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

December 2025

Data Privacy Week: An ideal time to review your data status

Data Privacy Week is a global initiative led by the National Cybersecurity Alliance to raise awareness of the importance of protecting personal information online. This year's theme – "Take Control of Your Data" – encourages consumers to manage their digital footprint in meaningful ways.

Before sharing or granting access to your data, keep in mind that:

- **Your data is valuable.**

Every click, search, and purchase creates a digital trail. This data is often collected by apps, websites and devices – and can be sold or used to profile and profit from you.

- **You have rights.**
  Even if you can't control every piece of data collected, you do have the right to privacy. It's essential to both understand and exercise these rights.

To protect the personal data you share:

- **Adjust privacy settings on apps and devices**.
  Most apps and devices have default settings that may allow more data sharing than you would prefer. Take time to review and customize these settings to limit access to your location, contacts, camera, microphone, and other sensitive data. This helps reduce unnecessary exposure of personal information.
- **Regularly review permissions for apps and services**.
  Over time, apps may accumulate permissions that are no longer necessary. Periodically check which apps have access to your data, and revoke permissions that seem excessive or dated. This minimizes the risk of data misuse.
- **Be cautious about what you share online**.
  Think twice before posting personal details such as your full birth date, address, or travel plans on social media or public forums. Cybercriminals can use this information to guess passwords, answer security questions, or even impersonate you.
- **Update passwords**.
  Changing your passwords periodically – especially for banking, email, health-care, and other sensitive accounts – helps protect against long-term breaches. If a company you use experiences a data breach, an immediate password change can prevent further damage.

Data is constantly being collected on everything from smartwatches to social media. Even seemingly harmless information – your favorite coffee shop, sports team, or university, for example – can be used to infer personal information. Data Privacy Week serves as a reminder that you deserve a say in how your data is used.

To keep your personal information private:

- **Review app and device settings**.
  - Set and review privacy settings on your device. This usually can be done in your user settings.
  - Check each app's permissions (location, camera, microphone, etc.).
  - Disable unnecessary tracking features.
  - Close apps when done using them.

- **Manage your online presence**.
    - Review privacy settings on social media.
    - Remove old or unused accounts.
    - Think before you share personal information online.
- **Clean up your digital footprint.**
    - Clear browser cookies and history regularly.
    - Use private browsing or tracker-blocking tools.
    - Unsubscribe from unwanted emails and services.
- **Stay informed.**
    - Learn about your data rights (www.staysafeonline.org).
    - Read privacy policies before accepting terms.
    - Follow trusted sources for cybersecurity tips.

How best to protect your children from identity theft?

To help prevent child identity theft, the Ohio Attorney General's Office urges parents and guardians to proactively place a security freeze on the child's credit report.

Child identity theft happens when someone uses a child's identity to open accounts or receive benefits. The impostor may be a family member, friend or stranger, and may use the child's name and Social Security number to open new accounts for cellphones, utilities, credit cards, and even mortgages.

According to the 2024 Child & Family Cybersecurity Study by Javelin Research, one in eight children have had their identity compromised since 2019, reinforcing children's vulnerability to fraud.

Children in foster care face a higher risk of identity theft, primarily because they relocate often and more people have access to their personal information. In fact, federal law mandates that child-welfare agencies annually review credit reports for foster youth ages 14 or older to spot identity theft.

Because children rarely check their credit, thieves can misuse a child's identity for years. Often, the problem isn't discovered until the child later applies for a student loan, car loan or job.

Red flags of child identity theft:

- Any information on a child's credit reports. A possible exception: If a parent has approved a child as an authorized user of a credit card.
- Suspicious mail addressed to a child, such as a preapproved credit card offer or a bill normally linked to an adult.
- Calls or mail linking a debt to the child.
- Correspondence directed to your child from the IRS, such as unpaid income taxes or information indicating that your child is listed on someone else's tax return.

How to place a child security freeze:

This video explains how a parent or guardian can ask the three major credit-reporting agencies to create and freeze a credit record in the child's name. Because most children do not have established credit, the credit-reporting agency will need to create a credit record and simultaneously freeze it. The freeze restricts the credit reporting agencies from releasing information about the child, making it more difficult for an impostor to use the child's personal information to be approved for credit, loans, or services.

To place a child security freeze, a parent should contact each of the credit-reporting agencies: Equifax, Experian, and TransUnion. The parent must provide proof of authority to act on behalf of the child, such as a birth certificate, and proof of identity for both the child and the adult.

Placing or lifting a security freeze is free. Once in place, the freeze remains in effect unless it is lifted by the parent or by the child after the child turns 16.

If you suspect that your child's identity has been stolen:

- Review copies of the child's credit reports. Normally, you will receive an indication that no credit report exists for the child. If you do receive a report, it shows what kind of accounts have been opened and additional information about the fraudulent activity.
- Contact the fraud department of the companies where the fraud occurred to report the activity and get the accounts closed properly.
- Report the fraud to the three major credit-reporting.
- Initiate a credit freeze on behalf of your child with all three of the bureaus.

Victims of identity theft of any age should contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioProtects.org for assistance. The office will work with the creditor, collectors, and the credit-reporting agencies to try to rectify the effects of the identity theft.

Those wishing to rectify the effects of child identity theft on their own should visit the FTC's IdentityTheft.gov website to create a recovery plan.

Smart holiday shopping is the best kind

Have you started shopping for the holidays yet? To avoid scams and maximize your money, the Ohio Attorney General's Office shares the following tips for smart holiday shopping:

- **Buy from trusted businesses.** You can check a store's reputation by researching its complaint history at the Ohio Attorney General's Office and/or the Better Business Bureau. Also, use the internet to look up consumer reviews by searching for the company's name and terms such as "complaint," "scam," or "review."
- **Only purchase from secure websites**. Check the beginning of the website address for the lock symbol and the "s" in "https," which tell you that the website is secure. Also, be sure the website you're buying from is the actual website, not an impostor site.
- **Don't use free, public Wi-Fi when entering sensitive information**. Hackers may be able to monitor your activity – such as inputting your credit card number – when you're using free Wi-Fi networks.
- **Limit what you share.** Only provide a seller with as much personal information as necessary. Also, familiarize yourself with a store's privacy policy, so you know how your information will be stored, sold, and shared.
- **If possible, pay with a credit card.** Credit-card purchases usually offer greater protections from unauthorized charges than other payment methods. With a credit card, your responsibility for unauthorized charges is generally limited to $50. You also have certain rights to dispute charges that you may not have with a debit card or other payment form.
- **Gift cards are popular holiday presents**. Gift cards are great for last-minute shoppers and for recipients who don't have a wish list. You can learn more here about what to consider when buying gift cards. Do not buy a gift card whose PIN number is exposed or packaging is tampered with.

- **Check refund policies.** Under Ohio consumer-protection laws, stores are not required to provide refunds or have a specific type of return policy. If they do have a return policy, however, they must clearly tell you what it is before you complete the purchase. Check a website's refund policy before making a purchase. If a website has a refund policy, it must be clearly and conspicuously posted.
- **Understand the role of third-party sellers.** Keep in mind that some websites, including Amazon and Walmart, have marketplaces that allow third-party companies to sell products through their website. In these cases, the third-party seller's return policy may vary from the website's policy. For example, even if you buy something from a website with a defined return policy, the actual seller may have a different return policy.
- **Beware of phony postal and delivery emails and text messages.** Fake shipping notifications are especially popular during the holiday season. Typically, the message offers an urgent update about your package, such as a shipping delay and directs you to click a link for more information. If you click the included link, you are taken to a malicious website. Here are some tips to keep you safe from shipping- and delivery-notification scams:
    - Legitimate shipping notifications include specific order information, such as your shipping address, an item description or the name of the sender.
    - Stay up-to-date on your orders by visiting the retailer's official website. If you receive an unexpected notification, visit the retailer's website using your browser – not by clicking the link in the email.
    - Never click a link or call back the number from an unexpected delivery notice. Contact the delivery service or seller directly using a verified number or website.

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.

Beware of AI-generated customer reviews

Businesses and organizations are increasingly using artificial intelligence, or AI, to communicate with customers. You may have interacted with AI without realizing it, perhaps when using an AI-powered chatbot while shopping or browsing social-media platforms.

Some companies also use AI to generate customer reviews. When reviews aren't based on real purchases, buyers may end up spending money on products or services that don't meet their expectations.

In some cases, fake review schemes are part of a larger scheme. Fraudulent websites may use fake reviews to lure users into making purchases or signing up for services, only to steal their personal or financial information. In such situations, the harm goes beyond wasted money; it also might include identity theft, financial fraud, and long-term security risks.

If you rely on customer reviews when deciding what to buy, here are some tips to help you determine whether a review is legitimate.

How to spot AI-generated (or fake) reviews:

- **Overly generic language**
  AI reviews often positive but vague. Example: *"This product is amazing! Highly recommend!"* Specifics are lacking. Real reviewers usually mention personal experiences or specific features, including how they used the product or what they liked/disliked about it versus similar products.
- **Repetitive phrases across multiple reviews**
  Look for identical or nearly identical wording. AI-generated reviews may repeat phrases across multiple reviews.
- **Timing patterns**
  A sudden flood of 5-star reviews in a short span – say, within hours or days of each other – should raise suspicions.
- **Reviewer profiles**
  Click on the reviewer's name to find his/her review and posting history. Real users usually have diverse reviews. Fake accounts may have only one or two reviews, often 5-star and for similar products.
- **Too perfect or too negative**
  Be wary of reviews that are *overly glowing* or *harshly critical* without any balance.

In October 2024, the Federal Trade Commission's Trade Regulation Rule on the Use of Consumer Reviews and Testimonials went into effect. The rule bans fake reviews, prohibits the suppression of negative reviews, forbids payment for positive reviews, and requires disclosure when insiders or employees post reviews.

Before making a purchase, compare product reviews from several websites. If one site has only glowing feedback and other sites have mixed reviews of the same product, you may be dealing with AI-generated reviews.

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