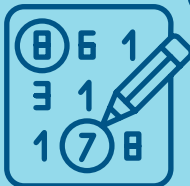
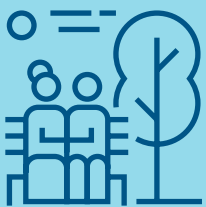
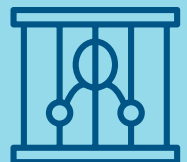
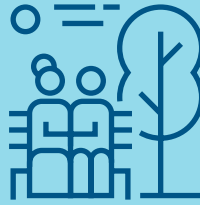
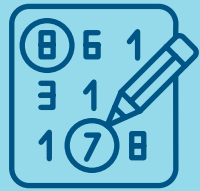




# SCAM SQUAD GUIDE

Simple ways to spot, avoid  
and report scams



# About Scam Squad

Scam Squad is a financial fraud task force created to help Cuyahoga County residents avoid, report and recover from scams.

Scam Squad's goals are to:

- Encourage residents to report scams
- Share scam reports with the agency best suited to investigate
- Alert residents to current scam threats

**The Cuyahoga County Department of Consumer Affairs** coordinates the activities of Scam Squad, whose members include nonprofit, social service and enforcement agencies at all levels of government.

**Report scams to Scam Squad**

**216-443-7226**

**[cuyahogacounty.gov/scamsquad](https://cuyahogacounty.gov/scamsquad)**

# How Scams Work



Scams change often, but most scams use the same basic techniques to convince us to act before we have time to think clearly. Knowing the basics makes it easier to recognize most scams.

## **Scammers manipulate our emotions**

Scammers know that when we're feeling scared, upset or excited, we have a hard time thinking rationally. So, most scams are designed to ramp up our emotions.

## **Scammers lie about who they are**

Scammers use technology to hide their true identities. They spoof, or fake, Caller ID so that it looks like the bank or sheriff is calling. They might mimic a friend's social media account or alter their voices to sound like a grandchild's. So, if we get an unusual request for money, we need to consider that it might really be a stranger asking.

## **Scammers pressure us to act now**

Scammers know if they give us time to think over what they said, we'll notice the flaws in their story. So, scammers say we have to act now, or a great

opportunity will pass us by ... or a bad situation will get worse. These are high-pressure sales tactics, and they're designed to push us to act before we can consider our options.

## **Scammers try to confuse us**

Scammers make up complicated stories, so we doubt our ability to understand or fix a problem on our own. They hope to confuse us enough that we'll rely solely on their instructions. The more confusing a story is, the more important it is for us to take a step back and independently check the facts.

## **Scammers try to isolate us**

Scammers know if we check with someone else, we'll find out their story is fake. So, they make up reasons we shouldn't tell anyone. They tell us to lie to bank tellers. Or they say that if we hang up to check with someone we trust – local police or our family – we'll be in worse trouble. But that's never true.



*It was an elaborate scheme. ...  
They didn't ask for money until  
they had convinced me that I  
needed to begin driving to the  
sheriff's office.*





# What Scammers Want

Most of the time, scammers want our money. And they want us to send it in specific ways that are hard for us to reverse and hard for law enforcement to trace. If a stranger ever pressures you to pay fast, using an unusual payment method, you are talking to a scammer.

## Money

ONLY scammers ask for payments in:

- Gift cards
- Cash sent by mail or a courier (in-person pickup)
- Gold

## Crypto

Cryptocurrency is a new payment method, and it can be confusing. Crypto is a digital currency, which means it only exists virtually.

The most important thing to know about crypto is that scammers love to be paid with it. Why? Because there are no protections against fraud. If scammers can convince us to pay in crypto, our money becomes theirs. Usually forever.

Scammers are sneaky when they try to get us to move our cash into their crypto accounts. They may claim our money isn't safe and that we need to move it into a "government locker." Or they'll try to mislead us by calling a crypto ATM a "government kiosk."

Our money is insured against fraud when it's in the bank. Once we move our money into an app or put our cash in a crypto ATM, we lose that protection.

## Peer-to-peer apps

Scammers sometimes ask for payments on peer-to-peer apps (like Zelle, CashApp, or Venmo). Don't send money to strangers through payment apps.

## Personal information

Personal, or private, information is any information that lets us create or access accounts – Social Security numbers, account numbers and logins, verification codes, PINs and passwords.

Guard this information. Don't tell people your verification codes, PINs or passwords.



**If a stranger asks us to type in codes or download an app, they may be trying to take control of our device to get our personal info or accounts.**



# Imposter Scams

If a stranger asked us to give them lots of money, we'd say no. So, instead, scammers pretend to be people we already know, love or trust.

There's a pattern to these crimes: The scammer contacts us about a problem. The longer we talk to the scammer, the bigger and more confusing the problem seems.

Imposter scams are designed to get us so worried about a made-up problem that when the scammer finally offers an easy "solution" – paying them – we're tempted.

## Government imposters

These scammers usually claim to be deputies or federal agents. They say we're in trouble with the law – maybe they say we failed to show up in court or that our accounts have been linked to crimes. The scammers claim that if we don't pay, we'll be jailed or our accounts will be seized.

Government imposters can be convincing. Scammers may use the names of real deputies or FBI agents. They may email fake court documents. Sometimes they tell people to start driving themselves to jail.

They don't want us to check with others, so they say if we put them on hold, we'll be arrested. Or, they say if we tell a family member, that person will be an accessory to a crime. Real officers would never say this, because it's not true.



**Never pay in response to  
upsetting news!**

If you get a call from law enforcement threatening you with arrest or demanding you pay or move your money, hang up. It's always a scam.

## **Company imposters**

These scammers pretend to work for a well-known company or bank to try to convince us to pay them. They might, for example, create a pop-up virus warning that directs us to a scammer.

Company imposters create elaborate stories to mislead us. They may say there's a problem with our account and then make up a reason we need to pay to resolve it. For example, they may claim they overpaid our account while trying to fix an error. Then they ask us to pay them back in cash, gift cards or bitcoin.

Sometimes they ask for remote access to our computers and then manipulate our screen so we "see" evidence of a problem that's not real.



## Protect yourself:

- Don't directly respond to calls, texts or emails about account issues. If you want to check, log into your account as usual or call the company using a number you know is real (for example, a phone number printed on your statement).
- Never give strangers remote access to your phone or computer. Banks and companies never need to access customers' devices.
- Never call the number on a pop-up. Turn your computer off for a few minutes to get rid of them.
- Hang up on any request to fix an employee's error by sending cash, gift cards or bitcoin. Only scammers make this kind of request.



***I was scared. They were just telling me to type things in, so I was.***




## Family and friend imposters

Some scams are intended to make us worry that someone we care about needs our help right away. Scammers might call posing as a family member who needs bail money. Or they might pretend to be our minister and email us for a favor that involves buying gift cards or sending money.

It's tricky to navigate friend and family imposter scams, because saying "no" can make us feel like we're letting someone down. But real people who care about us want us to be safe from scams.

Scammers can hack – take over – our friends' or family's emails and social media accounts. So, if we get an urgent request from someone that involves clicking a link or sending money, we need to think of a different way to reply. For example, if they email, we might call them. If they text, we should email.

Why? Because we want to make sure we're communicating with a friend, rather than a hacker posing as one.



**Don't use contact information that comes with an unusual request – that only leads back to scammers.**



# Romance Scams

In these crimes, a scammer using an assumed name and stolen photo typically contacts us through social media. They begin a flirtation designed to get us to send them money – over and over again.

Usually, romance scammers want to get us dreaming about a future together. Eventually, they tell us about a problem they're having and ask to borrow money from us to resolve it.

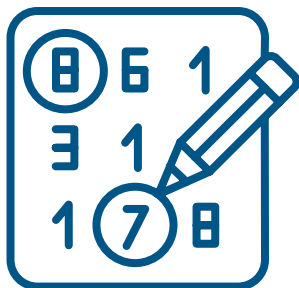
Or, they may say they're rich and can help us get rich too, by making a particular investment.

## **How can we tell if an online flirtation is a scam?**

Real friends who care about us aren't after our money.

Only scammers will ask us to send money or move our savings.

Romance scams are emotionally complicated and can be difficult to get out of. Although the relationship feels real and exclusive, the scammer always targets multiple people at the same time.



## Prize & Grant Scams

Prize scams follow a specific pattern. Someone tells us we won a big prize – like money, a computer or a car – but says we need to pay to collect it.

Legitimate prizes are always free.

- Only scammers will ask you to pay “taxes” or fees up front.
- Only scammers will insist you share your bank account or credit card number to claim a prize.
- Anytime someone tells you to deposit a check and forward money, that check is counterfeit. Banks may temporarily put cash from a deposited check into your account, but if you spend that money and the check turns out to be fake, you’ll owe the bank.

**If you’re asked to  
pay to collect a  
prize, it’s a scam!**

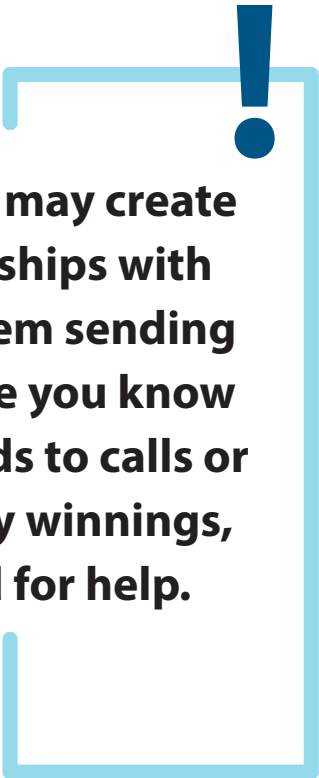


## Government grants

Scammers often use social media to promote fake “government grants.” These scams may ask for payments or give links to spoofed sites that collect personal info.

Federal grants go to entities, not ordinary people. Federal grants are always free, and they’re used to fund research or further policy goals.

Don’t pay anyone who says you won a government grant – not even if they claim to work for a federal agency.



**Lottery scammers may create ongoing relationships with people to keep them sending money. If someone you know frequently responds to calls or texts about lottery winnings, call Scam Squad for help.**



# Identity Theft

Identity theft occurs when criminals use our stolen personal information to access our accounts or to open new accounts in our names.

Signs of ID theft can include finding transactions you didn't make on your statements or getting bills or past-due notices about accounts that you didn't open.

## Protect yourself:

- Ask your bank and credit card company for free alerts so you can spot unauthorized transactions right away.
- Occasionally check your credit reports for errors or unauthorized accounts. Free credit reports are available as often as once a week through **annualcreditreport.com**
- Put a freeze on your credit reports to block thieves from creating accounts in your name. Visit **cuyahogacounty.gov/creditfreeze** to learn more.

If you've experienced identity theft, visit the **Federal Trade Commission's identitytheft.gov** to get a free, do-it-yourself recovery plan.



# Financial Exploitation

Financial exploitation is a growing crime that preys on vulnerable older adults – and it’s committed by someone the person knows. The exploiter steals the person’s money, property or financial identity.

We might suspect financial exploitation if a friend who used to be financially secure suddenly can’t pay bills or complains about new accounts they didn’t open. There may be someone new hanging around who has taken over banking tasks or uses our friend’s credit cards.

If you suspect someone you know is being exploited, call **Cuyahoga County Division of Senior and Adult Services at 216-420-6700.**



# Protect Yourself

## From scam calls and texts

- Let unknown callers go to voicemail. Don't call back hang-up numbers or respond to vague messages.
- If you get a call or text about a problem with an account, log into your account or call the company using a number on your bill. Don't click on links in unexpected emails or texts.
- If a call is upsetting, hang up. Give yourself some time to breathe and think how you can check the information you heard.

## From online scams

- If you're online and get a pop-up ad warning about a computer virus, it's a scam. Do not call the number on the screen. Turn your device off for a few minutes, and the pop-up will go away.
- Prevent pop-up ads altogether by going into the settings for your internet browser (Chrome, Safari, etc.) and toggling pop-up ads "off."



- Do not follow a stranger's instructions to type codes, download apps or allow remote access to your device.
- Avoid clicking on "sponsored" results in internet searches and ads that appear on the edges of your internet browser. These paid ads are not vetted well by social media sites, and scams are common.

## **From social media scams**

- Don't accept duplicate friend requests from people you're already friends with. Scammers sometimes impersonate your friends' accounts to gain access to your contacts.
- Ignore strangers contacting you in the messenger feature, these are likely scammers.
- Consider using the privacy settings on your social media accounts to restrict strangers from viewing your page and friends or followers.

## **From shopping scams**

- Before you buy online from a company you don't know, check reviews for both the company and product. One way to do that is to search for a company or product by name, along with the word "complaint."

## From email scams

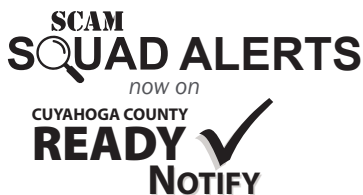
- Ignore arrest warrants, investigation warnings or court summons sent by email. They're not real.
- Know that government and banking emails will never come from free email addresses like Yahoo and Gmail.

Visit **[cuyahogacounty.gov/internetsafety](https://cuyahogacounty.gov/internetsafety)** for tips and tools for staying safe online.



### **Don't Google your way into a scam**

**Don't search the internet for phone numbers for tech companies because results can include scam numbers. Log into your account the way you normally do.**



# Protect Yourself and Your Loved Ones from Scams

Sign up to receive free Scam Squad Alerts by phone, text or email.

When you sign up, you'll get periodic alerts to help you spot and avoid scams.

Scam Squad Alerts are great for people who:

- Receive suspicious offers or robocalls
- Have paid or revealed personal information to a scammer
- Want information on current scam threats

Scam Squad Alerts are delivered through Cuyahoga County's Ready Notify emergency management system.

**To sign up:**

**Call 216-443-5700 or 216-443-7035**

**or**

**Visit [readynotify.us](https://readynotify.us)**

# My Action Plan

This action plan is designed to help you protect yourself from scams. Take time to fill it out now so you'll know what to do when you get a suspicious call, text, email, or letter.

## PAUSE if you're being pressured

- Hang up and give yourself time to think.
- Never trust anyone who tells you to lie or keep secrets.
- Always check with a trusted source before you act.

## List people you trust

List only people you know in person – reliable friends, relatives or neighbors. We've added organizations that can help you quickly identify scams.

Name	Phone Number
Scam Squad	216-443-7226
Sheriff's Department	216-443-6000
My local police	

**List companies you do business with**

Include utilities, banks, phone companies, and online shopping sites. Don't rely on internet searches. Use only verified contact information from bills, receipts, or the back of your bank cards.

Business Name	Phone	Website

**Report scams to Scam Squad**  
**216-443-7226**  
**[cuyahogacounty.gov/scamsquad](https://cuyahogacounty.gov/scamsquad)**



# Report Scams and Get Help

## **Report & recover from scams, talk to an investigator**

Scam Squad

216-443-7226 • [cuyahogacounty.gov/scamsquad](https://cuyahogacounty.gov/scamsquad)

## **Get services for older residents & report financial exploitation**

Cuyahoga County Division of Senior and Adult Services

216-420-6700 • [hhs.cuyahogacounty.gov/dsas](https://hhs.cuyahogacounty.gov/dsas)

## **Report financial losses to cybercrime**

FBI/Internet Crime Complaint Center

[ic3.gov](https://ic3.gov)

## **Report fraud & ID theft**

Federal Trade Commission

1-877-382-4357 • [reportfraud.ftc.gov](https://reportfraud.ftc.gov) • [identitytheft.gov](https://identitytheft.gov)

## **Ask a consumer question, file a complaint about a business**

Cuyahoga County Department of Consumer Affairs

216-443-7035 • [cuyahogacounty.gov/consumeraffairs](https://cuyahogacounty.gov/consumeraffairs)

## **Report mail fraud**

U.S. Postal Inspection Service

1-877-876-2455 • [uspis.gov](https://uspis.gov)

## **File a complaint against a business or a charity**

Ohio Attorney General

800-282-0515 • [ohioattorneygeneral.gov](http://ohioattorneygeneral.gov)

## **Connect with services for older residents**

Western Reserve Area Agency on Aging

216-621-0303 • [areaagingsolutions.org](http://areaagingsolutions.org)

## **Check company and charity ratings**

Better Business Bureau Serving Greater Cleveland

216-241-7678 • [bbb.org/cleveland](http://bbb.org/cleveland) • [bbb.org/scamtracker](http://bbb.org/scamtracker)

## **Get support services for older adults in Cleveland**

Cleveland Department of Aging

216-664-2833 • [clevelandohio.gov/aging](http://clevelandohio.gov/aging)

## **Get information about scams**

AARP

877-908-3360 • [aarp.org/fraudwatchnetwork](http://aarp.org/fraudwatchnetwork)

## **Access financial and other programs for older adults**

Benjamin Rose

216-791-8000 • [benrose.org](http://benrose.org)

## **Get free legal help (low income)**

Legal Aid Society of Cleveland

888-817-3777 • [lasclev.org](http://lasclev.org)

## **Get free legal advice for Ohioans age 60 and older**

Pro Seniors

800-488-6070 • [proseniors.org](http://proseniors.org)



216-443-SCAM (7226)

[cuyahogacounty.gov/scamsquad](http://cuyahogacounty.gov/scamsquad)



Cuyahoga County

**For copies of this booklet, contact:**

Cuyahoga County Department of Consumer Affairs

216-443-7035

[cuyahogacounty.gov/consumeraffairs](http://cuyahogacounty.gov/consumeraffairs)