

Ohio Attorney General's Consumer Advocate Newsletter

Keeping Consumers Safe and Informed



October 2026

Cybersecurity Awareness Month: Don't make it easy on them

MEET DPXAKER:

He cracks 1,000 passwords a second.

Is yours one of them?
Outsmart him. Find out how!

Don't Make It Easy For Them

Stay Safe Online.org

CYBERSECURITY AWARENESS MONTH

Each October, the Ohio Attorney General's Office proudly supports Cybersecurity Awareness Month, organized by the National Cybersecurity Alliance to remind Americans to stay safe in cyberspace. This year's theme – "Don't make it easy on them" – encourages consumers to proactively "make life difficult for cybercriminals." Cybercriminals can gain access to your personal information via data breaches, dark web monitoring, or personal data brokering.

Here are some tactics to keep your online identity safe:

- **Use long, strong unique passwords:** Scammers often use password-cracking software and artificial intelligence to test thousands of password combinations per second. One way to fight back: Create obstacles that the common scammer will struggle to overcome.

Long, randomly generated passwords are much harder for cybercriminals to crack. Make passwords at least 16 characters, including uppercase and lowercase letters, numbers, and special characters (such as #, !, :, or @). Every password needs to be unique; don't reuse passwords across accounts, apps, or programs. A password manager can help you securely store the unique passwords for all your accounts, many times across multiple devices.

- **Use multifactor authentication (MFA):** Turn on MFA for every account. MFA adds a layer of security beyond a password only – such as a code sent to your phone or email. It protects your account even if your password is stolen.

Many scammers hack into accounts that aren't using MFA by getting passwords off the dark web and through data breaches. Some breaches result in passwords being published all over the internet through automated software. Using an authenticator app or biometrics (such as fingerprints or facial recognition) whenever possible can help secure your data.

- **Update your software:** Fraudsters love to find potential victims among computer users with outdated internet browsers, operating systems, and apps. Regularly install software updates for your operating systems, browsers, and apps to ensure that your devices have the most updated security. Turn on automatic updates everywhere you can, and restart your device when required to buy an update.
- **Beware of phishing scams:** Some scammers pretend to be your bank or a government agency to “phish” for your personal information, often asking you to update or confirm your account by providing a bank account number, password, or Social Security number.

Never respond to unexpected requests for your personal information. Neither your bank nor the Internal Revenue Service will ever request your personal information by phone or e-mail. Be extremely skeptical of unexpected messages, especially those that seem urgent (look for wording that is used to instill fear and pressure). Take time to review all communications. If you see a potential phishing scam, don't click or respond. Delete any text or email messages that you suspect are part of a phishing scam. Let calls from unknown phone numbers go to voicemail or an answering machine.

- **Limit what you share online:** The more personal information a scammer has about you, the greater the scammer's chances of success. Not only can a scammer who has personal details about you seem more legitimate, but the scammer could use personal information to reset your password questions. For example, something as simple as posting where you work could entice a scammer to pretend to be your employer. Additionally, identifying someone as your mother on social media may allow a scammer to know your mother's maiden name, which is often used as a password reset question.

Throughout Cybersecurity Awareness Month, be sure to apply the above tips to make life hard for the scammers and put obstacles in their way.

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.

Help prevent home title fraud

You've probably seen TV commercials and news stories about deed fraud, also known as title theft. Because a home is many people's most valuable asset, it can be an alluring target for scammers.

Deed fraud takes place when a fraudster steals your personal information and illegally takes ownership of your home by filing forged documents with your county government, such as the county auditor's office or county recorder's office. The falsified documents transfer property to the fraudsters or to a related company controlled by the fraudsters. These perpetrators then attempt to profit by selling your property or taking loans using the property as collateral.

Scammers often look for unoccupied homes, undeveloped land, and vacation homes – especially those without a mortgage or with large amount of equity.

Here are some signs that you may be a victim of home title fraud:

- Eviction proceedings against you begin unexpectedly.
- Your property is listed as for sale without your authorization.
- You own vacant property that has been developed without your consent.
- You receive communication about home equity loans or a mortgage from a company with whom you aren't doing business.
- You receive official tax or property documents at your home in someone else's name.
- You see unusual changes in notices you receive regarding property taxes or utilities.

To best protect your home, explore whether your county auditor or county recorder has a free alert system that you can enroll in using your email address. If anyone files documents pertaining to your property, the alert system triggers an email notification. If you own unoccupied properties, do your best to physically visit them regularly or have someone watch for any "For Sale" signs or development activities on them.

If you believe you are a victim of deed fraud, AARP recommends that you file a report with your local law enforcement agency, contact the county recorder's office, and notify your title insurance company. You might also consider contacting private legal counsel and notifying your mortgage company.

In addition to deed fraud, the County Auditors' Association of Ohio recently issued an alert about a YouTube video falsely claiming that consumers should call their county auditor to get a "Senior Homeowner Tax Review Request" form "as required under a federal law."

There is no such federal law, and no such form exists for consumers.

According to the auditor's association, the video uses AI and misleading comments to lend credence to the bogus claims. Downloading and filling out fraudulent forms and clicking on suspicious links could potentially lead to uploading malware to your device, compromising personal information or losing money.

Ohio has legitimate property-tax relief efforts at the state level, such as the existing Homestead Exemption for qualifying homeowners. Also, recent legislation authorizes a one-time, state-funded property tax reduction for eligible recipients in 2027. Your county auditor is a reliable source for additional information about these efforts.

Ohioans should not pay to access any government forms. And, as always, be careful about providing any personal details through unofficial, nongovernmental websites.

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

Largest big tech settlement in history announced

In late August, Ohio Attorney General Andy Wilson announced [a landmark \\$17.1 billion multistate settlement with Meta](#) that requires the company to implement sweeping new safety measures designed to better protect children and teens on Instagram and Facebook.

"With this historic settlement, Meta agrees to establish meaningful protections for young users," Wilson said. "Digital platforms that cater to children have a duty to shield impressionable minds from the risks of unchecked exposure to social media."

Under the proposed agreement, Ohio is expected to receive more than \$319 million over the next decade. The settlement resolves claims that Meta designed its social media platforms with features intended to keep young users engaged and addicted, knowingly exposed children and teens to

serious mental harms, and intentionally misled the public about the safety of its platforms, while also violating the Children's Online Privacy Protection Act by collecting data of children under the age of 13.

The agreement represents a victory for the protection of children online and marks a significant step toward fundamentally transforming how the entire social media industry designs products for children and teens.

That safety features that Meta is required to implement on Instagram and Facebook include:

- Daily time limits and "productive pauses" for children. The hard cap for the two platforms is a combined two-hour daily time limit with mandatory pauses after 15 minutes of continuous use and again at 60 and 90 minutes to interrupt endless scrolling.
- "Nighttime blocks" restricting children's access from midnight to 6 a.m.
- Elimination of push notifications from 8 a.m. to 3 p.m. weekdays during the school year.
- Robust assurance measures to more effectively verify the age of young users.
- Safer, age-appropriate content controls, including stronger safeguards against bullying and content that may promote harmful behavior, such as eating disorders, suicide, and self-harm.
- Stronger, more user-friendly parental controls.
- Disabling of social comparison features, including beauty filters and visible "like" counts, that have been linked to poor mental health outcomes in children and teens.

Both the implementation and efficacy of the features will be assessed regularly by an independent auditor and the settling states.

Attorney General Wilson acknowledged that this problem extends well beyond one company. The agreement establishes groundbreaking changes to Instagram and Facebook that are more significant and comprehensive than any previously ordered by a court or agreed to by a social media company.

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

Protect yourself from employer impersonation scams

Employer impersonation scams occur when fraudsters pose as managers, human resources representatives, co-workers, or recruiters, attempting to trick employees into providing sensitive information, sending money, or granting access to systems. These threats are increasing across industries and growing more sophisticated.

Why these scams are dangerous:

- **Financial risks:** Scammers often use authority-based pressure to request urgent payments, gift cards, or banking changes. These tactics have led to significant organizational losses, including billions linked to business email compromise. For example, the scammer may pretend to be the CEO of the organization requesting that an employee send money to an external bank account.
- **Identity and credential theft:** Impersonators frequently attempt to collect login credentials or personal data by mimicking human resources, IT, or onboarding processes. Once inside, they can hijack accounts, intercept payroll, or gain access to internal systems, including employees' personal information in that system.
- **Reputational damage:** Scams targeting job seekers, such as fake recruiter outreach, could potentially harm a legitimate employer's reputation. It also could discourage real candidates from engaging with the company on genuine opportunities.

- **Legal and compliance exposure:** If scammers misuse your company's identity, it could trigger regulatory consequences and liability.
- **Operational and emotional impact:** These scams disrupt workflows, burden human resources and IT teams, and cause stress or embarrassment for employees caught in deceptive schemes.

How to prevent these scams:

- **Beware of urgency:** Messages insisting that you act immediately, especially ones involving money or confidential information, are a major red flag.
- **Verify email details:** Look for misspellings, unfamiliar domains, or personal email accounts. Even minor differences matter.
- **Confirm suspicious requests:** If a message seems off, contact the sender using your known company contact methods, not the number provided in the suspicious message.
- **Watch for unusual instructions:** Real employers won't ask you to buy gift cards, send codes, provide credentials over text, or update payroll information outside formal channels.
- **Scrutinize human resource- and ITS-themed messages:** Scammers know HR and ITS departments carry authority. Be cautious when notices that ask you to do something come from either of these departments.
- **Check links and login pages:** On mobile devices especially, fake login portals look real because URLs are harder to see. If the page feels unfamiliar, stop and verify.
- **Validate recruiter communications:** Recruiter impersonation is on the rise, especially for new hires. If asked to provide sensitive information before official onboarding, confirm the legitimacy of the request through verified channels.

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



For more information, contact Ohio Attorney General
Andy Wilson's Consumer Protection Section at 800-282-0515
or www.OhioAttorneyGeneral.gov