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

Consumer Advocate
April 2019

Warm Weather Brings Out Home Improvement Scammers

With warm and stormy weather comes less-than-reputable home improvement contractors who go door to door seeking your business. They may tell you they have extra materials from a nearby job and can offer a special deal because they're already in the neighborhood. Although a few of these stories may check out, others are ploys to take your money and do little or no work.

Often, home improvement scammers will ask for large down payments. After collecting payment, some simply take the money and run, leaving homeowners with no repairs and no refund. Then they move on to another community to repeat their routine.

Last year, the Economic Crimes Unit of the Ohio Attorney General's Office was appointed by the Washington County prosecutor to handle a case against Anthony Combs, a man accused of scamming more than $200,000 from 34 homeowners in Ohio and West Virginia. Combs and his company, AMC Remodeling, offered roofing services to consumers, many of them elderly, in the Belpre area. After taking thousands of dollars, Combs failed to deliver the agreed-upon services or provide refunds. In May 2018, he was sentenced to four years in prison and ordered to return $205,000 to his victims.

Follow these tips to help avoid becoming a scammer's next victim:

- Before signing a contract or making a payment, check a company's reputation with the Ohio Attorney General's Office and the Better Business Bureau. Conduct an internet search for the business and the names of individuals involved.
- Do not make a large down payment. Instead, pay in increments – for example, one-third at the beginning of the job, one-third after half of the work is completed to your satisfaction and one-third when the job is completed.
- Avoid paying in cash. It leaves you with a limited paper trail when something goes wrong.
- Get any promises the contractor makes in writing.
- Be cautious of contractors who want payment made out to themselves as individuals, instead of a company.

- Understand that Ohio's Home Solicitation Sales Act provides consumers with a three-day cancellation period for most contracts signed at their own home, including many home improvement contracts. The law also applies to contracts signed at any location that is not a company's normal place of business (such as a home improvement show).
- Look for the red flags of a traveling scam artist. If a contractor claims to have leftover materials from a nearby job or offers unbelievably low prices, be suspicious.

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.

Attorney General Yost Honors Winners of High School Consumer Video Contest

Ohio Attorney General Dave Yost announced the winners of the 2018 Take Action Video Contest, which was open to Ohio high school students.

For the contest students were asked to create a 60-second video about one of the following telemarketing-related topics: the National Do-Not-Call Registry, dealing with illegal robocalls or using technology to stop unwanted calls.

Attorney General Yost congratulated the following winners:

- **First place:** Melissa Farthing, from the Medina County Career Center in Medina, will receive a $2,500 college scholarship for her video "Just Hang Up: Robocall PSA."
- **Second place:** Rebecca Haywood, from Wadsworth High School in Medina County, will receive a $1,500 college scholarship for her video "Homework Call."
- **Third place**: Gracie Bennett, from Notre Dame Academy in Toledo, will receive a $1,000 college scholarship for her video "Keep Your Time and Information Safe – Register Today!"

"Congratulations to our three winners, who found creative and entertaining ways to share important and helpful information about consumer protection," the attorney general said. "I appreciate their hard work, and also thank all the students and advisers who participated in the Take Action Video Contest."

The contest drew more than 60 entries from nearly 100 students statewide.

In addition to the first-, second- and third-place winners, Attorney General Yost recognized the following finalists:

- Andre Young, Twinsburg High School in Summit County
- Valeria Grajdianu, Mentor High School in Lake County
- Levon Howard and Connor Rose, Bellefontaine High School in Logan County

- Monet Paul, Mentor High School
- Zachary Just, Wadsworth High School
- Logan Willis, Mentor High School
- Tony Nguyen, Westland High School in Columbus

Consumers who want to learn about consumer protection should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Extortion Emails Demand Payment From Consumers

Consumers throughout the country are receiving emails claiming that their computers have been hacked and that their online activity will be made public unless they pay money. What is so alarming to unsuspecting consumers is that scammers often provide an actual password previously used by the victim as "proof" that the account is hacked.

If you've received one of these extortion-type emails, don't be alarmed. Realize that the email is likely part of a widespread scam and that the "hacker" probably doesn't have any evidence of your online activity. Typically, the password disclosed to you is an old password obtained through a previous data breach.

Consider visiting a site such as haveibeenpwned.com, where you can conduct free searches of known data breaches to see whether your email address and potentially other personal information have been leaked. If you find that you are a data breach victim, your password might have been discovered through data from one of those online breaches and then used to scare you through the extortion email scam. This is why it is always a good practice to change your password after a data breach and to use unique passwords for every account. Of course, if you haven't already, change your password for any accounts that the hacker knows.

Here are some related tips for creating and using passwords effectively:

- **Always use a unique and complex password for each account,** and do not switch back to passwords you have used previously. Using the same password for email, social media, banking and credit card accounts makes it easy for cybercriminals to cause serious damage in little time. A study by the University of Illinois suggests that three in five people use the same password across multiple online accounts, which means cybercriminals have plenty of opportunities to cause harm.

- **Use strong passwords or passphrases.** All passwords should be at least 12 characters long (the longer, the better) and include random special characters, letters and numbers. You may want to think of passwords based on a phrase that uses a combination of letters and numbers. For example, "My dog's name is Brutus" plus a random number creates the password "MdniB239."

Or, try using a passphrase instead. A passphrase is a sentence or combination of words that is easy to remember but longer and more complex than a traditional eight- to 12-character password.

- **Try a reputable password manager.** If you have trouble remembering passwords or don't have the time to put together a variety of passwords, try using a password manager. A password manager stores your login and password information for all the websites you use and helps you log into those websites automatically. The password manager encrypts your password list with a master password, which is the only password you have to remember. The type of password manager you choose will depend on your personal preference and whether you want to pay for additional services or features. Research your options to learn which password manager works best for you.

- **Keep your passwords safe.** Never keep passwords written on a list that you keep with your computer or mobile device. Avoiding this common mistake will keep your personal information safer if your device is lost or stolen. If you prefer to write down your passwords, store them away from your computer in a safe or a safety deposit box that only you and someone you trust can access.

- **Don't store your passwords in an unsecure location on your computer or mobile device.** Many people keep their passwords in a single Word document, Excel spreadsheet or other unsecure location on their computer. Don't do this. Cybercriminals know that passwords are frequently stored in these files, and they often look for such files when they first break into your computer.

- **Consider using "two-factor authentication" for your online accounts, where it is available.** Two-factor authentication is a security process in which users provide two distinct authentication factors to verify themselves. Two-factor authentication methods require users to provide a password as well as a second factor, usually an email or text message verification code, that is sent each time they try to access their accounts. This better secures your online accounts.

Also, be sure to disable any automatic login functions on websites, and always log off from every website and account when finished.

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.

Social Security Scams Hit Ohioans

If you've recently received a call from someone claiming to be with the Social Security Administration, you're not alone. The current Social Security scam is a version of the impostor scam, which involves

scammers representing themselves as government employees in order to access your personal and/or financial information.

Typically, the scam starts when a consumer receives a call out of the blue from someone claiming to be from the Social Security Administration. These callers may ask you to confirm your Social Security number, ask for additional personal information to increase your benefits or even threaten to withhold your benefits unless you provide additional information.

It is important to know that Social Security officials will never call you and threaten to terminate your benefits, nor will they ever state that you will face potential arrest or other legal action if you fail to provide information or pay a fee.

Be sure to follow these tips to avoid falling for the Social Security impostor scam:

- Never provide personal information, such as your Social Security number or bank account details, over the phone or internet unless you are certain the request is from a legitimate source. In general, the Social Security Administration and the IRS will not contact you via phone.
- Whenever you are in doubt, contact the government agency at a phone number you know to be legitimate. This will help you verify whether the request is real or part of a scam. Don't call back using caller ID information because scammers can use spoofing technology to put whatever phone number they choose on your caller ID screen. To reach the Social Security Administration, you can call 800-772-1213. To reach the IRS, the legitimate phone number is 800-829-1040.
- Don't try to keep the Social Security scammer on the phone or otherwise engage the con artist. It is best to simply hang up and report the scam to the Office of the Inspector General of Social Security by calling 800-269-0271 or by submitting a report on the OIG website: https://oig.ssa.gov/report.

Consumers who believe that they have been treated unfairly or are the victim of identity theft should contact the Ohio Attorney General's Office at 800-282-0515 or visit www.OhioProtects.org.