Consumer Scams

Keeping Ohioans Safe and Informed

Scam artists use a variety of tactics to make their offers seem legitimate. Learn to recognize the signs of a scam to protect yourself and those you care about.

DAVE YOST
OHIO ATTORNEY GENERAL

Look out for scams!

Scammers want your money and personal information. They might contact you by phone, mail, email, text or phony website, or even show up at your door.

Signs of a scam

- You're asked to immediately send payment via cash, gift card, wire transfer or cryptocurrency.
- You're pressured to "act now!"
- You have to pay a fee to receive your "prize."
- Your personal information is requested.
- A large down payment is requested.
- The company refuses to provide any information in writing.
- You're asked to keep conversations a secret.
- You're guaranteed to make money.
- You've won a contest that you've never heard of or entered.

'Phishing' and spoofing

Some scammers "phish" for your personal information using cleverly designed calls, texts or emails. They pretend to be your bank, a trusted website or a government agency, asking you to update or confirm your account by providing your bank account number, password or Social Security number. Never respond to unexpected requests for your personal information, even if the caller appears to have some details about you or your account. Also, be aware that scammers can disguise or "spoof" the number appearing on your caller ID — so that the caller ID shows a local area code even though the call is coming from another country.

Common scams

Here are the scams most frequently reported to the Ohio Attorney General's Office:

Computer repair scams

A “computer company” — either by calling you or sending a pop-up message — claims that your computer has a virus. The scammer offers to fix the problem, then asks for access to your computer. Such access allows the scammer to install malicious software designed to scan your computer for personal information or to lock your computer, making it unusable until you pay a “ransom” to unlock it. Never allow remote access to your computer, and don’t download unfamiliar programs or files.

Credit repair scams

These scams involve false promises that bad credit can be erased, interest rates lowered and debts consolidated. Many of these “companies” charge hundreds or thousands of dollars but do little or nothing to improve your credit. If you want to improve your credit, contact a nonprofit credit-counseling agency or your creditor directly. You may be able to arrange a payment plan yourself — at little to no cost.

Cryptocurrency-related scams

Cryptocurrencies are not government-backed or -regulated and have few, if any, legal protections.

Scammers use techniques to target potential cryptocurrency investors. Some red flags of a cryptocurrency scam:

- The scammer has access to your “digital wallet.” If the scammer sets up or controls your digital wallet or you give the scammer security codes or passwords, the scammer can take and keep all your cryptocurrency.
- You’re told that you’re guaranteed to make money. Never believe any guarantees with investments in general. Also, if you’re asked to recruit other investors in order to make a profit, you may be involved in a Ponzi scheme.
- The crypto is being “given away” by a celebrity or influencer. In reality, the true celebrity isn’t even involved, and victims don’t get a jackpot, award or any other giveaway. Instead, they lose the value of any crypto they invested as part of the supposed promotion.

Cryptocurrency is quickly becoming the currency of choice for scammers. If someone demands payment by crypto or wants you to use a crypto-based ATM, it’s likely a scam.

Fake check scams

With these scams, the scammer typically sends a check as payment for something, perhaps an item you've sold online or to get you started with supplies for a new job. The scammer then asks you to send some of the money back or give it to a third party. However, keep in mind that the "check" has not yet cleared your bank. In reality, the check is fake, so no money will be permanently deposited into your account. However, the money that you've sent back is real, meaning the amount sent will be deducted from your account, often along with a returned-check fee.

Family and caregiver scams

Sadly, financial abuse involving older adults can be at the hands of family members, caregivers and friends. They might use your credit cards without permission, pressure you to sign legal documents or forge your signature. Beware of such behavior and watch for signs of a family or caregiver scam, including unpaid bills, a new "best friend," isolation from other family members or friends, unusual banking activities or missing belongings.

Grandparent scams

With these scams, a con artist poses as a grandchild. The "grandchild" calls with a false story, explaining that he or she is in trouble and needs you to send money immediately. Any money you send goes to the scammer, not a real grandchild. When in doubt, ask the caller a question that only a family member would know about and call your son or daughter to confirm the location of the grandchild.

Home-improvement fraud

Such fraud occurs when contractors or companies do little or none of the work they were paid to do. Door-to-door contractors may offer to repair your roof, pave your driveway or trim your trees for a good price or with leftover supplies from another job in the neighborhood. After you pay, however, the contractor disappears without doing any work or after doing a poor job.

To avoid scams:

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

Identity theft

Identify theft occurs when someone uses your personal information to obtain credit, take out a loan, receive medical treatment or otherwise pretends to be you without your knowledge. Never give personal information to anyone you don't know or trust, especially when solicited by phone. If you are a victim of identity theft, contact the Ohio Attorney General's Office.

Impostor scams

Government impostor: Someone may contact you pretending to be from a government agency such as the IRS or the Social Security Administration or a local court. The person demands payment, likely for back taxes or an old court fee, and threatens to arrest you if payment is not made immediately. The scammer might also request personal information, such as your Social Security number. Refuse to provide the information, and hang up.

Business impostor: Someone may contact you pretending to be from a popular business. The caller may lead you to believe that you have purchased an item that you did not purchase, and instruct you to call or follow a provided link to verify or dispute the purchase.

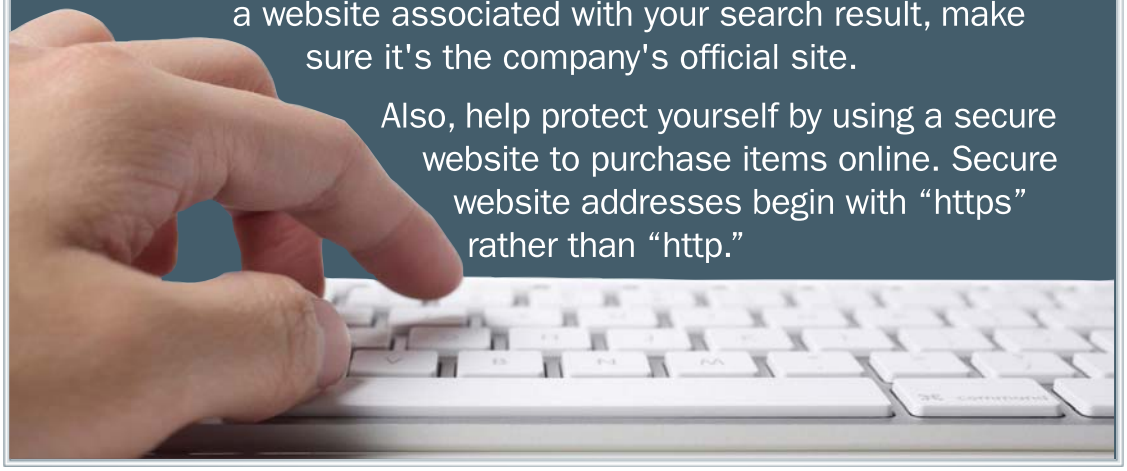
If you're concerned whether a call is real, look up the phone number for the business or agency on the company's or agency's official website and call that number.

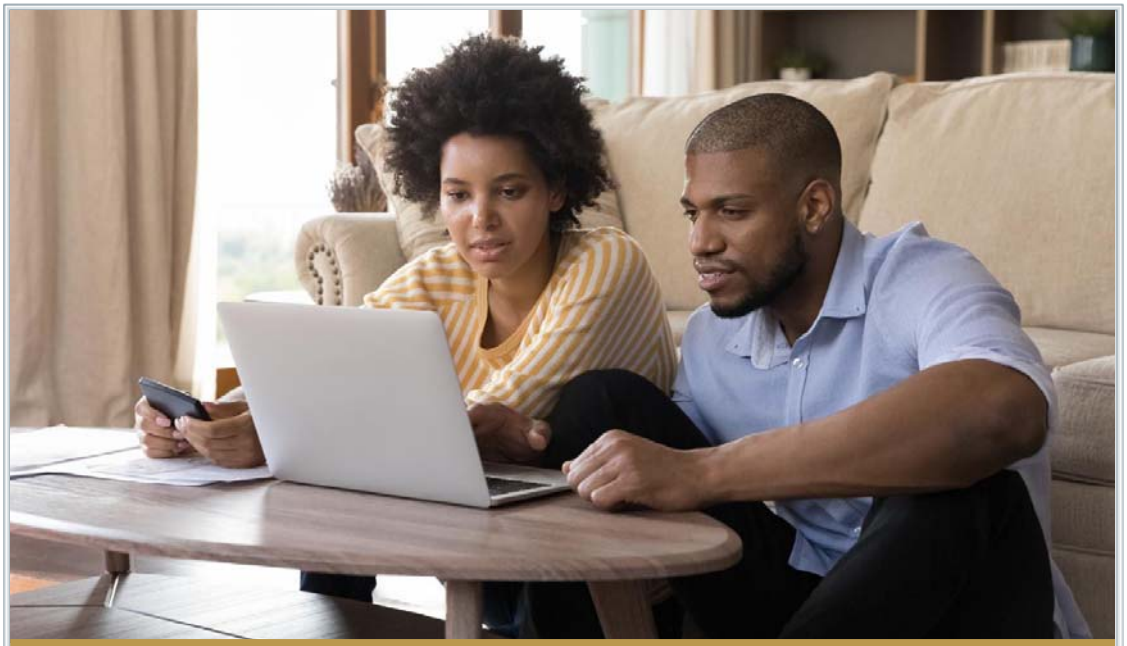
Online shopping scams

When using an online marketplace, verify that an item exists before buying it. If you are selling an item, a buyer might send you a "check" for an amount exceeding the asking price and ask that you return the "difference" or forward it to a "shipping agent." Refuse these checks; they're scams designed to steal your money.

When shopping online, be cautious of sponsored ads, often found at the top of your search engine results. Search engines often list paid results first. You will generally see "ad" or something similar listed to indicate that a result is bought or sponsored. If you see a website associated with your search result, make sure it's the company's official site.

Also, help protect yourself by using a secure website to purchase items online. Secure website addresses begin with "https" rather than "http."





Other common scams

Job opportunity scams: Some scammers ask job seekers to pay high fees for information, training sessions or promotional materials that turn out to be useless. The jobs are either nonexistent or very low-paying. If the job opportunity sounds too good to be true, it probably is. Consider applying for jobs directly through the company's website to ensure the posting is legitimate. Be cautious of work-from-home and mystery shopper jobs, especially when they involve paying for supplies up-front.

Advance-fee loans: Scam artists can trick you into paying money up-front to qualify for a loan or credit card. Despite their guarantees, you do not receive a loan, credit card or any money. Never pay money to qualify for a loan, credit card or grant.

Social media scams: Con artists may hack into others' social media accounts and contact you pretending to be your friend. While using your friend's profile, they may claim that you can receive a large amount of money as long as you pay a processing fee or taxes. Other scammers may impersonate your friend and pretend they are in trouble and urgently need money. Be skeptical of sending money in response to a message from a "friend" when asked via a social media app or website. Contact the friend in a manner other than social media to verify whether that person truly sent you the message or whether the account was compromised.

Phony charities

Such scams involve someone pretending to be a charity and requesting a donation. Always ask how much of your donation would actually go to the charity. Charitable organizations must register with the Ohio Attorney General's Office. Look up the charity at Charitable.OhioAGO.gov/Research-Charities.

Prize/Sweepstakes scams

With these scams, someone might falsely claim that you've won a lottery, prize or contest you never entered. To collect your "winnings," you'll be asked to pay a fee. Often, you'll be instructed to send money via wire transfer or money order, possibly to a foreign country. The scammer will tell you to expect your winnings once you pay, but the prize never arrives.

Be cautious of social-media "friends" or contacts who say that you've won a prize or sweepstakes; such messages probably aren't from your friends.

Romance scams

Someone you meet online or over the phone claims to be temporarily located overseas, perhaps due to a military assignment or mission trip. Your relationship develops over weeks or months, and then the person faces a "hardship" and asks you to send money to pay for airfare, medical costs, military fees or some other expense. In reality, the person is a con artist who is probably pursuing several victims and following a script. There was never "true love." Any money you send will be lost.

Robocalls, unwanted calls and texts

Robocalls are auto-dialed calls that deliver a prerecorded message. Generally, robocalls that you haven't consented to and that are seeking personal information or payment for something are illegal.

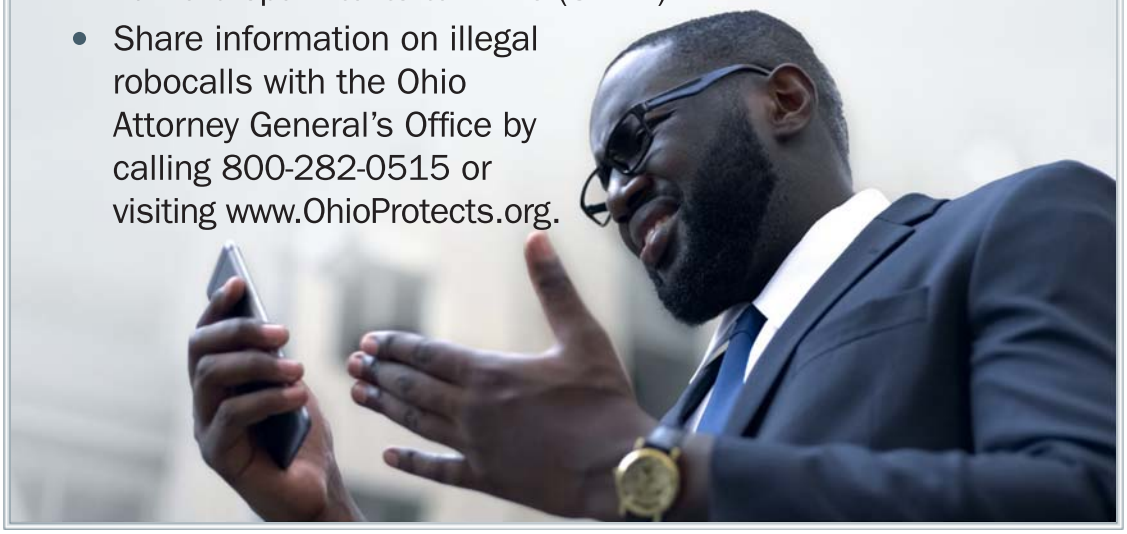
When it comes to numbers you don't recognize the best advice is JUST DON'T ANSWER.

Some tips for dealing with unwanted calls and text messages:

- Register your phone number(s) with the Do Not Call Registry online at www.DoNotCall.gov or by phone at 888-382-1222. Remember: If you're registered and someone calls trying to sell you something, it's a good sign that the company isn't legitimate.
- Research services offered by your phone provider to block unwanted calls.
- Install a reliable app on your cellphone to block or warn of suspicious calls.
- Add trusted phone numbers to your contacts.
- Limit the people and businesses with whom you share your phone number.
- If you don't recognize the number, allow the call to go to voicemail and review the message later. If you answer a robocall, don't interact with an unknown caller in any way; don't press numbers or speak to anyone. Don't call back unfamiliar phone numbers.
- Don't provide personal or financial information over the phone.

Reporting robocalls and unwanted text messages:

- Forward spam texts to 7726 (SPAM).
- Share information on illegal robocalls with the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioProtects.org.



For more information

These trusted resources can help you better protect yourself from consumer fraud.

Fraud and scam resources

Below are state and federal agencies that handle fraud and scam issues.

Federal Trade Commission | Consumer Complaint
877-382-4357 | www.consumer.ftc.gov

Ohio Consumers' Counsel | Utility & Phone Fraud
877-742-5622 | www.occ.ohio.gov

Ohio Department of Commerce | Securities
Investor Protection Hotline: 877-683-7841
www.com.ohio.gov

Ohio Department of Insurance
Fraud & Consumer Services
Medicare OSHIIP Hotline: 800-686-1578
Consumer Hotline: 800-686-1526
www.Insurance.ohio.gov

U.S. Postal Inspection Service | Report Mail Fraud
877-876-2455 | uspis.gov

Identity theft

Ohio Attorney General's Office
www.OhioAttorneyGeneral.gov/IdentityTheft
800-282-0515

Federal Trade Commission
Identitytheft.gov

Request for annual credit report

You're entitled to one free copy of your credit report annually from each of three credit-reporting companies. Make a habit of obtaining these free reports.

www.annualcreditreport.com
877-322-8228

Credit freezes and fraud alerts

An initial fraud alert tells creditors to take extra steps to verify your identity when any new credit account is applied for in your name. The alert is free to place and lasts for one year. A credit freeze, which is permanent, prevents third parties from accessing your credit reports without your permission. There is no charge to place, temporarily lift or remove a credit freeze. To place a fraud alert, contact one of the three credit bureaus listed below; to place a credit freeze on your credit report, contact all three:

- **Equifax:** www.equifax.com; 800-525-6285
- **Experian:** www.experian.com; 888-397-3742
- **TransUnion:** www.transunion.com; 800-680-7289

Legal resources

Pro Seniors is a nonprofit organization that provides free legal assistance to Ohio residents ages 60 and older.
www.proseniors.org
800-488-6070

Legal Aid is dedicated to providing legal counsel — at no cost to the client — to help Ohioans achieve justice.
866-529-6446

Ohio Legal Help "publishes online, self-help legal information and tools to connect Ohioans with local organizations that can help with their legal problems. (Ohio Legal Help) does not provide legal advice or assistance."
www.OhioLegalHelp.org

Mortgage problems

Save the Dream Ohio connects homeowners struggling to make mortgage payments with a federally approved housing-counseling agency or legal assistance.

savethedream.ohiohome.org
888-404-4674

Online safety

It is important to stay safe and secure online. There are many resources that highlight online safety for users of all ages and skill levels.

www.stopthinkconnect.org
www.staysafeonline.org

Researching businesses

You can learn about a business by checking with the Ohio Attorney General's Office and the Better Business Bureau.

www.OhioAttorneyGeneral.gov; 800-282-0515
www.bbb.org

Services for veterans

The Ohio Department of Veterans Services, which advocates for veterans and their families, can also provide resources about benefits.

www.dvs.ohio.gov
877-OHIO VET (877-644-6838)

Unwanted mail

You can reduce the amount of mail you receive from national catalog/marketing companies by registering with the Data and Marketing Association.

www.dmachoice.org
212-768-7277

Limit the pre-approved credit card offers you receive by registering with OptOutPrescreen.com.

www.optoutprescreen.com
888-5OPT-OUT (888-567-8688)

the 5 R's

These five important R's will further help you protect yourself and your wallet:

- **Research** businesses and charities with the Ohio Attorney General's Office and the Better Business Bureau. Ask family and friends for recommendations.
- **Remember** that scammers' preferred payment methods are gift cards, cryptocurrencies, wire transfers and prepaid money cards.
- **Relax**! Don't feel pressured to act immediately, even if someone threatens that you will lose money or be arrested.
- **Report** scams to the Ohio Attorney General's Office at 800-282-0515.
- **Realize** that if it sounds too good to be true, it probably is!

DAVE YOST

OHIO ATTORNEY GENERAL

Ohio Attorney General's
Consumer Protection Section
30 E. Broad St., 14th Floor
Columbus, OH 43215

For more information, to report a scam, or to schedule a speaker on consumer protection issues, contact Ohio Attorney General Dave Yost's office at **www.OhioAttorneyGeneral.gov** or **800-282-0515**.

For TTY, call Relay Ohio at **800-750-0750**.