Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

Consumer Advocate
December 2019

Ohio Attorney General Offers Holiday Shopping Tips for Consumers

With the holiday season upon us, Ohio Attorney General Dave Yost offers the following holiday consumer protection tips:

- **Beware of e-skimming while shopping online**: Cybercriminals can capture credit card and personally identifiable information by skimming your data online. To avoid e-skimming, consider saving your credit card number to your browser so you don't have to enter it for every purchase. You will still need to enter the CVV number that is on the card to ensure that you physically have access to the card. Also, use credit cards instead of debit cards because credit cards have more protections. Look for the "s" in "https" to ensure the site is secure, and always double check that the site you're on is the legitimate site for the company.
- **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.
- **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 to 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 who you've ordered from, in addition to your shipping confirmation emails. Don't click on links if you're not sure who they are from.
- **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 should 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.

- **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 will charge you 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 that may 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 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 want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Frustrated with Unwanted Calls? AG Yost Continues to Aggressively Address 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.

Generally, a robocall occurs when you hear an automated message instead of a live person when you answer your phone. 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 you have a relationship with are generally barred from making sales robocalls to your landline phone unless you have given your written permission.

To help reduce the number of robocalls consumers receive, Attorney General Yost and 50 other attorneys general recently announced an agreement with 12 phone service providers – including Verizon, Sprint and AT&T – to adopt anti-robocall practices. The agreement will help protect consumers from illegal robocalls and make it easier for attorneys general to investigate and prosecute bad actors.

“This agreement brings phone service providers on board as critical allies in our fight against illegal robocalls,” Yost said. “By adopting these commonsense business practices, service providers will reinforce our ongoing efforts to crack down on this growing nuisance.”

Under the agreement, the service providers will work to prevent illegal robocalls by:

- Implementing call-blocking technology at the network level at no cost to customers.
- Providing customers with free, easy-to-use call blocking and labeling tools.
- Implementing technology to verify that calls are coming from a valid source.
- Monitoring their networks for robocall traffic.

Additionally, the companies will assist attorneys general with anti-robocall enforcement by:

- Knowing who their customers are so bad actors can be identified and investigated.
- Investigating and taking action against suspicious callers, which includes notifying law enforcement and state attorneys general.
- Working with law enforcement, including attorneys general, to trace the origins of illegal robocalls.
- Requiring phone companies with which they contract to cooperate and trace back identification.

Going forward, the phone companies will stay in close communication with the coalition of attorneys general to ensure that robocall protections develop as technology and scam tactics change.

The phone service providers that joined the initiative are AT&T, Bandwidth, CenturyLink, Charter, Comcast, Consolidated, Frontier, Sprint, T-Mobile, U.S. Cellular, Verizon and Windstream.

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.

Get a New Device? Beware of Activation Scams

With all the excitement of getting a new electronic gadget, some consumers don't realize when they're being tricked into paying fake activation fees by imposters posing as customer support agents.

The Better Business Bureau (BBB) has warned that scam artists can create phony customer service information and post it to the web, hoping that unsuspecting consumers will believe that a new policy requires a fee to activate a device. According to the BBB's Scam Tracker, consumers have been charged between $80 and $100 for this phony service.

For example, a consumer in north-central Ohio reported to the BBB that they found a phone number online to supposedly activate a Roku streaming device. A person posing as a customer service agent falsely informed the consumer that there was a $50 "lifetime activation fee," which the consumer paid with a credit card. In the end, the customer found out that the real Roku company had no record of the account.

According to a BBB scam alert, "Once payment is made, [the scammers] may claim there was a problem and second payment is needed. In some cases they may 'help' you come up with a new username and password, thereby gaining access to your device account. In any case, scammers hope to get away with your hard-earned money along with your personal information."

Here are three tips to help you avoid paying phony activation fees for your new device:

- **Watch out for phony websites and search engine listings:** Con artists are creating look-alike sites with addresses that closely resemble the legitimate websites affiliated with your new device. Some scammers actually purchase ads or sponsored links to make their phony information appear higher up in your search engine results. Be careful and only use the actual website and phone number listed in your new device's printed materials.

- **Beware of requests for payment via a prepaid money card, gift card or wire transfer service:** Scammers prefer these types of payment methods because consumers have little chance of recovering the money after it's sent.

- **Never give out your login information or allow remote access to strangers:** If you need help setting up your new device, only go to the official websites and tech support contacts listed in the device's printed materials. Be careful to spell URLs exactly as they're listed in the official documentation and be certain that you've dialed the correct customer support phone number.

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.

Phony Emails Request Purchases of Gift Cards for Boss or Pastor

Business Email Compromise (BEC) scams involve a con artist impersonating someone with decision-making authority by using a hacked or spoofed email account. Before contacting the targeted victim, the fraudster often does his or her homework by finding out the names and job functions of employees within an organization. They then use that information to impersonate an executive or another member of the leadership structure. This is done by hacking into their real business or personal email account or by making up a fake account with an address that resembles one an executive might really use.

According to a report issued by the Better Business Bureau, BEC scams are "skyrocketing" in number and have cost legitimate businesses and organizations more than $3 billion since 2016.

For example, imagine a local church that has its staff and pastor's email addresses listed on its website. Using this directory, a BEC scammer could impersonate the pastor and make up an email to send to someone with access to the church's funds, such as a treasurer or secretary. The scammer might, for instance, draft an email directing the secretary to buy gift cards for parishioners who are in need. This scheme might even be timed perfectly to be executed when the pastor is really out of the office, making it plausible that he or she might need the assistance of staff. After buying the gift cards and sending the numbers, the money is gone and in the hands of the scammer.

Another BEC scam scenario involves the sale of a home, where the scammer impersonates a real estate agent or title company employee. While playing the role of the agent or title employee, they could claim that money from the transaction needs to be wired ahead of time to a new account. But in reality, the account was set up by the scammer to receive the payment from the unsuspecting homebuyer, and the money is now gone.

Human resources staff for an organization are also at risk of being targeted by versions of the BEC scam. These employees may receive an imposter email from their HR director asking for employee tax information. Or, they may get a fake email that appears to be from a real employee, asking for future payroll to be sent to a new account by direct deposit. Unsuspecting HR staff might fulfill such requests, unintentionally helping the BEC scammer uncover personal information they can use in a tax identity theft scam or to steal money from the company.

Some tips to help recognize a BEC scam include the following:

- If you own a business or run an organization of any size, maintain a strong, secure network to help prevent hacking into your system.
- Use multifactor authentication for employees to log in to the network or change settings. Multifactor authentication can require employees to, for example, input a one-time access code sent to their smartphone. Requiring this code in addition to the correct password will help defend against intruders trying to gain access to the network.

- Require emailed instructions to be verified through a follow-up telephone conversation, especially for departments that perform financial tasks or handle sensitive information, such as employee data.
- Train all leaders and staff to know how BEC scams work as part of their internet/data security training.

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.