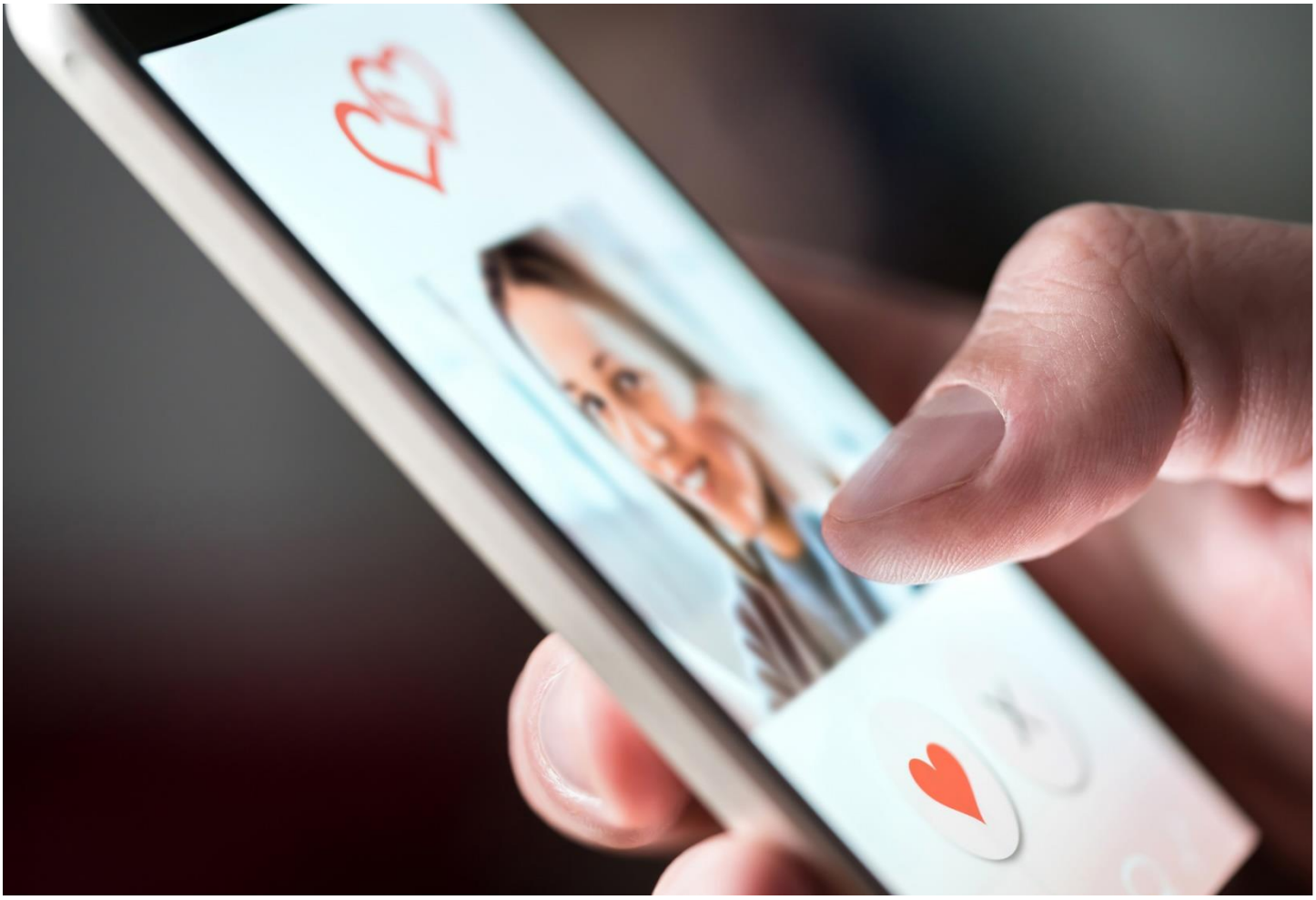
Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

February 2023



Beware of romance scams this Valentine's Day

If Valentine's Day has you motivated to meet someone special, be careful of con artists looking to take advantage of others.

It's important to protect your heart and your hard-earned money by watching for "sweetheart" – or online romance – scams.

Sweetheart scams typically originate with a phony profile on a dating website or social media as way

of attracting unsuspecting victims.

Many of these scammers claim to be in another state or country, often pretending to be a military member stationed overseas or a businessperson working outside the United States. They might even send fake photos or documentation to “prove” their identity.

Scammers might spend many hours communicating with a victim before asking for money. Or they might request money for airfare to visit, to pay a hospital bill, to get out of a foreign country or to access an inheritance that the scammers promise to share with their victims.

Victims are usually asked to send money via gift card, wire-transfer service, money order, prepaid card or other hard-to-trace payment method. Once the money is sent, it is nearly impossible to recover.

After receiving the money, scammers do one of two things: create a new emergency and ask for more money, or stop corresponding, leaving the victim duped and broken-hearted.

In 2022, 35 Ohioans reported sweetheart scams to the Attorney General’s Office with losses totaling almost $1.8 million.

In one instance, a Muskingum County woman sent $15,000 to a man she met on social media who pretended to be a member of the military in need of an emergency medical procedure. The scam was detected when the woman contacted the Army Investigative Unit and was informed that no such person existed.

In another sweetheart scam, a Mercer County man refinanced loans and sold property in order to send $200,000 to a woman he met on social media – money he never recovered.

Victims of sweetheart scams don’t fit a pattern; they may be male or female, young or old. The common denominator is that they believe in love and believe the romance is legitimate.

Here are some ways to avoid sweetheart scams:

- Research people you meet online; do not rely solely on what they tell you. Conduct internet searches, including reverse-image searches, and check with independent sources to verify a person’s claims. To do a reverse-image search, copy and paste the picture of the person you have been corresponding with into a search engine to see whether it is used on multiple accounts.
- Be cautious of “love bombing,” which occurs when a new love interest showers you with affection and compliments. Be cautious of individuals who claim that destiny or fate brought you together, or claim to love you after a short time.
- Be especially wary if you have just lost a loved one; many times, scammers study obituaries to find people who have recently suffered a loss.
- Talk to friends and family members about online relationships, even if the other person asks you to keep the relationship secret.

- Don’t send money to someone you have met only online, even if you have developed a relationship with the individual.
- Be very skeptical of requests for money to be sent via wire transfer, cryptocurrency, peer-to-peer payment systems, money order, prepaid money cards or gift cards. These are preferred payment methods for scammers.

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

Tips can help protect your online privacy

The Ohio Attorney General’s Office recognized Data Privacy Week last month (January 22-28, 2023). In an effort to help Ohioans protect their personal information, the office is reprinting below an edited version of an article published by the National Cybersecurity Alliance.

In today’s online world, it is more important than ever to protect your personal information from those who would use it to commit identity theft.

That is precisely why the Ohio Attorney General’s Office joined organizations across the nation last month to commemorate Data Privacy Week (Jan. 22-28). This year’s theme was “Data: The Story of You.”

No matter how careful you are, some data is likely generated from your online activities. Businesses and organizations collect data on many of your purchases, interests and behaviors through various apps and websites. So it’s vital to properly manage your data privacy to keep your personal information out of the wrong hands.

The National Cybersecurity Alliance provides three broad tips to help protect your privacy:

1) **Know the trade-off between privacy and convenience.** When you download an app, you’re often asked to approve permissions for the app to access information such as contacts, photos, camera, geographic location and more.

   Before you agree to grant an app any permissions to access your data, make an informed decision about whether the service being offered by the app is worth the data you are about to share. The National Cybersecurity Alliance suggests you ask the following questions:

   - Is the service, app or game worth the amount or type of personal data wanted in return?
   - Can I control my data privacy and still use the service?
   - Is the data requested even relevant for the app or service? (*Why does a Solitaire game need to know all my contacts?*)
   - If I haven’t used an app, service or account in several months, is it worth keeping knowing it might be collecting and sharing my data?

2) **Adjust settings to your comfort level**. It is important to review the security and privacy settings of each of your apps (typically found in Settings or similarly labeled section). Adjust settings to a level you are comfortable with for sharing. If you're not sure, it is best to choose to share less data rather than more.

   While it may seem overwhelming to adjust the settings of all your apps, you don't need to do them all in one sitting. You may also visit the Managing Your Privacy Settings page directly from the National Cybersecurity Alliance for links and guidance from dozens of commonly used apps.

3) **Protect your data.** As stated by the National Cybersecurity Alliance, "data privacy and data security go hand-in-hand." The organization recommends these "Core 4" cybersecurity tips:

   - Create long (at least 12 characters), unique passwords for each account and device. Use a password manager to store each password – maintaining dozens of passwords securely is now easier than ever.
   - Turn on multifactor authentication (MFA) wherever it is permitted. This keeps your data safe even if your password is compromised. MFA generally requires something you know (for example, a password) and something you have (a cellphone to receive a special code or an email address).
   - Turn on automatic device, software and browser updates, or make sure you install updates as soon as they are available.
   - Learn how to identify phishing messages, which can be sent as emails, texts or direct messages.

For more information about the National Cybersecurity Alliance, visit its website at www.staysafeonline.org. For cybersecurity tips from the Ohio Attorney General's Consumer Protection Section, click here.

Choice in tax preparer requires care

You should have received all of your 2022 tax documentation – including W2 forms – from your employer by now, and perhaps you're planning to hire a professional tax preparer.

First, consider what type of professional you may need. Tax preparers might be certified public accountants (CPAs), enrolled agents and/or attorneys. An enrolled agent is a person who has earned the privilege of representing taxpayers before the Internal Revenue Service (IRS). Enrolled agents, like attorneys and CPAs, are generally unrestricted as to which taxpayers they can represent, what types of tax matters they can handle and where they can practice.

It is important to thoroughly research the person preparing your taxes, as the preparer will have access to your personal information, including your Social Security number. No matter who prepares your taxes, ultimately you, the taxpayer, are responsible for the accuracy of your return.

The IRS recommends the following steps when selecting a tax preparer:

1. **Check the preparer's qualifications.** Use the IRS Directory of Federal Tax Return Preparers with Credentials and Select Qualifications. This tool helps taxpayers find a tax return preparer with specific qualifications. The directory is a searchable and sortable listing of preparers. Remember: Any tax preparer should have a Preparer Tax Identification Number.
2. **Check the preparer's history.** Check for disciplinary actions and the license status for credentialed preparers. For CPAs, check with the State Board of Accountancy. For attorneys, check with the Supreme Court of Ohio. For enrolled agents, go to the verify enrolled agent status page on IRS.gov or check the directory.
3. **Ask about service fees.** Avoid preparers who base fees on a percentage of the refund or who boast bigger refunds than their competition. When asking about a preparer's services and fees, don't give them tax documents, Social Security numbers or other information until you've actually retained that person.
4. **Ask to e-file.** The quickest way to get your refund is to electronically file your federal tax return and use direct deposit.
5. **Make sure the preparer is available.** Contact your tax preparer as early as possible to make sure he or she has time to file your taxes before this year's deadline. Be wary of tax preparers offering inexpensive last-minute services.
6. **Provide records and receipts.** Good preparers will ask to see your records and receipts. They'll ask questions to figure things such as total income, tax deductions and credits.
7. **Never sign a blank return.** Don't use a tax preparer who asks you to sign a blank tax form.
8. **Review before signing.** Before signing a tax return, review it. Ask questions if something is unclear. You should feel comfortable with the accuracy of your return before you sign it. You should also make sure that your refund goes directly to you – not to the preparer's bank account. Review the routing and bank account number on the completed return. The preparer should give you a copy of the completed tax return.
9. **Ensure the preparer signs and includes the PTIN.** All paid tax preparers must have a Preparer Tax Identification Number. By law, paid preparers must sign returns and include their PTIN.
10. **Report abusive tax preparers to the IRS**. Most tax preparers are honest and provide great service to their clients. However, some preparers are dishonest. Report abusive tax preparers and suspected tax fraud to the IRS. Use Form 14157, Complaint: Tax Return Preparer. If you suspect a tax preparer filed or changed your tax return without your consent, file Form 14157-A, Return Preparer Fraud or Misconduct Affidavit.

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

'Consumer Protection Up Close

This occasional column examines and explains cases filed by the Consumer Protection Section of the Ohio Attorney General's Office.

In November 2022, Ohio Attorney General Dave Yost sued a central Ohio contractor and his partners for allegedly swindling more than $130,000 from homeowners who made payments for decks that were never built.

The ringleader, Daryl Allen, was previously sued by the Attorney General's Office for shoddy home-improvement work and was prohibited from doing business. To get around that, the lawsuit says, Allen teamed with two men who registered new deck-building companies with the Ohio Secretary of State.

Allen, Bernard Crist and Shane Bates, all defendants in the lawsuit, offered deck-building services through Good News Builders and Columbus Deck Co. LLC.

The lawsuit stems from 12 unresolved complaints in central Ohio – one against Columbus Deck Co. and 11 against Good News Builders – submitted to Yost's Consumer Protection Section and the Better Business Bureau (BBB). In those complaints, consumers detailed financial losses totaling more than $132,000.

Allen, Crist and Bates are accused of violating the Ohio Consumer Sales Practices Act by accepting money from consumers and failing to deliver the promised goods and services, or performing shoddy work and failing to correct it. In one instance, no work was done.

Likewise, the defendants also are accused of violating the Ohio Home Solicitations Sales Act by failing to provide consumers with proper notice of the three-day right to cancel the contract.

The state's filing seeks an order requiring the defendants to reimburse customers and pay civil penalties and court costs. It also requests an order preventing the defendants from engaging in business as a supplier in any consumer transactions in Ohio until those debts are paid.

Consumers should take the following steps before signing a contract for home-improvement services:

- Check with the Attorney General's Office and BBB for any complaints against the contractor.
- Make sure your contract includes notice of your right to cancel a door-to-door sale. Contractors generally cannot start working until the three-day "cooling-off" period ends.
- Get written estimates from several contractors before making a final decision.
- Check to make sure that the written contract includes any oral promises made by the contractor; the project start and end dates; and an itemized list of all significant costs, labor and services.
- Be wary if the contract requires a large down payment or requires you to write a check directly to the contractor instead of his or her company.
- Check with the Ohio Secretary of State's Office to confirm that the business is registered properly.

If you suspect unfair business practices, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

‘SPOTLIGHT’ series

Economic Crimes Unit

The Consumer Protection Section’s Economic Crimes Unit assists local law enforcement and prosecutors in identifying, investigating and prosecuting consumer fraud of a criminal nature. The division consists of two attorneys and four investigators dedicated solely to criminal investigations.

In the past two years, the unit opened 765 criminal investigative matters. Working with local law enforcement and prosecutors, the unit logged more than $588,000 in consumer restitution orders.