Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

December 2021

Ohio Attorney General Offers Online Shopping Tips for Consumers

With the holiday season upon us, the Ohio Attorney General's Office is offering tips to help identify shopping scams.

Because it's a busy time of year, scammers are counting on you to be distracted – and thus vulnerable to scams while you shop for holiday gifts.

Here are some general tips for online shopping:

- **Beware of e-skimming while shopping online:** Cybercriminals can capture credit card and personally identifiable information by skimming your data online. Look for the "s" in "https" to ensure that a website is secure, and always double-check that the site you're on is the company's official (re: legitimate) site. Also, use credit cards instead of debit cards; credit cards have more safeguards.

- **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 whether limited quantities of an item are available for sale, the sale price is valid only during certain hours, and/or other terms and conditions apply.
- **Make sure to research online reviews:** Watch out for generic names and profiles that do not include a photo. Cross-reference customer reviews of the same products on different websites. If you see consistent reviews on several online stores, it may add validity to the feedback.
- **Check return policies:** In Ohio, sellers can set their own return policies, including policies of "no returns," but any retailer whose policy limits your ability to obtain a refund must clearly notify you of that policy before you complete the purchase. Be sure to check return periods, which might change during the holidays.
- **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 must provide a credit card number or pay for shipping and handling. In many cases, signing up for the offer automatically enrolls you in a program that then charges you on a regular basis (say, monthly).
- **Check delivery dates and fees:** Before you make a purchase, carefully review the expected delivery date and shipping costs. Find out whether you'll be charged shipping or restocking fees if you return the product. Also, retrieve delivered packages promptly to prevent them from being stolen or damaged outside your door.
- **Be aware that rain checks apply only in certain situations:** If a seller advertises a product at a certain price but sells out of the product by the time you respond to the ad, you may have the right to a rain check. Sellers aren't required to provide rain checks, though, if they clearly disclose the product quantity available at that price or clearly state that no rain checks will be given.
- **Keep cybersecurity in mind:** When shopping for deals online, don't use free public Wi-Fi when entering sensitive information such as a credit card number. Keep apps, software and operating systems up-to-date and use secure websites whenever you need to enter personal information.
- **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.
- **Beware of business impersonation scams:** Last month, AG Yost warned consumers that illegal robocallers are trying to ruin Christmas by posing as legitimate businesses such as Amazon and other big companies to get your money. Learn more here.

A final takeaway from AG Yost, "Online shopping can be a timesaver during the busy holiday season, but don't let convenience become a hassle."

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.

Be a Wise Donor This Holiday Season

The sound of jingle bells signals an uptick in charities seeking year-end donations. To prevent your holiday contributions from going to waste, it's important to learn to be a wise donor – by recognizing charitable giving scams and researching organizations that you're interested in supporting.

If you are asked to give money to an unfamiliar charity, take time to do a little investigating before you contribute. Call the charity – a reputable organization will welcome inquiries – and carefully examine the information and materials provided.

Sometimes, a charity calls to solicit its donations. Be aware that the solicitor must provide the charity's name and other basic information, including the location of the organization's principal place of business.

The Ohio Attorney General's Charitable Law Section advises donors to ask the right questions and do research to make sure their gifts will be used as they intend.

Check out AG Yost's tools for researching charities to help make informed decisions about giving.

Things to think about when giving to charity:

- If you're considering a donation to an unfamiliar group, check the organization's website first. Does the information match what you received when asked to contribute? Do the group's programs and services make sense? Does the charity provide useful information and seem to foster transparency?
- Talk with friends and family about unfamiliar solicitations. Have they heard of the group? Do they know of anyone who has been helped by it?

Most charities are well-intentioned, but there are inevitably some bad apples in the bunch. Watch for these warning signs of a potential charitable giving scam:

- Do not provide credit-card or banking information to unexpected callers. Ask for written information.
- Consider checking with the charity mentioned by a caller to determine whether its fundraising campaign is legitimate.
- Avoid groups that pressure you to make donation decisions immediately or offer to pick up a gift at your home.
- Beware of an individual or entity that doesn't provide a real callback phone number.
- Don't be fooled by a charity's name. Fraudulent organizations often create names similar to those of large, well-known charities. Scams often center on causes related to veterans, police and fire departments, natural disasters and cancer.
- Recognize that scammers may claim that you made a pledge or donated previously when you did not. They also may ask you to make a check payable to an individual instead of an organization.
- Ask for details. Some charities pay professional solicitors to raise money on their behalf. When asked, the fundraisers must disclose the percentage of donations that benefit the charity. Sometimes the figure is very low – not a good sign.

To reduce the stress and pressure involved in receiving charitable solicitations, consider developing a giving plan in advance. You can start by identifying the groups you feel strongly about, and donate solely to them. You can tell other solicitors that you have finalized your annual giving plan but would be happy to review written information for next year.

If you learn that a charity is misusing resources or know of fraudulent solicitations, please file a complaint with the Ohio Attorney General's Office at 800-282-0515 or by clicking here.

Gift Cards: To Give or Not to Give

Gift cards are a popular present – for giving and receiving – especially for last-minute shoppers or for people without a wish list.

Not all gift cards are created equal, though. It's crucial to know the basics about gift cards – from expiration dates to potential scams – before making a purchase.

Both state and federal law protect gift cards. Under Ohio law, gift cards in any form — electronic, plastic, paper, etc. — generally cannot expire for at least two years. Under federal law, gift cards issued in electronic form for a specific amount cannot expire for a minimum of five years. Pay attention to a card's expiration date, especially if you plan to buy a gift card from a reseller.

If a gift card has no expiration date, it is generally valid until redeemed or replaced with a new card. Nevertheless, it's often best to use a gift card as quickly as possible to reduce its chances of being lost or stolen.

Keep in mind that a gift card that is branded by a credit card company and can be used almost anywhere may reduce in value faster than a single-store gift card.

There are a number of exceptions in the gift card laws. For example, gift cards for a specific service – say, one for a manicure (as opposed to a specified amount to a nail salon) – are not protected under federal law. Neither are "bonus" cards. Around the holidays, many businesses offer deals, such as "buy a $100 gift card, get a $20 gift card free." Although the $100 gift card would have all the protections the law offers, the $20 gift card would not be subject to the protections and could expire at any time. Closely check the expiration dates and other restrictions of any bonus cards.

Gift cards are often a scammer's payment of choice. For example, say you come across a legitimate-looking website advertising better deals than the sites of other stores. On the checkout page, however, the site requests the number of a gift card (not associated with the company) rather than a credit or debit card. Beware! Scammers may create phony websites — complete with made-up customer reviews — to trick people into revealing redeemable gift card information. Once the information is provided, any money loaded on the card will be lost.

When buying gift cards in a store, make sure that their PINs, generally found on the back of cards, aren't already scratched off or appear to have been tampered with. Some scammers go into stores, scratch off PINs, record the numbers, and put the cards back on the shelf. Then they check to see whether a consumer has purchased (or put any funds on) one or more of the cards. If a card has money on it, scammers then attempt to drain it. Some scammers even replace the security film sticker – which can be bought in bulk – so the PIN does not appear to have been exposed. Look for signs that the security film has been replaced (i.e. if it has been applied crooked or has air bubbles).

Be sure to take note of when the gift cards you purchase are expected to be delivered. Then track their delivery so the cards aren't snagged by mail thieves or accidentally disposed of.

Likewise, be careful when mailing gift cards to others. Consider taking those items directly to the post office instead of putting them in an unlocked mailbox to be picked up. Remember that once a thief has control of a physical or electronic gift card with the PINs, it may be very easy for the thief to redeem or transfer the full value of that card.

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.

Package Delivery Scams May Contain Malware

Fake shipping notifications are especially popular during the holiday season. With the increase in deliveries, the Federal Communications Commission (FCC) has fielded many complaints about delivery notification scam calls, texts and emails.

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 that asks for login credentials or other sensitive information.

Here are some tips to keep you safe from shipping and delivery notification scams:

- **Legitimate shipping notifications** will 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, be sure to 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.

In some cases, a link may open a website that prompts you to enter personal information, or it may install malware on your phone or computer that can secretly steal your personal information. The number you call back may be answered by a scam "operator" asking to verify your account information or the credit card number you used for a purchase. Other scam calls and texts may claim that you need to pay a customs fee or tax before the delivery can be made.

National delivery companies such as FedEx and UPS do not seek personal or payment information through unsolicited texts and emails.

Common warning signs of mail, text or online scams:

- Requests for personal and/or financial information.
- Links to misspelled or slightly altered website addresses, such as "fedx.com" or "fed-ex.com."
- Spelling and grammatical errors or excessive use of capitalization and exclamation points.
- Certificate errors or lack of online security protocols for sensitive activities.

Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. It seeks to invade, damage or disable computers, computer systems, networks, tablets and mobile devices by taking partial control over a device's operations.

Although malware cannot damage the physical hardware of systems or network equipment, it can steal, encrypt or delete your data; alter or hijack core computer functions; and spy on your computer activity without your knowledge or permission.

Signs of malware on your computer include popup ads, redirection to other sites, disabled tools and scary warnings from an unknown source.

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.