



Ohio Attorney General's
**Consumer Advocate
Newsletter**

FEBRUARY 2018

[Trial Offers: When Free May Not Always Be Free](#)

Some advertisements promote free, no-risk trials for the latest and greatest product. But watch out! Asking for these free items may subject you to additional purchases and payments.

Do your homework before accepting a free trial offer. Businesses must clearly disclose that you will be charged for additional goods or services, but buying plans vary, and some may be difficult to cancel, make it hard to find terms and conditions, or have boxes pre-checked during your trial offer signup that will enroll you in a plan unless you uncheck the box.

Some buying plans will send you a notice before shipping more products to your home. Known as “opt out” shopping, you need to reject the shipment within a certain timeframe or you can expect to receive additional items along with an invoice or automatic charge to your credit card.

The Prenotification Negative Option Rule gives you the right to receive clear, prominent details of how the buying club works as part of the promotional materials used to enroll you. A company must disclose:

- How many notifications you may get per year, and how often you will see them in the mail;
- That you will have at least 10 days to reject the product before it is automatically shipped to your home;
- If you are required to buy a certain number of products; and
- That you may cancel the plan any time once you have met the minimum purchase requirement.

Other plans do not notify you of the additional products before they ship. This is called a continuity plan, where you keep getting the product until you cancel your membership. With continuity plans, there may be a “free trial” or “approval” period. If you don’t cancel by the end of this period, you become a member. If you use your credit card when you sign up, you can expect the card to be automatically billed with each shipment.

To help better understand what you are signing up for, consider the following:

- Research companies by going online to read consumer reviews and find out how they sell their products.

- Read the terms and conditions of the offer, even if you are responding to a TV or radio advertisement. Look online for more information and if you can't find the details, don't sign up.
- Look out for pre-checked boxes that may tell the company that you agree to receive more products or sign up for a membership-based plan.
- Keep copies of all documents and records of your communication with the company.
- Record the dates you mailed any forms or letters rejecting shipments.
- Find out how to cancel during the trial period to avoid any future shipments and charges.
- Review your credit or debit card statements carefully, looking for any charges you don't expect.

If you are charged for products you didn't order, first try to work out the problem with the company. If the company is not responsive, contact your credit or debit card company to dispute the charge. Ask the card company to reverse the charge because you didn't authorize the additional products.

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.

[Five Ways to Avoid Online Romance Scams](#)

It's that time of year when you or someone you know might be seeking out that special someone, and con artists know it. Fake online romance is prevalent, so we've outlined ways to avoid sweetheart scams and protect your hard-earned money.

Romance scams typically begin when a con artist creates a phony profile on a dating website or on social media to attract unsuspecting victims. Many times, con artists claim to be located in another state or country — pretending to be an oilrig worker, a military member stationed overseas, or a businessperson working in another country. They may even send fake photos or documentation in order to "prove" their identity. The scammer and the soon-to-be victim may spend countless hours communicating before the scammer asks for money for reasons such as airfare to visit, hospital fees or medical costs, to get out of a foreign country, or to access an inheritance the scammer promises to share with the victim.

Victims generally are asked to send money using a wire-transfer service, money order, prepaid card, gift card, or other hard-to-trace payment method. Once the money is sent, it is nearly impossible to recover. In 2017, about 40 Ohioans reported losing a total of \$1.6 million to sweetheart scams.

A woman in Henry County said she fell in love with a supposed foreign businessman who convinced her to send more than \$80,000, which he promised to return as soon as he finished a project in

Cambodia. She had received photos of him and talked to him over video chat (or so she thought), but her relatives convinced her that he was actually a romance con artist.

A Preble County woman met a con artist on a popular dating website and eventually sent him money and a new cell phone for his new business venture. The scammer sent her a copy of a passport and claimed to be from the Dayton area, making the ploy seem real, but the consumer ended up losing a reported \$37,000.

Tips to avoid sweetheart scams include:

1. Research someone you meet online; don't rely solely on what that person tells you. Conduct internet searches and check with independent sources to verify the person's claims.
2. Be cautious of individuals who claim it was destiny or fate that brought you together or who claim to love you soon after you meet online.
3. Talk to friends and family members about any online relationships, even if the other person asks you to keep the relationship a secret.
4. Don't send money to someone you've only met online, even if you have developed a relationship with the individual.
5. Be very skeptical of requests for money sent via wire transfer, 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 Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

[Know More About Credit Repair and Debt Settlement Companies](#)

Some services advertise that bad credit can be erased or your debts can be settled, but it takes a watchful eye to tell the legitimate services from the scam artists.

Credit Repair

Some for-profit "credit repair" services charge hundreds or thousands of dollars but do little or nothing to improve your credit. The reality is that they cannot erase negative information from your credit report if the information is accurate. With certain exceptions, negative information can generally remain on your credit report for up to seven years.

Here are some questions to ask credit repair companies before signing up for any of their services:

- How much do the services cost?
- What do you offer that I can't do myself?
- What proof will you provide that you are negotiating with my creditors?

- What are your cancellation policies?
- Are you in compliance with the [Ohio Debt Adjusters Act](#)?

The Credit Repair Organization Act – enforced by the Federal Trade Commission – and a similar Ohio law make it unlawful for a credit repair company to lie about their supposed benefits or to charge you before providing services.

Debt Settlement

Debt settlement companies typically offer to negotiate with creditors on your behalf. They may try to advocate for you to be able to pay one lump sum that is less than your total debt. To save up for the lump sum, you are typically asked to set aside an amount each month in an escrow account as the company negotiates with your creditors. The debt settlement company may tell you to stop making monthly payments and try to get the creditors to accept the lump sum.

Be very leery if a debt settlement company asks you to pay upfront fees. Debt settlement companies are only allowed to charge fees based on the debt they have successfully settled on your behalf. This amount should only be a portion of the company's full fee.

Some of the potential risks involved in a debt settlement company's process include:

- The programs may require three years or longer of monthly payments to achieve the needed lump sum. Some consumers having trouble making ends meet may not be able to keep up with those monthly payments.
- Your creditors may reject the debt settlement company's attempt to negotiate the settlement. Some debt settlement companies try to settle your smaller accounts first, while interest and fees continue to accumulate in your larger accounts.
- If you've been convinced to stop making monthly payments to your creditors, you may get hit with a lower credit score, along with potential late fees and penalties.
- You may end up paying more for the services provided than what you're saving in having your debt negotiated.

If you are having trouble paying your bills, you may want to first contact your creditor directly. You may be able to arrange a payment plan yourself at no cost. You can also contact a nonprofit credit counseling service in your area. Look for a service at www.nfcc.org or by calling 800-388-2227. If you decide to contact a debt settlement company, research the company first with the Ohio Attorney General's Office, check online for reviews, and look for previous lawsuits brought against the company.

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.

[Beyond Passwords: Four Cyber Tips For 2018](#)

Do you go online but wonder if you are taking all the right cybersecurity steps? Here are four tips you can apply right now.

Passphrases

Cybersecurity experts are encouraging people to use passphrases instead of passwords. A passphrase is a sentence or combination of words that is easy to remember but longer and more complex than a traditional 8-12 character password.

The following is an example of a good passphrase: IWantChocol@te2day. This passphrase works because it is unique and easy to remember. Additionally, it is long and complex and contains unexpected characters, increasing its strength.

When developing a passphrase, here are some tips to consider:

- A passphrase can include lines from a book, song, movie, or play.
- Increase complexity by adding unexpected characters, such as symbols, numbers, or capital letters.
- As with any password, the longer, the better.

Two-Factor Authentication

Two-factor authentication (2FA) is a security enhancement that requires you to present two pieces of evidence to log into an account. Beyond just something you know (like your password), you generally must also demonstrate something you have (like a phone) or who you are (like a fingerprint or retina scan).

Examples of 2FA that you may already use include:

- Inserting your debit card at an ATM and then entering your PIN.
- Logging onto a website that sends a numeric code to your cell phone, which you must enter in order to gain access to your account.

Using 2FA helps protect you by adding an additional layer of security, thus making it harder for cybercriminals to access your account. While no account can ever be completely safe from cybercrime, using 2FA can substantially reduce the likelihood that your account will be compromised.

You can verify if your online services offer 2FA by going to <https://twofactorauth.org> and clicking on the appropriate category that applies to your service. Just because a service offers 2FA doesn't mean it is active. You must enable 2FA on each of your accounts in order to use this additional layer of security.

Password Managers

Finding it next to impossible to remember all your complex, unique, and long passwords or passphrases? Consider using a "password manager" program or app to keep up. Password managers can create, use, and store passwords in a program that may use strong encryption to make your personal information difficult to hack but still easy for you to access using a master password that you must memorize or keep in a secure location that only you have access to.

Some password managers are free while others charge a monthly fee. Some store your passwords on your device while others use cloud-based storage. You may find it helpful to ask friends and family for recommendations, read consumer reviews, consult computer-related websites, and use other tech resources to find the password manager that is right for you.

Backup Your Devices

Computer viruses such as ransomware can lock up your device and demand money to let you access your own data. Given these risks, it is more important than ever to back up the information and other data on your devices on a separate external hard drive or through a cloud-hosted service. By backing up your device, you may be able to restore your data if it is lost or compromised. As with password managers, there are a variety of backup options, so look to recommendations, reviews, and your other tech-related resources to find the backup method that is right for you.

To learn more from the Ohio Attorney General's Office or to schedule a [free presentation](#) on the Cybersecurity Help, Information, and Protection Program (CHIPP), visit www.OhioProtects.org, or call 800-282-0515.