

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



February 2022

JANUARY 24 - 28 IS

**DATA  
PRIVACY  
WEEK**

LEARN MORE  
[staysafeonline.org/data-privacy-week](https://staysafeonline.org/data-privacy-week)

Data Privacy Week

## How to Take Back Control of Your Data

*The Ohio Attorney General's Office recognized Data Privacy Week last month (January 24-28, 2022). 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.*

From social media to online shopping, our lives and the digital world become more and more intertwined. Yes, the digital world provides convenience, but it's important to know how to protect personal data to ensure that it's being used the right way by the right people.

In the latest consumer privacy survey from technology manufacturer Cisco, 86% of individuals say they care about their data privacy. That said, even the most savvy digital users can have trouble managing their data.

Here are a few steps to better manage your personal information and make informed decisions regarding your data and how it is used.

### **Understand the privacy/convenience tradeoff**

Many apps, even before you use their services, ask for access to your geographic location, contacts list, photo album and other personal information. This data has tremendous value to businesses, allowing some to even offer you their services at little to no cost.

Consumers should decide whether or not to share their data by weighing the amount of personal information being sought against the benefits they might yield in return. Be thoughtful about who gets your personal information and wary of apps or services that require access to information that is not required or relevant for the services they're offering.

### **Manage your privacy**

Once you have decided to use an app or set up a new account, check the privacy and security settings on the app or website and set them to your comfort level for information sharing. Each device, app or browser may have different features to limit how and with whom you share information.

That said, with so many settings to manage, it can be very challenging to stay on top of them all. Here are some important ones to focus on first:

- **Location data:** In order to provide more relevant results, many apps ask you to share your location data. Make sure you that share this information only with apps you trust and that the apps are using your data responsibly. Also, pay attention to when the app uses your location information. Many apps give you a choice to always keep your location information on, never have it on or have it on only when using the app.
- **Contacts data:** Many email apps and video-conferencing apps allow individuals to automatically sync their existing contacts with their services. Again, be sure that you share this data only with trusted sources, as the data you're choosing to share may belong to others.
- **Camera and photo data:** Social media apps universally ask for access to an individual's photo library and related camera data – which, of course, contains troves of private information. Share it with only the most trusted sources, and, through the settings, control the photos to which those apps have access.

A couple of other suggestions: Be sure to delete unused apps on your devices and keep all apps secure by performing updates.

For additional guidance on personal data, consult the National Cybersecurity Alliance's [Manage Your Privacy Settings page](#).

For more information about the National Cybersecurity Alliance, visit its website at [www.staysafeonline.org](http://www.staysafeonline.org). For cybersecurity tips from the Ohio Attorney General's Consumer Protection Section, click [here](#).

---

## **Most Common Complaints of 2021**

The Ohio Attorney General's Office works every day to protect families from unfair and deceptive business practices and scams. The office accepts and handles complaints to assist consumers and businesses in reaching a mutual agreement to resolve issues. In 2021, the office received more than 20,500 complaints.

The Consumer Protection Section tracks complaints in several general categories for reporting purposes. In 2021, the categories generating the most complaints were:

1. Motor vehicles
2. Shopping, food or beverages
3. Professional services
4. Home or property improvement
5. Collections, credit reporting or financial services
6. Utilities, phone, internet or TV services

Consumer complaints are typically handled by specialists using an informal dispute-resolution process. A complaint specialist attempts to resolve the dispute by working with the consumer and the business. Complaint resolution might involve, for example, a refund for the consumer or an adjustment of charges or services.

Complaint specialists are trained to identify problems. If there appears to be a consistent pattern of deceptive behavior, the office may investigate further and possibly take legal action against the business on behalf of all Ohioans. This legal action can be taken in order to stop current bad conduct, prevent future misconduct, or obtain restitution or civil penalties. In addition to helping individual consumers, in 2021 the office continued to take complaints from small businesses and nonprofit organizations.

### **AG Yost's Consumer Protection Wins in 2021:**

- The Civil Investigative Unit opened 146 cases, and the Civil Legal Unit filed 42 lawsuits, obtaining more than \$37 million in judgments.
- The Economic Crimes Unit continued to identify, investigate and prosecute scam artists, opening 393 criminal investigative matters. Working with local law enforcement and county prosecutors, the unit filed four indictments and obtained three convictions. These cases resulted in more than \$465,000 in consumer restitution orders.

- The Elder Justice Unit continued to provide leadership and advocacy to combat elder abuse and exploitation throughout the state by aiding in investigations, forensic analysis, case presentation and prosecution, victim advocacy and assistance, and training and technical assistance. The unit conducted 45 trainings and presentations, reaching 3,469 attendees.
- The Robocall Enforcement Unit encourages Ohioans to not answer or reply to phone numbers they do not recognize. Using a complaint process designed specifically to empower Ohioans to report illegal robocalls, the unit analyzes complaint data to try stop illegal and unwanted calls and texts. The unit received more than 23,000 unwanted call reports in 2021. AG Yost's dedication to combatting robocalls was aided with the passage of Senate Bill 54, which provides additional tools to allow the attorney general to prosecute the use of illegal robocalls with the intent to defraud, cause harm, or wrongfully obtain anything of value.

### **Tools for Consumers:**

Consumers can also turn to the Ohio Attorney General's Consumer Protection Section to:

- Research a business by searching for consumer complaints as well as lawsuits filed and judgments obtained by the Ohio Attorney General's Office.
- Help obtain assistance to rectify the effects of identity theft.
- Request a presentation (virtual or in-person) about consumer scams, identity theft, smart shopping tips and cybersecurity.
- Receive publications about consumer protection issues.

Click [here](#) to learn more or to access the Consumer Protection Section's free services.

Consumers who believe they have been treated unfairly or been the victim of identity theft should contact the Attorney General's Office at 800-282-0515 or visit [www.OhioProtects.org](http://www.OhioProtects.org).

---

## **Beware of Romance Scams This Valentine's Day**

Valentine's Day is right around the corner, and for many the day serves as a reminder that they are single. That, in turn, can provide motivation for some people to seek out that special someone – and con artists know it.

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

Romance scams typically originate with a phony profile on a dating website or social media as way of attracting unsuspecting victims.

Many con artists claim to be in another state or country, pretending to be a military member stationed overseas or a businessperson working in another country. 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, pay a hospital bill, get out of a foreign country or access an inheritance that the scammers promise to share with their victims.

Victims generally are asked to send money using a 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.

In 2021, 41 Ohioans reported to the Attorney General's Office sweetheart scam losses totaling almost \$1.7 million.

In one instance, a Ravenna man sent upward of \$300,000 to a woman he met on the internet over the course of seven years via Western Union transfer, MoneyGram, cash in the mail, gift cards, and Bitcoin. She has asked him for money for a new car, plane tickets and new homes.

In another romance scam, a Franklin County woman was scammed out of \$5,000. The initial contact was made through an online Scrabble game with a social component. The criminals asked her to buy gift cards from Google Play, Apple, eBay and other companies.

Victims of such scams fit no 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 someone you meet online; do not rely solely on what that person tells you. Conduct internet searches, including reverse image searches, and check with independent sources to verify the person's claims.
- Be cautious of love bombing. Love bombing is a manipulation tactic done by showering a new love interest with affection and/or 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 scour through obituaries to find people who have recently suffered a loss.
- Talk to friends and family members about any online relationships, even if the other person asks you to keep the relationship a 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 sent via wire transfer, Bitcoin, peer-to-peer payment systems, money order, prepaid money cards or gift cards. These are preferred payment methods for scammers.

Consumers who suspect a scam or an unfair business practice should contact the Attorney General's Office at [www.OhioProtects.org](http://www.OhioProtects.org) or 800-282-0515.

---

## Business Impersonation Scams Are on the Rise

Consumers choose to work with businesses they trust, but that trust can be wiped out in an instant by an impersonation scam. Fraudsters know that consumers are more likely to click on a link that appears to come from a trusted business.

In some instances, the scammer impersonates a popular online business with which many people have accounts. The scammer might call, text or send an email to confirm a purchase that the scammer knows the consumer did not make. After the consumer says that he or she did not make the purchase, the scammer asks the consumer for his/her banking information to initiate the refund process. Instead of refunding money, however, the scammer takes money from the consumer's account.

Here are some ways to avoid a business impersonation scam:

- **Check your accounts first before clicking on a link.** If you receive an unusual text or email claiming to be from a trusted business, do not click on the link in the message. Check your accounts through verified websites or phone numbers to make sure that the accounts are intact and that you have not purchased any unwanted items. Something to look for: Many times a fake link contains a slight misspelling or differs slightly in other ways from the legitimate website.
- **Never call back an unknown number.** Use the information on the company website and not a number listed in an unexpected email or text.
- **Don't pay a stranger with a gift card.** If anyone asks you to pay with a gift card, it's likely a scam.
- **Don't give remote access to someone who contacts you unexpectedly.** The contact might claim to be from a government office, computer repair company or popular online store. Remote access to your computer or other electronic devices gives scammers easy access to your personal and financial information, such as bank account information.

Also, keep in mind that "phishing" emails and "smishing" texts are commonplace. These are communications typically meant to trick the consumer into clicking on links in a message so the sender can steal personal information and/or money.

For example, you may receive an email or text message instructing you to click on a link to confirm your account information. The message will likely include a threat that you must do this within a limited period of time or your account will be suspended. By entering your username and password on a fake account, the scammer can then steal your personal information to gain access to your account.

If you get an unwanted email or text messages claiming to be a business, there are four ways to report it:

- Report it on the messaging app you use. Look for the option to report junk or spam.
- Copy the message and forward it to 7726 (SPAM).

- Report it to the Federal Trade Commission at [ReportFraud.ftc.gov](https://www.ftc.gov/whistleblower).
- Report it to the Ohio Attorney General's Office at [www.OhioProtects.org](https://www.OhioProtects.org).

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

---

## Consumer Conferences

- Protecting older Ohioans is everyone's business, so consider joining Attorney General Dave Yost's Elder Abuse Commission on Feb. 23 when it presents the 2022 Protecting Older Ohioans Forum: Responding to Financial Exploitation, Scams and Fraud in Facility Settings. This event is free but requires registration [here](#).
- Registration is also open for the 21<sup>st</sup> Annual Emerging Trends in Fraud Investigation and Prevention Conference. This event will be held both in person and virtually on May 16-17, 2022. Click [here](#) for additional details, including the agenda and speaker bios.