Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

December 2024

Last-minute holiday shoppers: Beware of scams

Last-minute holiday shopping is all but inevitable. These tips can help you make smart, secure purchases and avoid scams.

- **Do your research**.
    - Before buying, take a moment to research the product(s) you're looking for and current sales. Compare any deals carefully, checking ads for important exclusions or limitations. Restrictions might involve the number of sale items available or promotion times and dates.

- Read online reviews to learn about other shoppers' experiences, both good and bad. Check reviews on multiple websites to ensure credibility.

- Think and act skeptically if you find a hard-to-find item at a great price. Live by the maxim "If it sounds too good to be true, it probably is."

- **Keep cybersecurity in mind.**

  - When shopping online, don't use free public Wi-Fi; others may be able to view and capture your credit-card number and other sensitive information.

  - To ensure that a site is secure, look for the "s" in "https" in the address bar. Always make sure that the site you're on is the company's official site; knockoff sites often have small misspellings or variations in the web address.

  - Before making an online purchase, carefully review the expected delivery date and shipping costs. Also, use credit cards instead of debit cards or other payment methods because credit cards generally have more consumer protections.

- **Monitor your accounts.**

  - Regularly check your bank and credit-card accounts for unauthorized charges or unexpected activity. If you notice anything unusual, immediately notify your credit-card provider or bank. The sooner you identify a problem, the sooner you can work to correct it.

- **Watch out for business impersonation scams.**

  - Unexpected calls or emails claiming that you have purchased an item should raise a red flag. Verify unfamiliar "purchases" directly with the retailer using contact information from the company's official website.

  - Do not call back the number on your caller ID or the phone number mentioned in the message.

- **Be smart when buying gift cards.**

  - Ensure that the security film on a gift card hasn't been scratched or replaced. Scammers tamper with cards to steal funds.

  - Be sure to monitor the delivery of gift cards to prevent theft.

  - Mail gift cards directly from a post office; don't use an unlocked mailbox.

- **Don't be a victim to package-tracking scams.**

  - A package-tracking scam may involve an email alert informing you of a "delay" in the shipping of a package. The email either asks you to provide personal information or click on a link for additional information. Providing personal information, however, could lead to financial harm, and clicking on suspicious links can infect your device with malicious software.

- Keep both your shipping confirmation emails and a list of the retailers from which you've ordered.

- Don't click on links or download any attachments if you're unsure whether the sender is legitimate. If you have questions or want to verify an email supposedly from that shipper, contact the shipping company using the contact information on its official website.

One additional tip: Be sure to promptly retrieve delivered packages to prevent them from being stolen or damaged outside your door.

Consumers who believe they have been defrauded should immediately report the details and contact the company used to make the payment. Ohioans can report scams to the Ohio Attorney General's Office at www.OhioProtects.org or by calling 800-282-0515.

Tech toys for kids raise privacy, safety concerns

If you're shopping for internet-connected technology toys for kids, it is essential to understand the privacy and safety issues. Internet-connected toys range from wearable devices to interactive games and robots. To protect your child's privacy and safety, follow these tips:

- **Check age appropriateness**: Make sure the toy is suitable for someone of your child's age. For video games, check the content ratings provided by the Entertainment Software Rating Board (ESRB) at www.esrb.org.
- **Understand toy features**: Be aware of interactive features such as cameras, microphones and internet connectivity. Learn the default settings for each function.
- **Familiarize yourself with parental controls**: Parental controls should be included in the product. Under the Children's Online Privacy Protection Act (COPPA), parents may have control over what personal information the toy or app collects.
- **Do your research**: Check trusted sources, such as online parental blogs, for known security issues related to the toy.
- **Be present during setup**: If personal information is required, use nicknames or alternative details to reduce the risk of identifying your child.
- **Set privacy settings**: *Opt in* to safeguards, *block* access to chat rooms and *enable* parental controls. Regularly update the toy's software and check the settings.
- **Interact with the toy**: Learn how the toy operates. Discuss online safety, risky behaviors and in-app purchases with your child.
- **Use strong passwords**: Create unique, strong passwords for each account. Avoid connecting the toy to free public Wi-Fi, as it may be less secure than a home network. Always log out before shutting down the toy.
- **Establish rules for device use**: Discuss how to report inappropriate behavior online. Set house rules about where and when devices can be used, as well as limits on daily screen time.

For additional resources, the Federal Trade Commission offers free online publications to help keep kids safe online.

For more general cybersecurity tips, visit www.OhioAttorneyGeneral.gov and review the Cybersecurity Help, Information and Protection Program (CHIPP) booklet as well as Social Media Pointers for Parents.

Be careful where you click

The digital age has made life more convenient, with phones being used to pay for parking, view restaurant menus and much more. But such convenience comes with risks, as scammers exploit websites, emails, text messages, QR codes and other digital tools to steal personal or financial information.

Fraudulent QR codes are a growing problem. Scammers can place a sticker over a legitimate QR code to get you to a website where they can steal personal information, including your credit-card numbers.

The Better Business Bureau has reported that phony QR codes on parking signs have directed some consumers to scam websites when they try to pay. Also, if you scan a QR code that gives you a link to a spoofed site, that site could try to download spyware, ransomware or other malicious software to your device.

In any situation, if a QR code appears to have been tampered with or is covering up another QR code, *do not* click the link that the QR code populates. Always inspect the link generated by the QR code and, if anything seems amiss, *do not click it*.

For additional protection, consumers should consider downloading a QR code reader app on their device instead of just using a device camera to decipher the QR code. Some QR code readers warn users about websites that are likely designed by scammers.

Besides using phony QR codes, many fraudsters continue to send suspicious links via email or text message. Here are additional signs that correspondence you have received may be a scam:

- The link asks you for personal identifiable information.
- You are pressured to act immediately.
- Payment is sought by gift card, cryptocurrency, peer-to-peer payment (i.e. Venmo or Cash App), wire transfer or prepaid money card.
- You're told not to tell friends or family about a conversation or exchange.
- You're told that you've won something you didn't enter to win, or you're unexpectedly being given money.

Consumers who believe they have been defrauded should immediately report the details and contact the company they used to make the payment. Ohioans can report scams to the Ohio Attorney General's Office at www.OhioProtects.org or by calling 800-282-0515.

Stay social without being scammed

A social-media platform is any internet-based platform that allows users to interact, create, share or exchange information with others. Common social-media platforms include TikTok, YouTube,

Snapchat, Instagram, Facebook, BeReal and even certain gaming communities, such as Roblox and Minecraft.

Consumers use social-media platforms to connect with friends and family, get their news, follow celebrities, and buy and sell online.

Unfortunately, scammers also insert themselves into all aspects of social-media interaction. Here are some social-media scams to guard against:

- **Facebook messenger scams**: Scammers often use Facebook Messenger to send users requests for money or fake offers for loans or lotteries. If you do not know the person messaging you, ignore the message. If you recognize the person making the request, do not respond to the person via Facebook Messenger. Instead, contact that person using a method you know to be his/her direct contact information, such as a phone number or an email address, to confirm whether the request is legitimate.
- **Fundraiser scams:** After a major tragedy such as a mass shooting or natural disaster, it's common to see ads and posts from charities offering to aid victims. Some of these offers, however, might be scams. Bad actors falsely represent a charity or even use sound-alike names for their organizations. Before you donate to a charity, you should conduct an independent web search outside of the post. Be cautious about donating to newly created charities over those with a track record of dealing with disasters or community needs.
- **Romance scams:** Think twice before accepting friend requests from people you don't know. Accepting a friend request from a stranger can lead to a potential romance scam. The interactions might start innocently, perhaps with an offer of friendship or the trading of personal stories. If your new "friend" starts asking you for money or other gifts, though, it is likely a scam. Some scammers invest significant time in developing a romance to gain your trust and secure financial payments under false pretenses.
- **Job scams:** The adage "If it seems too good to be true, it probably is" applies to job scams. Scammers know that increasing numbers of people prefer to work from home. Some attempt to persuade you to apply for a job and turn over identifiable personal information by offering a job with a vague description and a too-good-to-be-true salary. To learn more about job scams, click here.
- **Online marketplace scams:** With millions of people using online social-media platforms to buy and sell goods, plenty of scammers work to take advantage of first-time or infrequent online shoppers. One telltale sign of a scam: The seller asks you to pay or communicate with him/her outside of the platform. Also, look for potential scams when a sale seems too extreme (for example, when the price of a popular product is drastically marked down) or when a very hard-to-find item is suddenly available through an unfamiliar site or a store based on social media.

The Federal Trade Commission suggests the following ways to steer clear of scams on social media:

- Limit who can see your posts and information on social media. All platforms collect information about you from your social-media activities; visit your privacy settings to set restrictions.
- If you get a message from a friend about an opportunity or an urgent need for money, call the friend. The friend's account may have been hacked. Note that scammers often ask for payment by cryptocurrency, gift card or wire transfer.
- If someone appears on your social-media platform and rushes into a friendship or romance, slow down. Learn more about romance scams. And never send money to someone you haven't met in person.

- Before you buy, check out the company. Search online for the company name and terms such as “scam” and “complaint.”

Consumers who believe they have been defrauded should immediately report the details and contact the company they used to make the payment. Ohioans can report scams to the Ohio Attorney General’s Office at www.OhioProtects.org or by calling 800-282-0515.