Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

Consumer Advocate
June 2019

Attorney General Yost Warns of Travel Scams

Consumers should beware of travel scams during spring and summer vacation months.

Commonly cited problems include offers for free travel or vacations that are not truly free, travel services that don't deliver promised benefits and timeshare "resellers" who make false promises to consumers who are trying to sell their timeshares.

In Ohio, if a seller advertises that a consumer has won a free vacation or other prize, the advertisement must state important exclusions and limitations of the offer. For example, if a consumer is required to listen to a sales presentation about travel club memberships in order to receive a free cruise, that requirement should be disclosed in the ad.

Additionally, if a sale takes place outside a seller's normal place of business, such as at a hotel meeting room, the consumer likely is entitled to a three-day right to cancel the sale under Ohio's Home Solicitation Sales Act. Under this law, sellers must notify consumers of their cancellation rights.

To avoid problems with travel services, consumers should:

- Research companies before doing business with them. Look for complaints filed with the Ohio Attorney General's Office and Better Business Bureau. Search online for reviews using the company's name and words like "reviews" or "complaints."
- Get the details. Carefully review the terms and conditions of any agreement before signing.
- Make sure verbal promises are put in writing. Otherwise, they're not guaranteed.
- Consider paying with a credit card. You generally have stronger protections to dispute credit card charges if something goes wrong.
- Keep documentation. Maintain a copy of the contract or purchase agreement. If a problem arises, document the situation. For example, track the names of people you contact.

- Verify your reservations. If you book a trip through a third party, call the resort or hotel where you will be staying to confirm your reservation.

Questions to ask before signing up for a travel club membership include:

- Will you have to take several trips per year to get any savings?
- Do trips book up quickly, limiting your ability to schedule a vacation?
- Can you find similar or better deals yourself online?
- What is the cancellation policy?
- Are deposits refundable?
- Are there any non-refundable fees?
- Will you get a refund if a trip is canceled because of a natural disaster or bad weather?
- Will you have to pay an extra fee if you change your reservations or reschedule a trip?
- What's the total cost of the membership?
- Will additional fees kick in later, after you sign the agreement?

Consumers who suspect a scam or who have problems they can't resolve on their own should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515. The office provides a free informal dispute resolution process to help resolve complaints. It also takes enforcement actions against travel services that violate Ohio's consumer protection laws.

Learn the Red Flags: Don't Become a Money Mule

Some scammers rely on money mules to transfer money and avoid being detected. A money mule is someone who – often unwittingly – is recruited to launder money. Often the money laundering is based on a business or romantic relationship the money mule has with the scammer, who may be posing as a legitimate businessperson, employer or love interest. The money mule is being used to help the scammer commit fraud, so it is important to know the red flags and stay away from any unlawful and fraudulent activities.

Money mules are often recruited under the guise of "work from home" jobs. In a fact sheet called "Understanding and Protecting Yourself Against Money Mule Scams," the United States Computer Emergency Readiness Team (US-CERT) named eight warning signs that include commonly used tactics by scammers soliciting for money mules:

- The position involves transferring money or goods.
- The specific job duties are not described.
- The company is located in another country.
- The position does not list education or experience requirements.
- All interactions and transactions will be done online.
- The offer promises significant earning potential for little effort.
- The writing is awkward and includes poor sentence structure.
- The email address associated with the offer uses a web-based service (Gmail, Yahoo!, Windows Live Hotmail, etc.) instead of an organization-based domain.

Money mules are often recruited through online employment, dating, social networking and classified advertisement websites. According to the Federal Bureau of Investigation (FBI), money mules "help criminals and criminal organizations launder their proceeds derived from criminal activities, by adding layers of recipients to the money trail. These layers complicate and negatively impact the FBI's ability to accurately trace the money from a specific victim to a criminal actor."

Before considering opportunities to earn money, be sure to research the potential job online using the subject line of the email solicitation, the name of the organization offering the job, and either the name of the person who supposedly sent the email or the contact name associated with the opportunity. The Better Business Bureau can also be a valuable online resource during your research.

In its article "Don't Be A Mule," the FBI's Money Laundering, Forfeiture and Bank Fraud Unit provides the following indicators that you may be a money mule:

- You received an unsolicited email or contact over social media promising easy money for little to no effort.
- The "employer" you communicate with uses web-based services such as (Gmail, Yahoo Mail, Hotmail or Outlook).
- You are asked to open up a bank account in your own name or in the name of a company you form to receive and transfer money.
- As an employee, you are asked to receive funds in your bank account and then "process funds" or "transfer funds" via a variety of means to include: wire transfer, ACH, mail, or money service business (Western Union or MoneyGram).
- You are allowed to keep a portion of the money you transfer.
- Your duties have no specific job description.
- Your online companion, whom you have never met in person, asks you to receive money and, subsequently, forward these funds to an individual you do not know.

If caught, a money mule could receive jail time and be forced to repay victims through law enforcement and the justice system. The schemes can also ruin the money mule's credit and his or her ability to open

bank accounts. Money mules also might reveal personal information to the scammers, which could result in identity theft.

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.

Searching for Jobs? Be Careful Sharing Your Personal Information

Searching for a job can be stressful. Scammers often advertise in the same places where legitimate job placement services advertise. In order to protect your personal and financial information during your job search, do the following: know the signs of a scam, properly research job placement services and know what to do if you become a victim of a job scam.

Signs of a Jobs Scam

Here's how to identify a job scam:

- You need to pay to get the job. Employers and employment firms should never ask you to pay for certification, training materials or a placement fee.
- They ask for your credit card or bank account information during the job interview process.
- The advertisement is for a "previously unavailable" federal government position. Information about available federal jobs is free at www.usajobs.gov

Job Placement Services

Identifying legitimate job placement agencies with real employment opportunities can be difficult. Many job placement services are legitimate, but there are services that will charge you fees to gain access to jobs that have already been filled or that misrepresent jobs that are actually job training.

One of the most important things to know is whether the agency is offering job placement, counseling or training. Job placement is the service you are expecting if you want to be placed into employment. This involves being referred to a specific position for which you are qualified. Job counseling and training could be referrals to classes offered by the company to increase your interpersonal skills, or courses that may require payment for you to prepare for the position without any guarantee of being hired.

Here are a few tips before you engage a job placement service:

- If the placement service is acting on behalf of a specific company, check with that company first to see if they have hired a job placement service for the position you are seeking.
- Make sure to get all the details in writing of what the job service will provide.

- Research the company to see if it is merely a "lead generator." Lead generators are companies that collect your contact information and then sell it to marketing companies who use it to promote their own services.

- Check for complaints. You can search for the company's web address with the terms "review" or "complaint." You can also check with the Ohio Attorney General's Office or Better Business Bureau for complaints filed against the company.

If you become a victim of a job scam, you can do the following:

- Check your credit report at www.annualcreditreport.com or 877-322-8228 to make sure your personal financial information has not been compromised.

- Report the company to the Ohio Attorney General's Office at 800-282-0515 or the Federal Trade Commission at www.ftccomplaintassistant.gov

- Consumers who suspect a scam or who have problems they can't resolve on their own should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515. The office provides a free informal dispute resolution process to help resolve complaints. It also takes enforcement actions against companies that violate Ohio's consumer protection laws.

Password Managers Can Help Keep Online Accounts Safe

Many consumers get frustrated over constantly needing to come up with long, complex passwords for each of their online accounts. What has been a difficult process is made much easier through the use of a reputable password manager. In a nutshell, password managers require you to come up with one complex "master password." Then, the manager helps you log in to your various accounts using passwords the program can help you create and that you don't need to remember.

A password manager stores your login and password information for all the websites you use and helps you log into those websites automatically. The type of password manager that you use depends on personal preference and whether you want to pay for certain services or features.

The first step is to research your options and find which password manager works best for you. You can visit the popular app stores or consumer technology websites to find a variety of options. Read consumers' opinions online, ask friends and family for recommendations, and read reviews in technology magazines to explore your options.

While some password managers may require a fee-based subscription – especially to access advanced features – most of these services offer free trials to help you get started. There are password managers that offer optional family plans so you can have multiple users sharing the benefits. Also, some password managers can sync across multiple gadgets and work with mobile devices so you can hit the road with the benefits of the password manager.

So, what are the chances that a hacker will guess your master password or gain access to everyone's master password if there is a data breach? There is always some risk, but the good news is that some password managers encrypt your password information. While some password managers store your "vault" of passwords in the cloud (through the company's servers), other password managers can store your information locally (on your device itself). Keep in mind that two benefits of cloud storage are 1) if your computer crashes, your passwords will survive; and 2) you can easily sync among multiple devices.

Also, some password managers use "two-factor authentication." Two-factor authentication is a security process in which the consumer provides two different authentication factors to verify themselves. Two-factor authentication methods rely on you to provide a password as well as a second factor, usually an email or text message verification code. This will better secure your passwords through the password manager program.

With some password managers, you must remember your master password. Forgetting the master password means you might have to reset all your accounts' passwords individually. Some password managers can give you a password hint or a method to reset the master password. In any event, some experts recommend writing down your master password and keeping it in a safe location.

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.