Ohio Attorney General's
Consumer Advocate
Newsletter
AUGUST 2018

August 2018

Ten Tips for Smart Back-to-School Shopping

With the new school year just around the corner, we're providing tips for the fall shopping season, including knowing when rain checks may apply, when "free" offers may cost you, and ways to avoid scams.

1. **Check the exclusions and limitations of an offer.** Exclusions and limitations must be clearly disclosed in advertisements, including online, so review terms and conditions carefully before you go to the store or make a purchase.

2. **Know that used items may not be sold as new.** Refurbished or reconditioned products must be properly labeled. For example, a company that sells electronics may not advertise or sell a computer as new when, in fact, it has been used or refurbished.

3. **Find out if rain checks apply.** If a seller advertises a product at a certain price but sells out of that product, you may have the right to a rain check. However, sellers are not required to provide rain checks if they clearly disclose the number of goods available at that price or if they clearly state that no rain checks will be given.

4. **Be cautious with trial offers.** Purchases sometimes come with free trial offers, such as free anti-virus software with the purchase of a computer, but signing up may subject you to additional purchases and payments. Trial offers vary, and some may be difficult to cancel or they may automatically renew. Always remain cautious when a trial offer requires you to provide your credit card number up front. Even if you're not charged immediately, you may be charged later.

5. **Know that free means free**. Under Ohio law, the cost of a "free" item cannot be passed on to the consumer by raising the regular price of the good or service. For instance, if a pair of shoes is normally sold for $50, a seller cannot run a buy-one-get-one-free sale and increase the cost of the shoes to $100.

6. **Understand return policies before you buy.** In Ohio, sellers can choose to set their own return policies, including policies of “no returns,” but they must clearly disclose the policy before you check out. Watch for any “restocking fees,” especially on electronic items. Ohio law does not prohibit these fees, but the business should clearly disclose any restocking fees before the purchase is made.

7. **Keep your receipts.** Maintaining a complete record of a sale will help you handle problems that may arise after the purchase. Keep receipts, copies of advertisements, photos of products, and other documentation until the transaction and billing process are complete.

8. **Stay safe online.** Research websites you plan to use, and make sure a website is secure before you enter any personal information or payment details. In the web address, look for the “s” in “https” and/or a lock symbol to help ensure a website has security features. Also consider paying with a credit card, which generally gives you stronger protections to dispute unauthorized charges.

9. **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.

10. **Watch for scams and identity theft.** Con artists operate year round. They may even run scams related to popular back-to-school items or services. Remember, if it sounds too good to be true, it probably is.

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.

New Electronic and Mobile Payment Methods

Consumers today often have a variety of options when it comes to paying for products and services – from cash and credit card to mobile wallets and peer-to-peer payment apps. As new methods are developed, it is a good idea to review the features and security of each method.

In addition to traditional forms of payment, such as credit cards, debit cards, bank checks, or cash, there are now other options and features.

We've grouped new electronic and mobile payment methods into three general categories — online banking, mobile wallets, and standalone payment apps — and we've listed factors to consider about each.

Online banking generally allows you to set your bank account to provide recurring payments to approved vendors. For instance, you might set up automatic payment plans for monthly bills, such mortgages, utilities, or loan payments, for convenience, to save on paper and postage, or to help avoid late fees for forgetting to pay bills. When using this feature, it is important to track your bank accounts to ensure you have enough money in an account when payments are debited.

Many mobile banking apps also allow consumers to send and receive money directly between banks. Some banks allow these transfers only between accounts housed within their banks, while other apps allow for transfers and receipts from any bank.

Mobile wallets generally allow you to carry and use your credit, debit, or gift card information in a digital form on your mobile device. Rather than carrying and swiping your physical card to make a purchase, you use your phone instead. Mobile wallet apps have the potential to be safer than credit cards if used with mobile-device security. For example, if you use a passcode or PIN to unlock your phone, that also can serve as a form of security needed to access the credit card or bank account information stored on your phone. The downside is that if all your financial information is stored on one device, if the app is hacked or you lose your device, the consequences could be severe. In other words, losing your phone could be like losing your wallet too.

Standalone payment apps generally store your payment information and allow you to pay a particular merchant or person using the app. For example, if your favorite restaurant has a payment app, it may allow you to order and pay for food at that restaurant through its app. Other standalone payment apps can give you the ability to conduct person-to-person transactions, such as paying a friend by transferring funds from your account to your friend's immediately.

When using online banking, mobile wallets, or standalone payment apps, be sure to understand the security features and risks of each. These payment methods are generally secure, but it's important to follow security protocols. For example:

- Maintain a strong password on your mobile devices and apps.
- Do not use free, public Wi-Fi to shop using any passwords or credit card numbers.
- Make sure the app you are downloading is the legitimate banking or mobile payment app, not an imposter with a similar name or look.

- Read the terms and conditions to see if there are fees associated with any of the payment services and whether transactions can be reversed or refunded.

- Always make sure the person you are paying is the actual person you want to receive the money. (Otherwise, if you send money in what turns out to be a scam, it may be difficult to recover your money.)

- Beware of “phishing” scams, or emails and texts designed to look like they are from your bank or mobile payment app that seek your personal or financial information. When in doubt, contact the company at a phone number that you know to be legitimate.

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.

Beware of Sweepstakes Scams

The thought of winning millions of dollars is exciting, but beware of common sweepstakes scams, including those that appear on social media.

Since Jan. 1, 2018, the Ohio Attorney General’s Consumer Protection Section has logged about 60 complaints about sweepstakes scams. Reported losses range from hundreds of dollars to tens of thousands of dollars or more.

Sweepstakes scams generally begin when someone unexpectedly contacts you and claims that you have won a prize. Many times, the scam comes in the form of a fake foreign lottery or a phony notice that appears to come from a well-recognized sweepstakes company. You are asked to send a fee to collect your winnings, but if you pay, the prize never comes.

Earlier this year, a Cuyahoga County resident reported being contacted by someone stating he had won $1.5 million and $450,000 from two separate sweepstakes, but he needed to pay “luxury taxes” to receive the prize. The consumer reported sending hundreds of thousands of dollars, pulling money from his retirement account, credit card, and loans. Despite being promised a large prize, he never received any money in return.

Many sweepstakes scams begin with a phone call or a letter, but they also can start on social media. Scammers may pose as “friends” on social media in order to gain trust. They then contact you via direct message saying that you’ve won money.

A Montgomery County consumer was contacted by a “friend” stating that he would have money coming to him if he first sent money to receive his prize. The consumer sent $2,000, only to find out that his real friend never contacted him and that the prize money did not exist.

To avoid sweepstakes and social media scams, remember:

- Legitimate sweepstakes or lotteries will not charge you to receive your prize.
- Con artists often ask their victims to send money using wire transfer, cash, or gift card, so be skeptical when asked to pay using one of these methods.
- In general: you cannot win a contest you did not enter; you cannot win a lottery unless you purchase a ticket; and U.S. citizens are not eligible to win foreign lotteries.
- Be skeptical if a "friend" sends you a message saying you've won a lot of money. The message may be part of a scam.
- Ensure that your anti-virus and anti-malware programs are up to date.

As with any unsolicited communication, research the offer before you consider replying. A quick internet search as to the legitimacy of the contest could prevent heartache and financial loss.

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.

Learn About Unlawful Robocalls

It can be frustrating to answer the phone and hear an automated telemarketing message, especially when your phone number is on the national Do Not Call Registry. Learning more about robocalls is the first step to controlling unwanted calls.

Generally, a robocall occurs when you hear an automated message instead of a live person when you answer your telephone. While there are some exceptions – such as calls from charities or political organizations – if you receive a call that is an automated message and you haven't given your written permission, that call may be illegal or part a scam. Even businesses with which you have a relationship are generally barred from making sales robocalls to your landline telephone unless you have given your written permission.

You may wonder why we are getting so many robocalls these days. As the Federal Trade Commission (FTC) explains: "Technology is the answer. Companies are using autodialers that can send out thousands of calls every minute for an incredibly low cost. The companies that use this technology don't bother to screen for numbers on the national Do Not Call Registry."

Unfortunately, finding out where an illegal robocall is coming from can be difficult. Many robocalls are made using internet technology that hides the caller's actual location. Scammers may use "spoofing" technology to trick your caller ID so that what appears to be a local call may be coming from across the country or around the world. For instance, calls from another country may appear to be coming from your own area code and even your own three-digit exchange. This is called "neighbor spoofing." Scammers use neighbor spoofing to increase the chances that you will answer the phone call.

Often, the best way to handle unwanted robocalls is to ignore them. Although it may be tempting to answer the calls or to press a key (supposedly to speak to a live operator or to be removed from the calling list), responding usually won't reduce the number of calls you receive. Instead, you may find yourself receiving even *more* calls once the caller knows they've reached a "live" phone number. If a call is important, the caller likely will leave a message.

Certain apps and other services can help stop robocalls calls from reaching you in the first place. The FTC recently announced an initiative to release the "robocall" phone numbers that consumers report to help companies that are attempting to block the illegal calls. Consumers' reports also assist law enforcement in efforts to find the perpetrators and help stop these unwanted calls.

If you receive illegal robocalls from a company that fails to identify itself, report those calls to the FTC at www.ftc.gov/complaint.

If you need help, or if you want to report a suspected scam or unfair business practice to the Ohio Attorney General's Office, visit www.OhioProtects.org or call 800-282-0515.