communication: Maintain open communication about family financial situations without sharing sensitive details publicly.

Scammers often exploit family financial stress or major life changes, so being aware of each other's circumstances helps everyone stay alert to potential targeting.

TOP TEN FRAUD FIGHTER HABITS

01

YOU DON'T OWE ANYONE YOUR TIME

Your time and attention are valuable resources, and scammers try to consume both to prevent you from thinking clearly. Whether it's a phone call, email, or in-person interaction, you have the right to end any conversation that makes you uncomfortable or pressures you for immediate action.

Practice saying "I need to think about this" or "I'll call you back" when faced with high-pressure situations. Legitimate opportunities will still be available after you've had time to research and consider your options.

02

DOUBLE-CHECK EVERYTHING

Verification is your strongest defense against fraud. This means independently confirming the identity of people contacting you, researching companies before doing business with them, and fact-checking claims that seem too good to be true.

Use official contact information to verify requests, rather than phone numbers or websites provided by the person contacting you. When someone claims to represent a company or organization, hang up and call the official number to confirm their identity and the reason for contact.

03

MONITOR YOUR ACCOUNTS

Regular monitoring of your financial accounts helps you catch fraud early, when it's easier to resolve and limit damage. Check your bank statements, credit card bills, and investment accounts regularly for unauthorized transactions.

Set up account alerts for transactions over certain amounts, foreign transactions, or any activity outside your normal patterns. Most banks and credit card companies offer these services free of charge.

Review your credit reports from all three bureaus at least annually through **annualcreditreport.com.** This helps you identify new accounts opened in your name or other signs of identity theft.

04

VOICES LIE, FRIENDLY DOESN'T MEAN LEGIT

Scammers are skilled at building rapport and seeming trustworthy. They may spend considerable time getting to know you, sharing personal stories, and creating a sense of friendship or partnership before making their real request.

Remember that anyone can be friendly and personable, including criminals. Judge people by their actions and verifiable information, not by how likeable they seem or how well they relate to your situation.

05

DON'T BE RUSHED

Time pressure is one of the most common tactics scammers use because it prevents you from making rational decisions. Any legitimate opportunity will give you reasonable time to research, consult with others, and make an informed decision.

When someone insists you must act immediately, that's often a sign of a scam. Take time to step back, research the opportunity, and discuss it with trusted friends or family members before making any commitments.

06

BE SKEPTICAL OF FREEBIES

”Free” offers often come with hidden costs or obligations. Read all terms and conditions carefully, and understand what you’re agreeing to before accepting any free trial, sample, or promotional offer.

Many subscription traps begin with free offers that automatically convert to paid subscriptions. Make sure you understand the cancellation process and set reminders to cancel before any trial periods expire.

07

ASK QUESTIONS

Legitimate businesses and professionals welcome questions and provide clear, consistent answers. If someone becomes evasive, defensive, or annoyed when you ask for clarification, that’s a red flag.

Don’t be afraid to ask for references, credentials, written documentation, or time to research before making decisions. Scammers often try to discourage questions by claiming they’re unnecessary or that asking questions shows distrust.

08

AVOID “RELOAD” TRAPS

If you’ve lost money to a scam, be especially cautious about offers to help you recover those funds. “Recovery” scams target previous victims, claiming they can get your money back for an upfront fee.

Similarly, avoid throwing more money at investments that aren’t performing as promised. Legitimate investments may have periods of poor performance, but they should provide clear explanations and documentation of what’s happening with your money.

09

KEEP YOUR DATA PRIVATE

Your personal information is valuable to scammers, who can use it for identity theft, account takeovers, or to make their scam attempts seem more legitimate. Be cautious about sharing passwords, PINs, Social Security numbers, or other sensitive information.

Never give personal information to unsolicited callers, even if they claim to be from legitimate organizations. Real companies don’t need you to verify information they already have on file.

10

REPORT IT

Reporting scams and fraud attempts helps protect others and assists law enforcement in tracking criminal activity. Even if you didn’t lose money, reporting helps authorities understand current scam trends and develop warnings for other potential victims.

Don’t be embarrassed about reporting fraud, even if you feel you should have known better. Scammers are skilled criminals who exploit psychological vulnerabilities that affect everyone.

INVESTMENT CHECKLIST

PRE-INVESTMENT DUE DILIGENCE

1. Is the seller liscensed and in good standing?

All investment professionals must be registered with appropriate regulatory bodies. Call the Iowa Insurance Division at **877-955-1212** to verify their license status and check for any disciplinary actions or complaints.

Don't rely solely on credentials displayed on their website or business cards, as these can be easily faked. Always verify through official regulatory channels.

2. What are the specific risks and expected returns?

Every legitimate investment involves risk, and you should understand exactly what those risks are before investing. Be suspicious of anyone who downplays risks or claims their investment is "guaranteed" or "risk-free."

Don't ask for specific information about how returns are calculated, what factors could affect performance, and what happens if the investment performs poorly. Get this information in writing.

3. Are there hidden fees or commissions?

Investment fees can significantly impact your returns over time. Ask for a complete breakdown of all costs, including management fees, transaction fees, surrender charges, and any other expenses.

Be particularly cautious of investments with high upfront fees or complex fee structures that are difficult to understand. Legitimate investments provide clear, transparent information about all costs.

4. Who holds the funds and how liquid is the investment?

Understand where your money will be held and how easy it will be to access if you need it. Legitimate investments typically use third-party custodians or well-established financial institutions to hold investor funds.

Ask about withdrawal procedures, any restrictions on accessing your money, and how long it typically takes to process withdrawal requests. Be wary of investments that make it difficult or expensive to get your money back.

5. Is there comprehensive written documentation?

Never invest based solely on verbal promises or informal agreements. All legitimate investments provide detailed written documentation, including prospectuses, offering memoranda, or other disclosure documents.

Take time to read and understand all documentation before investing. Don't hesitate to ask questions about anything you don't understand or to have the documents reviewed by a financial advisor or attorney.

Additional Investment Safety Measures

Research the Track Record: Look for independent verification of the investment's performance history. Be cautious of performance claims that can't be verified through independent sources.

Check References: Ask for references from other investors but be aware that scammers sometimes provide fake references. Try to verify these references independently.

Start Small: Consider making a small initial investment to test the legitimacy and performance of the opportunity before committing larger amounts.

Seek Professional Advice: Consider consulting with a licensed financial advisor who isn't involved in selling the investment. They can provide objective analysis and help you understand how the investment fits into your overall financial strategy.

CREDIT FREEZE INFORMATION

Understanding Credit Freezes

A credit freeze is one of the most effective tools for preventing identity theft and unauthorized account openings. When you freeze your credit, potential creditors can't access your credit report, which means they typically won't approve new credit applications in your name.

Credit freezes are free and don't affect your credit score or existing accounts. You can still use your current credit cards and make payments on existing loans, and your credit score will continue to be calculated based on your payment history and account activity.

When to Consider a Credit Freeze

After a Data Breach: If you've been notified that your personal information was compromised in a data breach, freezing your credit can prevent criminals from using that information to open new accounts.

Before Major Life Changes: Consider freezing your credit before events that might make you a target for identity theft, such as moving, changing jobs, or going through major life transitions.

As a General Precaution: Many security experts recommend that everyone maintain credit freezes as a general precaution, only lifting them when applying for new credit.

How to Freeze Your Credit

Contact each of the three major credit bureaus separately to freeze your credit:

Equifax
800-685-1111
www.Equifax.com

Experian
888-397-3742
www.Experian.com

Transunion
888-909-8872
www.TransUnion.com

You can freeze your credit online, by phone, or by mail. Online is typically the fasted method. You'll need to provide personal information to verify your identity, including your Social Security number, date of birth, and address.

Managing Your Credit Freeze

Keep Your PINs Secure: Each bureau will provide you with a unique PIN or password to lift your freeze. Store these securely and don't share them with anyone. If you lose your PIN, you'll need to contact the bureau to reset it.

Lifting Your Freeze: When you need to apply for new credit, you can temporarily lift your freeze for a specific period or permanently remove it. This can typically be done online or by phone and usually takes effect within a few minutes to 24 hours.

Consider Fraud Alerts: If you don't want to freeze your credit, consider placing fraud alerts on your credit reports. These alerts require creditors to take additional steps to verify your identity before opening new accounts, though they're not as effective as credit freezes.

FAQ SECTION

Communication and Phone Scams

Q: How do I stop scam calls?

A: Don't answer calls from unknown numbers and let them go to voicemail. Block repeat callers using your phone's built-in features or contact your carrier about blocking services. Register your number on DoNotCall.gov, though this primarily affects legitimate telemarketers, not scammers.

Consider using call-blocking apps or services that can help filter out known scam numbers. Many phones now have built-in spam detection that can warn you about potential scam calls.

Q: Someone texted me asking for gift cards, claiming to be my boss. My boss would never ask for this.

A: Trust your instincts! This is a common impersonation scam. Always verify unusual requests through direct contact using a phone number or email address you know is legitimate. Don't use contact information provided in the suspicious message.

Scammers often impersonate employers, coworkers, or other authority figures to pressure people into quick compliance. Real employers have established procedures for purchasing supplies or handling financial matters.

Q: I keep getting calls about my car's extended warranty. How do I make them stop?

A: These calls are typically scams, even if you do own a car. Don't engage with the callers or press numbers to "opt out," as this often confirms your number is active and leads to more calls. Instead, hang up and block the number.

If you're interested in extended warranty coverage, contact your car manufacturer or a reputable insurance company directly rather than responding to unsolicited calls.

Reporting and Recovery

Q: I'm embarrassed I fell for a scam. Should I report it?

A: Absolutely yes. Reporting scams helps protect others and assists law enforcement in tracking criminal activity. Don't feel embarrassed. Scammers are skilled criminals who exploit psychological vulnerabilities that affect everyone.

Report to local law enforcement, the Iowa Attorney General's office, and the Federal Trade Commission. Also contact your bank and credit card companies immediately if you shared financial information or sent money.

Q: What should I do if I gave personal information to a scammer?

A: Act quickly to minimize damage. Contact your bank and credit card companies immediately to report the compromise and monitor for unauthorized transactions. Consider freezing your credit to prevent new accounts from being opened in your name.

Change passwords for all important accounts, especially if you shared any password information. Monitor your accounts closely for several months and consider signing up for identity theft monitoring services.

Q: Can I get my money back if I was scammed?

A: Recovery depends on how you sent the money and how quickly you act. If you used a credit card, contact the card company immediately to dispute the charges. If you used a debit card, contact your bank right away, as you have less protection than with credit cards.

Money sent through wire transfers, cryptocurrency, or gift cards is typically not recoverable. However, you should still report the scam to help prevent others from being victimized.

Investment and Financial Scams

Q: What phrases should make me suspicious of investment opportunities?

A: Be wary of terms like "risk-free," "guaranteed return," "limited time offer," "exclusive opportunity," or "act now." Legitimate investments always involve risk, and high-pressure tactics are common in scams.

Also be suspicious of claims about "insider information," "proprietary trading systems," or testimonials that seem too good to be true. Real

investment opportunities provide comprehensive information and time for due diligence.

Q: How can I tell if a cryptocurrency investment is legitimate?

A: Research the currency thoroughly, including who created it, how it works, and where it's traded. Be extremely cautious of new cryptocurrencies or investment schemes that promise guaranteed returns.

Never invest in cryptocurrency opportunities promoted through social media or by people you don't know personally. Always use established, regulated exchanges for cryptocurrency transactions.

Online and Digital Safety

Q: What's the best way to protect myself online?

A: Use two-factor authentication on all important accounts, create unique passwords for each account using a password manager, keep software and security systems updated, and be cautious about what personal information you share online.

Be especially careful about clicking links in emails or text messages, downloading software from unknown sources, and sharing financial information through unsecured websites or communications.

Q: How can I tell if a website is legitimate?

Look for "https://" in the URL and a lock icon in your browser's address bar. Check for contact information, clear privacy policies, and professional design. Be wary of websites with spelling errors, poor grammar, or pressure to act quickly.

Research the company independently through search engines and review sites. Be particularly cautious of websites that ask for sensitive information or payment details without clear security measures.

Family and Relationship Scams

Q: How can I protect elderly family members from scams?

A: Maintain regular contact and open communication about financial matters. Help them understand common scam tactics and establish procedures for verifying unusual requests for money or personal information.

Consider setting up account alerts, involving trusted family members in financial decisions, and discussing any unusual contacts or offers they receive. Be patient and non-judgmental, as shame can prevent people from seeking help.

Q: My teenager received a scholarship offer that requires an upfront fee. Is this legitimate?

A: Legitimate scholarships never require upfront fees. This is a common scam targeting students and families seeking educational funding. Real scholarships may require application fees to the school or organization, but they don't charge fees to process or guarantee awards.

Research any scholarship opportunities through official school guidance counselors or established scholarship databases. Be wary of unsolicited scholarship offers, especially those that seem too good to be true.

READY TO TEST YOUR SCAM IQ?

1. What's one red flag that a job offer might be fake?

2. **True or False:** It's safe to send money to someone you met on Instagram.

3. What should you do before investing in a crypto opportunity?

4. What's one tactic scammers use to trick you into acting fast?

5. What's your plan if someone impersonates a friend or family member in crisis?

Answer key and online quiz at
www.IowaFraudFighters.gov/quiz

NOTES

NOTES

REPORT FRAUD

If something feels off, report it. It's free, confidential, and helps protect others.

Iowa Department of Insurance and Financial Services
(877) 955-1212
www.iowa.gov/difs

Iowa Attorney General
(888) 777–4590
www.iowaattorneygeneral.gov

Federal Trade Commission (FTC)
800) 351–4664
www.shiip.iowa.gov

BE A FRAUD FIGHTER

Visit www.IowaFraudFighters.gov and:

- Read real scam stories
- Download digital checklists
- Get updates on trending scams
- Share this guide with friends & family

Scammers count on silence. You can break the cycle.
Let's outsmart the scam.

IOWA | Department of Insurance and Financial Services

SHIIP IOWA'S MEDICARE RESOURCE