Consumer Advocate April 2020

AG Yost Warns of an Outbreak of Scams Related to Coronavirus

Fear and uncertainty surrounding the coronavirus pandemic could give rise to an outbreak of scams.

"COVID-19 is not the only thing we have to protect ourselves against," Ohio Attorney General Dave Yost said. "Thieves and crooks prey on fear and uncertainty. Ohioans need to inoculate themselves against an outbreak of scams with knowledge and good practices."

The Ohio Attorney General's Office has received a few calls from consumers reporting attempted scams related to COVID-19. One caller reported a twist on a recurring scam, the grandparent scam, where a scammer calls pretending to be the victim's grandchild in need of money. In this twist, the scammer called saying he needed money to get home because he was delayed in Philadelphia due to the pandemic. With many young people coming home from spring break, these calls may increase. If you receive a call from someone claiming to be a relative in need of financial assistance, do the following:

- Confirm with another family member this person is out of town or in need of assistance.
- Confirm the caller is who they claim to be by calling them back at a phone number you know to be their number.
- Ask the caller something only they would know the answer to, such as the alleged caller's birthday.

Follow these tips to avoid coronavirus-related scams in general:

• Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other expert sources with special advice or information about the coronavirus. Legitimate information is available for free on the <u>CDC's website</u>.

- Ignore online advertisements promoting cures for the coronavirus. According to the Federal Trade Commission, "There currently are no vaccines, pills, lotions, lozenges or other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19) online or in stores."
- Research nonprofit organizations and crowdfunding campaigns before donating. A <u>database of</u> <u>registered charities</u> is available on the Ohio Attorney General's website. Avoid groups that pressure you into donating and never donate via cash, gift cards, wire transfer or prepaid money card. These are the preferred payment methods of scammers.
- Be cautious of anyone going door to door offering coronavirus testing or temperature readings and requesting personal information. Call law enforcement immediately if you see a suspicious person. Never let strangers into your home.
- Beware of emails and other attempts to "phish" for your personal, financial and medical information. When in doubt, do not share. If the source claims to be your bank or a government agency, confirm they are legitimate by calling the organization at a phone number you have verified.
- When online, avoid clicking on unknown links or pop-ups and never download any suspicious email attachment. Doing so could infect your devices with malicious software designed to steal your personal information or lock your computer until you pay a ransom.

Consumers who suspect an unfair or deceptive sales practice should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

Follow These Legitimate Resources for Accurate COVID-19 Updates

Knowing where to go to for legitimate, accurate information about the COVID-19 pandemic and related issues can be challenging. There are many sources of information – from social media and blogs to newspapers and television. The Ohio Attorney General's Office offers these tips for Ohioans to stay up-to-date safely:

- For free, updated information about changes in the coronavirus pandemic, visit <u>the Centers for</u> <u>Disease Control and Prevention (CDC)</u> website. Reliable information is also available from the <u>World Health Organization (WHO)</u>. For updates closer to home, be sure to visit <u>Ohio's own</u> <u>coronavirus website</u> through the Ohio Department of Health.
- With so many electronic devices in use by Ohioans, this is a great time to review cybersecurity tips, precautions and warnings. The National Cyber Security Alliance has launched a helpful resource, the <u>COVID-19 Security Resource Library</u>, which has lots of information and links to

advice from organizations and agencies, such as the Federal Trade Commission (FTC) and the Cybersecurity and Infrastructure Security Agency (CISA).

- For updates regarding federal tax filings and changes related to COVID-19, visit the <u>Internal</u> <u>Revenue Service's coronavirus webpage.</u>
- The state of Ohio has extended unemployment benefits. To access or learn more about those benefits, visit the <u>Ohio Department of Job and Family Service's website</u>.
- Check legitimate media and government sources for updates about federal government payments to Americans amid the COVID-19 pandemic. Don't fall for scams that target your personal information under the guise of issuing you a pandemic-related payment. The government will never ask for any upfront payment and will not call you to request Social Security, credit card or bank account numbers.

At the moment, many companies are adjusting their normal policies. Always check their official website for accurate updates. You should manually type the company's website address instead of clicking links in emails from unknown sources. The website addresses for most governments and charities end in .gov or .org.

For an email sent by a company, hovering your curser over the sender's email address can reveal if the sender is not actually who they claim to be. If the end of the email address does not match the legitimate web address of the company, that is a red flag that the email might be from a scammer.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

Beware of Phony Work-From-Home Offers and Other Job-Related Scams

With the current economic conditions caused by the COVID-19 pandemic, many Ohioans are looking for work and may be tempted with work-from-home employment offers. Watch out because some job offers are actually scams.

Examples of phony job opportunities may include:

• **Mystery shopping**: A job seeker finds an offer to make money as a secret shopper. The first assignment is to receive and deposit a check, and then wire-transfer a portion of the funds to "evaluate" the transfer service. In reality, the job seeker will be wiring his or her own money to a con artist who has sent the job seeker a bad check.

- **Package processing**: A job seeker finds an offer to work from home for a logistics company by receiving and shipping packages, but the company is bogus and the job seeker won't make any money.
- Vehicle advertising: An offer online claims individuals can make hundreds of dollars a week by wrapping their car in an advertisement for an energy drink or other product. The individuals are told they need to provide payment before the ads can be placed on their vehicles, but in truth it's all a scam.
- **Babysitting**: A babysitter receives an offer to work for a couple who has not yet moved into town. The couple supposedly needs the babysitter to check out their new apartment, so the couple sends the babysitter payment in advance. They ask the babysitter to deposit the payment, withdraw as much as possible, then purchase prepaid money cards and provide the couple with the cards' numbers so they can provide the money to a rental agent. In reality, there is no couple or babysitting job; it's all a scam.

Regardless of the pitch, many scams follow a similar pattern. First, the scam artist sends a realistic check and asks the victim to deposit it. Once the check is deposited (but before it has cleared), the victim is told to wire or otherwise send a portion of the funds to someone else, possibly out of the country. Later, after the victim has sent his or her own money, the victim finds out from the bank that the deposited check was a counterfeit.

To avoid scams, Attorney General Dave Yost encourages job seekers to research the companies offering the work by contacting the Ohio Attorney General's Office and the local Better Business Bureau. Job seekers also can use a search engine to look up reviews by searching the company's name along with terms such as "complaint," "scam," or "review."

Signs of a potential job scam include receiving a check before any work is performed, claims about making hundreds or thousands of dollars doing very little work, vague job descriptions, requests to wire transfer money or purchase prepaid money cards, and interviews conducted strictly through a messaging system.

In terms of job placement services, some are legitimate, but others misrepresent their services, promote outdated or fictitious job offerings, or charge high fees for services that never lead to a job.

When researching job placement firms, the <u>Federal Trade Commission</u> recommends that you:

- Reject any company that promises to get you a job.
- Be skeptical of companies that charge first, even if they guarantee refunds.
- Get a copy of the firm's contract and read it carefully before you pay any money.

- Understand the refund or cancellation policy.
- Get all verbal promises in writing.
- Avoid high-pressure sales pitches that require you to pay now.
- Don't trust a firm that is reluctant to answer your questions.

Also research the company's reputation with the <u>Ohio Attorney General's Office</u> and the <u>Better Business</u> <u>Bureau</u> before you sign a contract or make a payment.

Keep in mind that you can find many legitimate job postings for free. For example, state job listings are available at <u>www.Ohio.gov</u> and federal job posts can be found at <u>www.usajobs.gov</u>.

Check With Your Lender Before Taking out a High-Interest, Short-Term Loan

As a result of COVID-19, many Ohioans are now facing unemployment or uncertainty about the length of their employment. In this environment, some people may look to short-term loans to cover immediate expenses.

Generally, short-term loans are between \$100 and \$500. The interest rates for short-term loans are typically very high, so these types of loans can be hard to pay back immediately. Ohioans may struggle to pay off the balance while covering other expenses. If the loan is extended, consumers will likely be charged additional fees, resulting in higher amounts of money owed.

When considering a short-term loan:

- Shop around. Before doing business with a particular company, check for complaints filed against it with the <u>Ohio Attorney General's Office</u> and the <u>Better Business Bureau</u>.
- Many lenders must be registered with the <u>Ohio Department of Commerce</u>. Verify that a lender is properly registered or licensed.
- Read and understand the terms and conditions of the loan. Check the payback dates and find out if you can make partial payments or if the loan must be paid off in one payment.
- Make sure you understand all costs, including interest rates. Be especially aware of any extension fees if you are unable to repay the loan within the original time period.
- If you don't feel comfortable with the terms of a loan, walk away.

Also consider alternatives such as:

- Working with a nonprofit credit counseling agency
- Identifying unnecessary short-term expenses
- Going to a bank or credit union for a short-term loan
- Borrowing from friends or family members
- The business community is aware of the drastic change in many Ohioans' finances and may offer payment programs and deferrals of payment that have not been offered previously. Check with your lender (mortgage, landlord, utility, credit card, personal loan provider) for pandemic-related payment programs before taking out a high-interest, short-term loan.

If consumers are unable to pay a bill on time, they should contact the business or credit card company as soon as possible to ask if they offer hardship or forbearance plans due to COVID-19. If an arrangement has been made between the lender and the consumer related to COVID-19 hardships and the consumer pays in accordance with that arrangement, the lender cannot report such payments as being late to the credit reporting agencies.

At the request of consumers, a lender may be able to add a code to the consumer's account that indicates they have been affected by the pandemic. That circumstance will be noted on the consumer's credit report until the lender removes it. The presence of the code can help minimize the impact to the consumer's credit score. Consumers can also contact credit bureaus directly to dispute information or to add a statement to their credit report explaining that they have been impacted by COVID-19.

Small businesses are also being affected by COVID-19 and may need help paying bills. Small businesses should follow the same tips as above, but they should also be mindful of fake grants. Scammers may pretend to offer grants for an up-front price; never pay up-front to receive grants.

If you suspect a scam or an unfair business practice, report it to the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.