Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

February 2024

Beware of job scams

Beware of job offers that seem too good to be true.

Many job scams promise high pay with minimal effort, but they often result in fraudsters obtaining the job seeker's personal information or access to their financial accounts. These scams may be advertisements on social media, email or text messages.

Many job scams use fake checks, where scammers send a check to cover equipment cost like a new computer. They instruct you to deposit the check into your bank account and then use a money-transfer service, gift card, or prepaid money card to send the same amount to a “vendor.” The check inevitably bounces, however, which means the money you sent to the fake vendor comes out of your pocket.

Before applying for any job posting, research the company thoroughly. Signs of potential job scams include the following red flags:

- The posting includes vague job descriptions and claims you can make hundreds or thousands of dollars doing very little work.
- Communication from company representatives uses free or personal email accounts, such as those from gmail.com, yahoo.com, hotmail.com or aol.com.
- You’re hired without ever meeting anyone in person.
- The company doesn’t have a website.
- You receive a check before any work is performed.
- You’re asked to wire-transfer money or purchase prepaid money cards.

Common scams include postal scams, mystery shopper scams, and offers for high-paying data entry jobs, often requiring upfront fees or sharing banking information.

Postal scams

Postal scams can be marketed as a convenient work from home opportunity. The job posting will list the job duties as repackaging and/or reshipping items. The compensation for the work is unusually high and even includes shipping costs. This “job” is actually a scam that allows the poster to use the applicant to ship stolen goods without receiving any compensation.

Mystery shopper. An applicant is selected for a “secret shopper” job and receives a check. The first assignment is to deposit the check and then wire-transfer a portion of the money to someone else using the wire-transfer service at a local retail store. In reality, the check the applicant has received is no good, and any money the person sends will be lost.

Running a web-based business. In exchange for an upfront fee from the applicant, a company promises to set up a web-based business that will generate income through

advertising revenue or products sold online by other businesses. The claims are false and no money will be generated for the applicant.

High-paying data entry jobs

Scammers often advertise illegitimate data entry jobs. The job description will claim you can earn high wages for minimal work. The job listing may require you to pay up front for job training or equipment. It also may require you to share your banking information prior to employment. If you see a data entry job offering a wage that seems much higher than the market average, investigate the company. Verify the company is posting this position publicly for the wage stated before responding to the job offer.

Job seekers should be sure to research the companies by contacting the Ohio Attorney General's Office and the local Better Business Bureau. Additionally, search engines can help find reviews by searching the company's name along with terms such as "complaint," "scam," or "review."

Consumers who need help resolving a complaint against a business, or 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.

Wise steps toward choosing the right tax preparer

You've likely received all of your 2023 tax documents, including W2 forms, and may be considering hiring a professional tax preparer. Choosing the right person is crucial. Here are some considerations:

First, determine, the type of professional you need. Tax preparers may be certified public accountants (CPAs), enrolled agents, or attorneys. An enrolled agent is a person who can represent taxpayers before the Internal Revenue Service (IRS). Enrolled agents, like attorneys and CPAs, are generally unrestricted as to which taxpayers they can represent, what types of tax matters they can handle and where they can practice.

Thoroughly research the preparer, as they'll have access to your personal information, including your Social Security number. Remember, you're ultimately responsible for the accuracy of your return.

The IRS recommends the following steps when selecting a tax preparer:

1. **Check the preparer's qualifications.** Use the IRS Directory of Federal Tax Return Preparers with Credentials and Select Qualifications. This tool – which is both searchable and sortable – helps taxpayers find a preparer with specific

qualifications. Remember: Any tax preparer should have a Preparer Tax Identification Number. Also, check out the preparer through the Better Business Bureau.

2. **Check the preparer's history.** Check for disciplinary actions and the license status for credentialed preparers. For CPAs, check with the State Board of Accountancy. For attorneys, check with the Supreme Court of Ohio. For enrolled agents, go to the verify enrolled agent status page on IRS.gov or check the directory.
3. **Ask about service fees.** Avoid preparers who base fees on a percentage of the refund or who boast bigger refunds than their competition. When asking about a preparer's services and fees, don't give them tax documents, Social Security numbers or other information until you've actually retained that person.
4. **Ask to e-file.** The quickest way to get your refund is to electronically file your federal tax return and use direct deposit.
5. **Make sure the preparer is available.** Contact your tax preparer as early as possible to make sure he or she has time to file your taxes before this year's deadline. Be wary of tax preparers offering inexpensive last-minute services.
6. **Provide records and receipts.** Good preparers will ask to see your records and receipts. They'll ask questions to figure things such as total income, tax deductions and credits.
7. **Never sign a blank return.** Don't use a tax preparer who asks you to sign a blank tax form.
8. **Review before signing.** Before signing a tax return, review it. Ask questions if something is unclear. You should feel comfortable with the accuracy of your return before you sign it. You should also make sure that your refund goes directly to you – not to the preparer's bank account. Review the routing and bank account number on the completed return. The preparer should give you a copy of the completed tax return.
9. **Ensure the preparer signs and includes the PTIN.** All paid tax preparers must have a Preparer Tax Identification Number. By law, paid preparers must sign returns and include their PTIN.
10. **Use *your* account.** If you are receiving a refund electronically through direct deposit, be sure that your routing number and account number are being submitted, not those of your tax preparer.
11. **Report abusive tax preparers to the IRS**. Most tax preparers are honest and provide great service to their clients. However, some preparers are dishonest. Report abusive tax preparers and suspected tax fraud to the IRS. Use Form 14157, Complaint: Tax Return Preparer. If you suspect a tax preparer filed or changed your tax return without your consent, file Form 14157-A, Return Preparer Fraud or Misconduct Affidavit.

Also, be sure to review the IRS' list of tax scams so you don't become a victim by losing money and/or personal information.

The Ohio Attorney General's Office advises consumers to file early in the tax season if possible. The sooner you file, the less likely it is that someone else can commit tax identity theft. Tax identity theft occurs when someone steals your personal information to file a tax return and fraudulently obtains your refund.

If you suspect a scam or an unfair business practice, contact the Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Dollar General settlement brings help to Ohioans

In November 2023, Ohio Attorney General Dave Yost announced that the bulk of a $1 million settlement with Dollar General would go to food banks or other hunger-relief organizations in each of the state's 88 counties.

Under an agreement reached between Yost's office and Dollar General, $750,000 of the settlement money was distributed to food banks for the purchase and distribution of food and/or personal-care items. Each county auditor chose the beneficiaries in his or her county to receive the funds.

Dollar General, a Tennessee-based discount retail chain with more than 980 stores in Ohio, charged more for some items at the register than the price marked on the shelves, and failed to adjust for the lower price when customers pointed it out.

County auditors conduct inspections at retail businesses to make sure products ring up at the correct price. The Dollar General case originated in Butler County, and many other auditors eventually uncovered similar errors upon inspecting Dollar General stores in their counties.

In addition to monetary relief, the settlement requires Dollar General to make various changes to ensure that its products ring up at the correct price:

- It must staff its stores sufficiently to keep shelf tags updated.
- If a consumer points out that the register price is higher than the shelf price, the checkout clerk must adjust the price to match the shelf tag; in addition, the shelf tag must corrected within 24 hours.
- District managers must conduct random price checks every 45 days.

- Stores that receive three “failed” auditors reports within six months must complete a full-store assessment and check the price of every item in the store to ensure accuracy.
- The company also must educate all employees about this policy and post signs in its Ohio stores informing customers of the same.

Ohioans who suspect unfair business practices should contact the Ohio Attorney General’s Office at OhioProtects.org or 800-282-0515.

The basics of virtual private networks: Is a VPN right for me?

Installing a virtual private network (VPN) is a wise step to ensure security and privacy while on the internet, whether at home or on the go. A VPN establishes a secure connection between an individual’s device and the internet, enhancing safety when browsing, shopping or working on any internet-connected device.

VPNs serve three primary functions: privacy, anonymity and security for electronic devices. VPNs help protect your personal data, passwords, credit card and banking information and browsing history -- all items that are vulnerable to being sold to others. Primarily utilized for remote access to private networks, VPNs enable secure connections to company intranets or restricted applications, particularly for employees working from branch offices or remotely from home. Without a VPN, connections are less secure when connecting to company networks remotely, traveling and accessing unencrypted websites.

VPNs are compatible with computers, tablets and mobile devices. Devices at home often use Wi-Fi by connecting to a router, so if you install a VPN on your router, every device that connects to your home network will automatically enjoy the VPN’s added layer of protection.

You can access your VPN anywhere with any device or operating system through a secure username and password. One of the benefits of a VPN is that you can have protected internet anywhere – at an airport, a hotel, a coffee shop, or anywhere else.

While it is still recommended that you not put personal information and passwords on any device relying on free public Wi-Fi, if you routinely use Wi-Fi outside of your secure home network, using a VPN may be a good fit for you.

Deciding whether a VPN is suitable for your needs involves consulting trusted acquaintances for their experiences with VPN products and conducting thorough research on companies. Check for any complaints filed with the Ohio Attorney General’s Office and Better Business Bureau and seek out online reviews using relevant keywords.

Regardless of VPN usage, adopting additional online protection measures is prudent.

- Create unique, long passwords (at least 12 characters) for each account and device.
- Use a password manager and regularly change your passwords. Password managers make it easy to maintain dozens of passwords securely.
- Turn on multifactor authentication (MFA) wherever it is permitted. This keeps your data safe even if your password is compromised. MFA generally requires something you know (for example, a password) and something you have (a cellphone to receive a special code or an email address).
- Turn on automatic device, software and browser updates, or make sure you install updates as soon as they are available.
- Use secured Wi-Fi.
- Use firewalls and anti-virus software on all devices.

Consumers who need help resolving a complaint against a business, or 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.

BONUS TIP YOU CAN USE

Did you know that the three major credit reporting bureaus – Equifax, Experian and TransUnion – have agreed to permanently let consumers access their credit reports for free on a weekly basis? Under federal law, consumers have long been able get a free credit report once every 12 months from each of the three reporting bureaus. During the pandemic, however, the reporting bureaus decided to let consumers check their credit reports once a week for free. That decision was extended twice by the bureaus and made permanent in late 2023. Credit reports are available at www.AnnualCreditReport.com.