Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

June 2026

Protect yourself from impostor scams involving 'payment notices'

Impostor scams involve fraudsters pretending to be a trustworthy source – often a government official – to deceive you into sending money or providing personal information. Notably, there has been a recent uptick in impostor scams involving fraudulent court-related notices, which arrive via email, text or phone call.

Among the most common types:

- **Jury duty.** A "court or law enforcement official" claims that you missed jury duty and will be arrested unless you immediately pay an identified fine. Payment is often sought via gift card or

cash deposit. The scammer may invoke the name of a real judge and/or real case details gleaned from public records – an effort to make the scam seem more credible.

- **Warrant/arrest threats.** Claiming that there is a warrant out for your arrest for failing to appear in court, these fraudsters pressure you into "posting bond" via a gift card or money transfer. They often spoof local phone numbers – making it appear as if the call is coming from the area code in which you live – to seem legitimate.
- **Traffic or parking fines.** You might receive a text message or an email alleging an unpaid traffic, toll or parking violation, complete with a fake case number, official seal or QR code. The official-like presentation is designed to trick you into clicking or paying unknowingly.
- **"Zoom court" or other video hearing.** Scammers schedule fake online hearings, sometimes with a "judge" on Zoom demanding immediate payment of a fine. It's important to know that real courts wouldn't make initial contact via a video call to ask for money.
- **Bond for a family member**. People with loved ones in custody may get calls or texts demanding bail or bond money. Scammers impersonate a sheriff's office and tell you to wire money or send cash via a barcode-based system. Some scammers claim that your loved one is eligible to be released and monitored by ankle bracelet. They, too, demand money, but the loved one isn't actually eligible for release.

Tips on identifying these scams:

- Be aware that real communications from courts or law enforcement will never demand payment via gift card, QR code, cryptocurrency or cash transfer.
- Know that legitimate jury duty notices are sent by mail, not by phone, text or email.
- Always verify questionable communications with official sources. Look up numbers or websites independently and never use the contact information provided in the suspicious message.

How to protect yourself against impostor scams:

- Never provide personal or financial information in response to unsolicited contact.
- Independently verify claims using official phone numbers and/or websites.
- Beware of untraceable or unconventional payment methods.
- Hang up on suspicious calls and delete suspicious texts or emails.

If you suspect a scam or an unfair business practice, contact the Attorney General's Office at www.OhioProtects.org or 800-282-0515.

World Elder Abuse Awareness Day prioritizes protection of elders

World Elder Abuse Awareness Day, marked globally on June 15, is designed to raise awareness of the mistreatment, neglect and exploitation experienced by many older adults. The observance reinforces to communities, organizations and governments the importance of protecting the rights and dignity of older adults.

Elder abuse encompasses physical, emotional, financial and/or sexual abuse as well as neglect. Abusers can be caregivers, family members, institutions and/or others.

With age, more adults become vulnerable to mistreatment. World Elder Abuse Awareness Day helps spark conversations, education and policy efforts to help ensure that older adults are safe and supported. Once you know who may be at a higher risk of abuse, the next step is to look for warning signs of exploitation.

Older adults most at risk of abuse may:

- Be socially isolated.
- Rely on family members or friends to handle their finances.
- Have recently lost a spouse or loved one who handled their finances.
- Have cognitive impairment.

Warning signs of fraud or financial exploitation include:

- Unexplained withdrawals or charges, or missing cash.
- Calls regarding unpaid bills.
- Requests to sign over a power of attorney or modify a will.
- Requests to keep conversations or relationships a secret.
- Requests to send money via wire transfer, gift card or prepaid money card.
- Pressure to act immediately.
- Guarantees to make money.
- Attempts to isolate an older adult from family and friends.
- Threats of harm, neglect, abandonment or removal from the home.

In an effort to shine a light on elder abuse, the Ohio Attorney General's Office, through the Elder Justice Unit, has partnered with the Ohio Pharmacists Association, Ohio Bankers League and the Ohio Health Care Association. The initiative educates pharmacists and other professionals about red flags of abuse and neglect, and publicizes the Elder Abuse Hotline (1-855-OHIO-APS).

For assistance, training, or additional information about elder justice issues – or to report suspected abuse, neglect, or financial exploitation, call (800) 282-0515 or visit www.OhioAttorneyGeneral.gov. For additional information on elder abuse, visit the resources provided by the Ohio Attorney General's Office at https://www.ohioattorneygeneral.gov/Individuals-and-Families/Seniors/Elder-Abuse-Resource

---

Securing your mobile devices is crucial

With society's increasing reliance on mobile devices, it is crucial to secure those devices. These practical tips can help you guard against digital threats seeking to expose your personal information and data:

- Use strong, unique passwords or other authentication methods, such as biometrics, to help protect your data. Passwords should be 16 or more characters and contain letters, numbers and special characters. Consider using a password manager that helps design those hard-to-crack passwords, requiring you to remember just one “master password.” Also, be sure to sign out of apps after you use them.
- Use multifactor authentication (MFA) when offered. With MFA, you will be required to enter your password and authenticate your identity through a second method, such as a passcode sent via a text message or email.
- Be cautious when connecting to free public Wi-Fi. Ask the business or facility the name of the official Wi-Fi network and assume everyone can see what you’re doing when connected to it. Do not provide personal information or type in passwords while using an unsecured public Wi-Fi network.
- Install and regularly update reputable apps, anti-virus and anti-spyware programs, and operating systems. If available, opt to have the programs update automatically to ensure effectiveness against new viruses and bugs. Remove apps you no longer use.
- Only use official app stores such as Google Play and Apple’s App Store to download applications. Downloading free apps from unknown sources may lead to malware and put personal information at risk.
- Review apps’ permissions to ensure that you’re not allowing apps to collect data you don’t want to share, such as your location. To review apps’ permissions, look for guidance for iPhone and Android devices. Permissions may be stored in the app, in your device’s settings or both.
- Back up your data, including contacts and photos, in case your device is compromised. Automated backups to a cloud server or another source can save you time and effort; backups are often done overnight, when you aren’t typically using the device.
- If your device is lost or stolen, use resources based on the operating system you use to find, lock and/or erase the contents.
    - Track location: iPhone - Find Devices; Android - Find My Device
    - Lock: iPhone - Lost Mode; for newer Android phones - Remote Lock
    - Erase data: iPhone and Android
- Only recycle or dispose of a mobile device once the hard drive is wiped clean. If needed, take the device to a professional to be sure that all information is deleted before recycling, selling or disposing of the device.

In addition, there have been reports of scam emails and text messages appearing to come from Apple and Google related to accounts. Generally, Apple will not make unsolicited phone calls or send communications to you requesting passwords or other personal information. Google typically contacts customers by email from an @google.com domain or through in-product account alerts. Google never asks for payment or other sensitive information over the phone.

If you suspect a scam or an unfair business practice, contact the Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Ohioans warned about investment scams on social media

The Ohio Attorney General's Office is cautioning Ohioans about the prevalence of fraudulent investment schemes on social media platforms. Scammers are increasingly using deceptive advertisements and "deepfake" technology to lure investors into high-stakes scams to defraud them of their savings.

Be sure to scrutinize investment advertisements before making any decisions. Most reputable broker-dealers and investment advisers do not post investment advice on social media platforms.

- **"Pump and dump" scams**. Victims are lured into investment groups and persuaded to invest in cryptocurrencies or low-priced stocks. The scammers advertise, hype and recommend the stock or cryptocurrency purchases, then sell when the price is high – and the victims lose their money. Scam ads often appear on social media featuring recognizable figures but without their permission. The ads often promise exclusive "insider" memberships or "guaranteed" high-return investment tips.
- **Confidence scams** Fraudsters develop trusting relationships with their victims and persuade them to "invest" using fake investment platforms that drain the victims' money.

  Scammers generally post ads suggesting that investors can make money using an investment platform or strategy. The scammers may offer to "teach" the user how to trade on a fake investing platform or even connect the victim with their own personal adviser, who speaks with the user daily. The scammers then guide their victims to a professional-looking website or app, which is often a clone of a real trading platform.

  Once the victims seek to withdraw their profits, they are told they need to pay a commission, tax or other type of fee. Even when victims pay, the scammers give other excuses not to return the money. Once the victim stops paying the fees or making additional investments, the scammers disappear – along with the victim's investment.

Ohioans should stay vigilant and learn to identify the following red flags:

- **Promises of guaranteed returns**. No legitimate investment is risk-free or offers a guaranteed return.
- **High-pressure tactics**. Scammers often suggest that you will "miss out" if you don't invest immediately.
- **Celebrity endorsements**. Scammers often use AI-generated images or videos of famous entrepreneurs to lure victims.
- **Currency demands**. Requests to use hyper-specific payments – such as gift cards, peer-to-peer payment or crypto – should be regarded with suspicion.
- **Requests to accept other people's money.** Scammers sometimes ask victims to accept other people's funds in their bank accounts and convert them to cryptocurrency.

- **Platform hopping.** Scammers may rask to move the conversation from Facebook to encrypted apps, such as WhatsApp or Telegram.

Before investing, be sure to conduct some independent research:

- **Verify credentials**. Use FINRA's BrokerCheck to confirm whether a professional is registered. Be aware, though, that scams often impersonate people or firms and their credentials.
- **Search for online reviews**. Search the company name and/or salesperson alongside words such as "scam" or "complaint."
- **Check email addresses**. Verify that the email you're communicating with is that of a real adviser associated with a legitimate company. Remember that scammers may register email addresses that are very similar to a legitimate domain, perhaps changing only one letter.
- **Look for spelling errors**. Given that many scams originate overseas, ads and other communications may contain spelling mistakes.
- **Consult with a trusted adviser.** If your bank or investment/financial adviser cautions you about your new investment, don't dismiss those concerns. Further investigate the new "investment opportunity."
- **Trust your instincts and think twice before investing**: If an investment seems fishy or too good to be true, it probably is.

To protect your identity and network:

- **Lock down your profile**. Change your settings to keep your friends lists, photos, and posts private. This prevents scammers from learning specific information about you as well as your friends.
- **Verify friends**. If a friend suddenly messages you about a "great investment opportunity," contact that person outside of social media (via phone call or text) to ensure that his or her account hasn't been hacked.
- **Never share credentials**. Do not provide login information, a Social Security number or financial details to anyone you meet online.
- **Do not provide strangers with access to your devices.** Do not allow anyone you do not know to access your computer or mobile phone remotely. Oftentimes, scammers pose as a representative of a company with which you have an account and ask for a password or answers to security questions. Within seconds, they are able to empty everything in the accessed account.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.