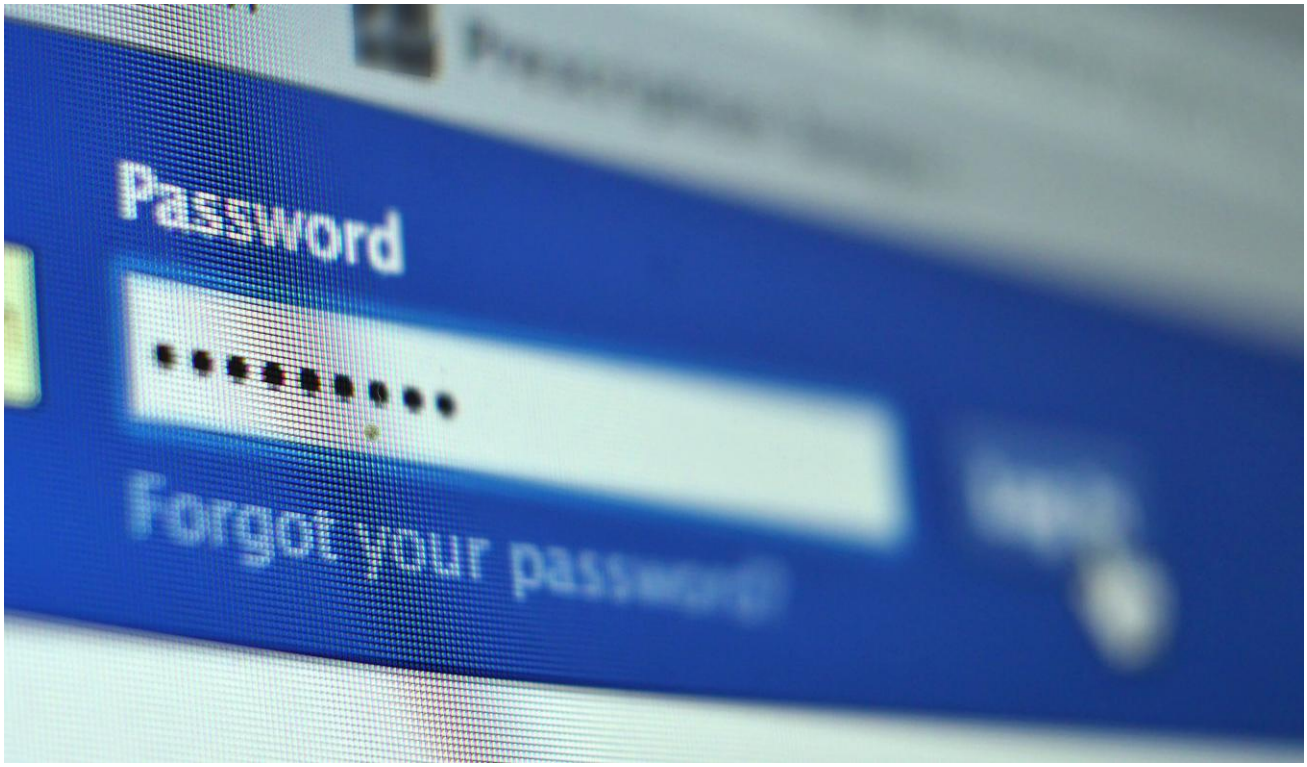
Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

October 2025



Passphrases, passkeys and password managers enhance cybersecurity

October is Cybersecurity Awareness Month, and the Ohio Attorney General's Office proudly supports this annual awareness effort by promoting the "Core 4" steps to improved security in cyberspace:

- **Use strong passwords and a password manager.** Long, unique and randomly generated passwords are much harder for cybercriminals to crack. A password manager helps you securely store these unique passwords for all your accounts, many times across multiple devices.
- **Turn on multifactor authentication (MFA).** MFA adds a layer of security beyond a password only – such as a code sent to your phone or a fingerprint scan. It protects your account even if your password is stolen.
- **Recognize and report phishing.** Be cautious of unsolicited messages or links that attempt to steal your information. Knowing the common signs of phishing helps you identify such scams; reporting the scam helps protect you and others.
- **Update your software.** Regularly install software updates for your operating systems, browsers, and apps to ensure that your devices have the most up-to-date security.

Safety in cyberspace demands strong passwords – at least 16 characters, including uppercase and lowercase letters, numbers and special characters (such as #, !, : or @).

Strong passwords help to prevent unauthorized access, guard against cyber-attacks and enhance overall online security. Although reusing passwords across multiple accounts can make them easier to remember, the practice is discouraged because if one of those accounts is compromised, all accounts using that password could be compromised.

A newer tool in password maintenance and security is a password manager using passphrases as passwords and passkeys. Password managers offer numerous benefits. They enable the creation and use of strong, unique passwords for each account. Password managers also streamline the login process with autofill features. A final benefit: A password manager allows passwords to be shared and remembered across devices – such as your phone and your computer.

Passphrases are longer alternatives to traditional passwords. They typically consist of a sequence of multiple words, making them easier to remember while still providing strong protection against hacking attempts. Because passphrases utilize a phrase developed by the user, they are generally easier to remember. An example of a passphrase: *I like to read books and pet cats*. As the password, this phrase could be entered as: *Ilike2ReadB00ks&petcat$*

When using passphrases, be sure to:

- Avoid using famous quotes.
- Avoid personal information.
- Vary the capitalization of letters and add special characters.
- Avoid the same passphrase for multiple accounts.

Using passkeys is a new way to protect your security with your online accounts. Passkey examples include using your fingerprint or face scan to log in to your account through your own smartphone instead of typing a password. A passkey requires a bit of work upfront. After the initial setup, the passkey uses either facial recognition or fingerprint, eliminating the need to remember a password for that account.

- Register passkey on device: When you create a passkey, your device generates a unique, encrypted pair of cryptographic keys – a public key and a private key. The public key is sent to the website you're signing up for; the private key remains securely on your device.
- Log in to account: When you try to log in, you're prompted to authenticate using a local method, such as a fingerprint, facial recognition, or a device PIN.
- Verify: After the first login, you may be asked to verify your account by a code sent via text message or email.

For more information about passwords and related issues, visit the Cybersecurity & Infrastructure Security Agency.

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

‘Account takeovers’ pose a growing threat

Cybercriminals use various tactics to gain access to your personal and financial accounts, often with the goal of stealing money or personal information. Often, they gain your login credentials and change your password to lock you out – a crime known as an “account takeover.” Being aware of this type of crime may keep you from becoming a victim.

Account takeovers allow criminals to gain complete access to an account. From there, they can transfer money to themselves, redirect payroll deposits, or pretend to be that person on social media.

For victims, account takeovers can lead to significant financial losses and a loss of personal information, which can lead to identity theft. When account takeovers happen on social media, the scammer – pretending to be the victim – may try to get “friends” or connections to send money or disclose other information.

According to the Internet Crime Complaint Center (IC3), criminals that seek access to your personal and financial accounts can achieve their goals using several methods:

- Taking advantage of a consumer’s weak passwords and/or the lack of two-factor authentication. Multifactor authentication (MFA) is a security enhancement that requires you to present two pieces of evidence to log in to an account. Beyond just something you know (such as your password), you generally must also demonstrate something you have (such as a phone) or who you are (such as a fingerprint or face scan).
- Phishing for personal information using a legitimate-looking email to trick consumers into disclosing login credentials. Scammers also use bogus websites that may appear to be a consumer’s online bank portal or payroll website.
- Deploying social engineering tactics by pretending to be an employee of a consumer’s bank, customer service representative from a company they do business with, or a tech-support or computer-repair professional.
- Obtaining data breach information available on the dark web to gain a consumer’s login credentials.
- Installing malware (malicious software) on a consumer’s device. Consumers can unknowingly download malware by clicking on suspicious links and pop-up advertisements or by opening suspicious email attachments. There are many types of malware, including viruses, adware, ransomware, and spyware. This malware could infect a computer, spread to other computers, show consumers unwanted advertisements, lock up their device, and even capture personal information stored on their device.

Experts at IC3.gov recommend the following tips to prevent account takeover fraud:

- Be mindful of the information you share online, especially on social media platforms. Through oversharing, consumers might be helping scammers to guess their passwords or the answers to password-reset security questions.
- Keep a close tab on your financial accounts, including bank, investment and credit card accounts. Examine these resources for potential problems, such as a missing deposit or an unauthorized withdrawal.
- Be sure to use unique, complex passwords or hard-to-guess passwords for each account, and make sure that two-factor authentication is enabled on accounts that allow this extra security mechanism.

- Maintain links to your favorite account websites to avoid visiting fraudulent login pages. Fraudulent logins may be found when using internet search results or advertisements to help connect to your accounts.
- Guard against impostor bank employees, customer-service reps, and tech-support professionals. Remember that scammers can spoof the caller ID information you see on your phone using readily available technology. Rarely do legitimate companies contact consumers out of the blue to request their login/password or one-time security/access code.

In addition, be vigilant and never allow a stranger "remote access" to any of your devices. Some scammers try to gain access to your account by posing as technical-support companies and try to persuade you to let them "fix" your computer by accessing it remotely through special software and/or websites. Once access is gained, however, the scammer may install malware or hold the computer hostage until you send money to regain control.

For more information, including what to do if you're a victim of account takeover fraud, click here.

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.

Buying a new car or truck? Pre-purchase tips, consumer laws are here for you

Before visiting a dealership, here are some pre-purchase tips for Ohioans looking to buy their next new vehicle:

- Research any vehicles you're considering – to narrow down the models you're most interested in, the features you want on the vehicle, optional features you would like, and the price you're willing to spend. You may want to consult recommendations and new-car comparisons in consumer magazines and/or auto magazines.
- Allow enough time to make a well-informed buying decision. Compare prices at different dealerships and invest time with each salesperson.
- Know your credit score, which often dictates the financing terms available to you if you take out a car loan. You can check your credit reports free at www.AnnualCreditReport.com. Although the site won't provide your exact credit score, it will give you a sense of what credit you have opened in your name. Also, keep an eye out for accounts you don't recognize. Some credit card companies put a version of your credit score on monthly statements to lend insight into your credit-worthiness.
- If you have frozen your credit reports at the three major credit-reporting bureaus, you will need to temporarily unfreeze it at whichever bureau will be used to run your credit. Once your bank and/or dealership are finished, you can then re-freeze that credit report at that bureau.
- Compare the interest rate of local banks and credit unions along with financing options available through dealerships.
- Dealerships offer many consumers additional product and service options, including extended service contracts, undercoat protection and dealer-installed alarms. Such add-on purchases are not required to buy the new vehicle.
- If you plan to trade in a vehicle, know its general value based on guides such as Edmunds (www.edmunds.com) and Kelley Blue Book (www.kbb.com) before negotiating the trade-in value.

Every financed vehicle sale must include a Truth in Lending Act disclosure box. This box explains to the consumer the true cost of financing the vehicle, including the interest rate, down-payment amount, purchase price, cost of interest payments, and overall cost of the vehicle (with interest and principal payments). Consumers should carefully review this information before completing the sale.

New-car buyers should be aware that Ohio's Lemon Law generally covers new vehicles within the first 12 months or 18,000 miles, whichever comes first. A "lemon" is a new vehicle that has one or more problems, covered by the warranty, that substantially impair the use, value or safety of the vehicle. Under the Lemon Law, the auto manufacturer must be given a reasonable opportunity to fix the problem; if the problem is not corrected, the consumer might be eligible for a refund or a replacement.

For more information on Ohio's Lemon Law, including the process to exercise your consumer rights under this law, click here.

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.

Job hunters: Beware of opportunities that seem too good to be true

Many job scams promise high pay for little work, but instead of delivering income, they often result in fraudsters obtaining your personal information or access to your financial accounts. These scams may be presented as advertisements on social media, email messages or text messages.

A common tactic involves fake checks. Scammers send a check to supposedly cover equipment costs, such as a new computer or software. They instruct you to deposit the check into your bank account and then use a money-transfer service, gift card, or prepaid money card to send the same amount to a "vendor." The check inevitably bounces, however, which means the money you sent to the fake vendor comes out of your pocket.

Before applying for any job posting, research the company thoroughly. Some red flags to watch out for:

- The posting includes a vague job description and claims that you can make hundreds or thousands of dollars doing very little work.
- Communication from "company representatives" comes from free or personal email accounts, such as those from gmail.com, yahoo.com, hotmail.com or aol.com.
- You're hired without ever meeting anyone in person.
- The company doesn't have a website.
- You receive a check before any work is performed.
- You're asked to wire-transfer money or purchase prepaid money cards.

Common scams include task-based scams, mystery shopper scams, and offers for high-paying data-entry jobs, often requiring you to pay upfront fees or share banking information.

Forbes lists the following as the top job scams to beware of in 2025:

Remote Work Opportunity Scams

This scam begins with the promise of a work-from-home job that requires little effort, with the posting appearing alongside legitimate job postings. The biggest red flag is compensation that is greatly outsized compared with the effort and skill required for the work. Some offers may be described as updating data or increasing visibility for the company, for example, with compensation listed at $100 to $500 a day.

Reshipping Job Scams

These job scams recruit individuals to receive packages at their home, repackage them and ship them to a destination. The packages received are often purchased with stolen credit cards. Receiving items purchased with stolen money shifts the individual from an “employee” to a reshipper. Victims don’t realize that they’re participating in criminal activity by receiving and distributing the items. In addition to possibly facing criminal charges, victims are unlikely to ever be compensated for packaging and shipping the items.

Bogus Employment Agency Scams

Bogus employment agencies appear to be legitimate, offering resume enhancement, interview coaching and/or direct access to upper management at the hiring agency. After collecting payment, the fake agencies either disappear or continue stringing victims along with a series of additional fees for premium services.

Consumers who need help resolving a complaint against a business or 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.