Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

October 2021

Ohio Attorney General Offers Online Shopping Advice

Retail stores' holiday decorations seem to pop up earlier and earlier every year. Before you know it, the winter holidays will be here, so it's best to prepare early to shop smart.

Ohio Attorney General Dave Yost offers the following holiday consumer protection tips:

- **Beware of e-skimming while shopping online**: Cybercriminals can capture your personal information by inserting skimming code into the payment processes of unsecure or fake websites. To avoid that trouble, look for the "s" in "https" in the website address to ensure the site is secure, and always double-check that the site you're on is the legitimate site for the company. Also, when possible, use credit cards instead of debit cards because credit cards have more protections.
- **Plan before you shop:** Review ads carefully and compare deals. Important exclusions and limitations must be disclosed in ads, even online, so check the details to see if limited

quantities of an item are available for sale, if the sale price is valid only during certain hours, or if other terms and conditions apply.

- **Research online reviews:** Be skeptical of reviews posted with generic names and profiles that do not have a photo; they could be impersonating a legitimate shopper. You can cross-reference customer reviews of the same products on different websites: If you see consistent reviews on several online stores, that may add validity to the feedback.
- **Beware of package tracking scams:** In a package tracking scam, you may receive an email alerting you of a delay in the shipping of a package. The email will either ask you to provide personal information or click on a link for additional information. But providing personal information could lead to financial harm or infect your computer with malware. Keep track of which retailers you've ordered from, in addition to your shipping confirmation emails. Don't click on links if you're not certain the sender is legitimate.
- **Check return policies:** In Ohio, sellers can set their own return policies, including policies of "no returns." But if they have a policy that limits your ability to get a refund, they must clearly notify you of that policy before you complete the purchase. Also, be sure to check return periods as they may change during the holidays.
- **Be aware of third-party sellers:** Many companies offer the ability for multiple venders to sell products on their website. When purchasing an item from a company website, ensure you know if you are purchasing the item from that company or a third-party seller. The company's refund polices and warranties may differ from those of a third-party seller.
- **Look out for "free" offers that renew automatically:** Before signing up for a free trial of a product or service, check the details, especially if you are asked to provide your credit card number or pay for shipping and handling. In many cases, signing up for the offer will automatically enroll you in a program that incurs charges on a regular basis.
- **Compare gift cards:** Not all gift cards are alike, so review the terms and conditions before you buy. In general, most gift cards must last at least five years, but fees may vary depending on the type of card, such as a single-store card or a prepaid network-branded card that can be used almost anywhere. Also, promotional cards like those that come free with a purchase may not have the same protections.
- **Keep your receipts:** Maintaining a complete record of a sale will help you handle problems if they arise after the purchase. Keep copies of receipts, sales agreements, advertisements, photos of products and other documentation of a sale until the transaction and billing process are complete.
- **Check delivery dates and fees:** Carefully review the expected delivery date and shipping costs before you make a purchase. Find out whether you'll be charged return shipping or restocking fees if you return the product. Also, pick up delivered packages promptly so they're not stolen or damaged outside your door.
- **Monitor your accounts:** Regularly check your credit card and bank accounts for unauthorized charges or unexpected activity. If you find problems, immediately notify your credit card provider or bank. The sooner you identify a problem, the sooner you can work to correct it.

Consumers who suspect an unfair business practice or who want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Cybersecurity Awareness Month: Learn the Red Flags of a Phishing Scam

October is Cybersecurity Awareness Month, and it is a great time to learn more about essential elements of protecting computers and mobile devices – such as smartphones and tablets – from attacks and unauthorized access. One method scammers use in an attempt to pry personal identifying information out of unsuspecting consumers is called "phishing."

Phishing occurs when a scam artist sends an email pretending to be a trusted organization. For example, a scammer might pretend to be your bank, even using the bank's logo. Scammers often create imposter websites to trick you into revealing personal information to untrusted sources. According to published reports, 43% of cyberattacks last year came through phishing or pretexting, which occurs when a con artist invents a fake scenario in order to gain access to your personal information.

When reading emails, text messages and other communications, be sure to look for these red flags:

- **Suspicious email addresses:** Always review the address your email is coming from. If it is off by just a single letter, it's a sign that a phishing scam is in action. Also, hovering your cursor over the supposed email address may reveal a different source. You should scrutinize every email before clicking on any links or taking any requested action.
- **Generic greetings:** Phishing attempts often begin through a mass email to thousands or millions of recipients. If there is no greeting or if the greeting is generic ("Dear Accountholder"), if it uses only your email address or differs from past communications with the same sender, be skeptical.
- **Spelling and grammar:** Phishing messages often contain grammatical errors or spelling mistakes. Many phishing attempts originate in foreign countries, so be sure to watch for awkward language or verbiage that appears out of character for the source the information is supposedly coming from.
- **Deceptive web addresses:** Know that links in an email or on a website or document may show text that is different from the link's true destination. Try hovering your curser over the text or link without actually clicking on it: You will likely see the URL (web address) of the actual destination that you would be sent to. (Sometimes this appears at the bottom left of your browser window.) Also, remember that the web address you are asked to click on may be similar to a legitimate company, organization or government agency, but not exact. It is important to look for subtle differences, such as an extra dot or a missing letter.
- **Expressions of urgency:** Is the sender trying to use language to get an emotional response from you? The goal of some phishing scams is to get you to act quickly based on emotions such as fear or excitement. If the letter or notice is too good to be true, be especially careful. For example, did you win a contest you never heard of or entered in? Gain an inheritance from a distant relative you never met? Get an unexpected refund or credit? Be a skeptic!
- **Unexpected or suspicious attachments:** Treat all attachments with caution. Did the sender provide an attachment you didn't request? Does the sender typically send you attachments or is it out of character? Is the attachment's file name or file type unusual? If you have any hesitation, verify with the sender before opening or clicking anything.
- **Requests for account details or other sensitive information:** Many phishing scams begin with an email supposedly from a well-known bank or other organization where you might have an account. These days, such institutions are not likely to ask for account information in an email. Responding could bring you to a fake website's login page in hopes of stealing your login credentials and other personal information.

Experts are also warning consumers about scammers who use QR codes to disguise harmful links to fraudulent websites, hoping to convince consumers to scan the code that, in reality, leads to downloading malicious software. If you ever scan QR codes using your device, read the Better Business Bureau's scam alert and be aware that some scammers are directing consumers to phishing websites using QR codes.

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

Warning: “Free Trial” Offers May Be Costly

Some advertisements promote free, no-risk trials for the latest and greatest products. But buyer beware: Signing up for some of 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. Some offers may be difficult to cancel, make it hard to find terms and conditions, or have boxes pre-checked during your trial offer signup to automatically enroll you in a plan unless you uncheck the box.

Know that you typically have to provide a credit card number when requesting a free trial. That is often so the business can charge you if you don’t cancel before the trial period expires. Some unscrupulous businesses may make it hard to cancel, potentially charging you when you really want to unsubscribe. A smart consumer tip is to always mark your calendar when you need to cancel or when a promotional rate expires. Also, you may need to pay shipping and handling, making the “free trial” offer come with a cost to you.

To help better understand what you are signing up for:

- 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. What are you agreeing to? If you can’t find details, don’t sign up.
- 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 – called a “chargeback” – because you didn’t authorize the additional products.

Once a free trial period expires, oftentimes an ongoing subscription begins using “auto-renewal.” With auto-renewals, your credit or debit card gets charged for the next subscription term. Before a subscription can auto-renew, it should send you a renewal notice as a reminder about when your subscription expires and that you’ll be charged automatically for the next term.

Pay attention to the subscription rate indicated on the renewal notice. For example, the rate may have increased, especially if you were offered a temporary promotional rate that has expired. If you notice a higher than expected rate or if no rate is listed at all, contact the company and inquire. This may also provide you the opportunity to negotiate a new rate or begin the cancellation process if you so choose.

Before you give out your credit card information for a free trial or subscription, the Federal Trade Commission advises that you:

- **“Read all of the details.** Check whether the business will keep charging you unless you tell it to stop. If that’s not clear, assume it will. Why else would the business want your credit card number?
- **Look for pre-checked boxes.** Some businesses use these hoping that you won’t notice you’re agreeing to be billed later. Uncheck the box if you don’t agree with what it says.
- **Make sure you know how to cancel.** Check the business’s website for an explanation on how to cancel. Businesses should make this easy for you. It’s the law. If it’s not clear how to cancel, walk away.”

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.

Be on the Alert: Advanced-Fee Loan Scams

Have you had difficulty obtaining a loan? Scammers could target you with an advanced-fee loan scam. Typically, they look for people with poor credit who have recently applied for loans, offering them a guaranteed loan or access to a list of potential lenders who aren’t as concerned with credit scores, as long as the individual pays in advance. These scammers claim to work for a legitimate lending institution, such as a bank or credit union, but none of these assertions are true. Once the fee is paid, the scammers stall the process with endless excuses or disappear altogether.

Consumers throughout Ohio are reporting losing money to advanced-fee loan scams. In some cases, they have sent hundreds of dollars out of the country for loans that are nonexistent.

For example, a Central Ohio consumer received a call saying she qualified for a loan worth up to $5,000. In order to receive the loan, she first had to send $300 via wire transfer to India. She sent the money, but never received the loan. It was all a scam.

In an advance-fee loan scam, con artists ask for upfront fees in exchange for a loan or line of credit. Victims often are asked to wire money to another country to secure the loan. After sending the money, however, victims receive nothing.

Requests for wire transfers in exchange for a loan almost always signal a scam.

Signs of an advance-fee loan scam include:

- Calls or emails offering loans.
- Claims of “guaranteed” loans or lines of credit.
- Demands for advance fees, such as a “bank processing fee.”
- Requests for money sent via wire transfer.
- Companies that fail to provide loan information in writing.

In a related scam, consumers are contacted by “debt collectors” who demand payment on past-due loans. Consumers who receive these calls frequently say they had applied online for a payday loan but never received the loan and do not owe the money.

Sometimes the callers threaten consumers with arrest or jail time if they refuse to pay.

If you receive calls demanding that you pay a debt, tell the callers to provide written verification of the debt. If they refuse, don't trust them and don't send any money. The law requires debt collectors to provide verification that you owe a debt.

Protect Yourself
Not sure if the lender you're talking with is legitimate? These steps can help you protect yourself against scammers.

Check to see if the lender is registered in your state. Lenders must register where they do business. In Ohio, contact the Department of Commerce, Division of Financial Institutions to find out if a lender is registered.

Search online. Type the company's name into a search engine with words like "review," "complaint" or "scam." You can search for phone numbers to see if other people have reported them as scams.

Hang up on robocalls. If you pick up the phone and hear a recorded sales pitch, hang up and report it using the Ohio Attorney General's Unwanted Call Notification Form. These calls are illegal. Don't press 1, 2 or any number to get off a list or speak to a person. That just means you'll get even more calls.

Don't pay for a promise. Whether someone asks you to pay in advance for a credit card, loan offer, debt relief, mortgage assistance or a job, walk away. No one legitimate will ever ask you to pay for a promise. If they do, it's a good bet it's a scam.

Get help dealing with debt. You may have more options than you think. Nonprofit organizations in every state offer credit counseling services that often are free or low-cost. Learn more about possible options for coping with debt here.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.