



Ohio Attorney General's
**Consumer Advocate
Newsletter**

OCTOBER 2016

Scholarship Contest Now Accepting Entries!

The Ohio Attorney General's eighth-annual Take Action Video Contest gives Ohio high school students the opportunity to learn about consumer protection while creating a short video for the chance to win college scholarships.

The top three winning individuals or teams will receive college scholarships of \$2,500, \$1,500, and \$1,000, respectively, and their videos may be featured on the Attorney General's website.

To enter the contest, Ohio high school students (grades 9 through 12) must produce and submit a 60-second informational video on one of the following topics:

- Imposter scams
- Cybersecurity
- Importance of checking your credit report

The deadline to submit a video is Dec. 9, 2016. Winners will be announced in March 2017 during National Consumer Protection Week.

Visit www.OhioAttorneyGeneral.gov/TakeActionContest to view last year's winning videos, the official guidelines, and the 2016 Take Action Contest flier. Teachers are encouraged to print out and display a copy of the flier in their schools.

Contest questions should be directed to ConsumerOutreach@OhioAttorneyGeneral.gov.

Beware of Computer Repair Scams

October is National Cybersecurity Awareness Month, and it's a good time to catch up on the latest computer repair and tech support scams that can trap consumers into revealing personal information or paying for phony assistance with their digital devices.

Many Ohioans have reported a common variation of the scam – receiving unexpected telephone calls from con artists pretending to be affiliated with Microsoft, Windows, or a legitimate-sounding tech support or anti-virus software company.

In this scam, the caller claims the consumer's computer has been infected by a virus or other malicious software. The caller attempts to convince the consumer to pay to have the "problem" fixed. Ultimately, the scammers request remote access into the consumer's computer, supposedly to install antivirus software to resolve the issues. (Remote access allows someone to gain access to a computer through the Internet and free downloadable software.)

Consumers who fall for this scam face at least two potential problems. First, they likely have provided their credit card information to the scammer and paid for an unnecessary or worthless service. Second, by allowing remote access into their computer, they may have compromised any personal information stored on their device and opened the door to malware being loaded onto their computer by the con artist.

While the scams often begin with a phone call, con artists also use other methods to try to dupe Ohioans into falling for a computer repair or tech support scam.

In some cases, consumers receive warning messages on their computers stating they have a virus or other serious problem. The message often looks official and includes a telephone number to call for tech support. Upon calling, the consumer is persuaded to let the scammer "fix" the issues for a price, often hundreds of dollars.

Other consumers have searched online for computer help and have ended up contacting a scammer who had placed a legitimate-looking advertisement designed to lure unsuspecting consumers. They pretend to offer computer repair services, but they never provide any real help. Instead they work to gain access to consumers' money or personal information.

Follow these tips to help steer clear of potential computer repair and tech support scams:

- **Guard your personal information.** If you receive an unexpected computer repair call, never provide personal information, allow the caller to access your device, or purchase software the caller may be selling. The best course of action is to hang up the phone immediately.
- **Beware of pop-up messages.** Know that scammers may use scare tactics such as full-screen warning messages or pop-up advertisements cleverly disguised as official-looking virus warnings. Never click on suspicious links or pop-up advertisements. Do not contact toll-free numbers contained in these messages or ads.
- **Know where to find real help.** To find legitimate computer repair help, look through the tech support information found with your security or antivirus software package, contact your Internet Service Provider, or locate documentation from your computer manufacturer. You may want to talk to friends and family for referrals and find out if a local computer repair service is available in your area.
- **Dispute unauthorized charges.** If you have used your credit card to pay a scam artist, contact your credit card company right away to have the charges reversed and your accounts protected.

- **Beware of phony refund offers.** Scam victims should be extremely cautious of any telephone calls claiming to offer a refund, even if the offer comes months after the initial scam. The supposed refund may simply be another scam, where a con artist pretends to offer compensation, asks for the consumer's personal information (such as credit card or bank account number), and then makes unauthorized withdrawals from the consumer's account.

Warnings about computer repair scams are part of the Attorney General's new "Ohio Protects" initiative, which aims to help Ohioans recognize and avoid scams. The campaign includes three 30-second videos that use humor to help convey messages about scams using the tag, "It's never this obvious." The videos, including one about the computer repair scam, can be viewed on the Ohio Protects microsite at www.OhioProtects.org/Videos. Closed captioning is available in English and in Spanish.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioProtects.org.

Scammers' Favorite Payment Methods

Fraud can be difficult to detect, but recognizing payment methods used regularly in scams can help consumers spot one sign of a potential problem.

Scammers, including those in faraway locations, often request payment using one or more of the following methods:

- Wire or money transfers,
- Prepaid money cards, or
- Gift cards

Scammers often choose these payment methods because once they receive the money, it is virtually impossible for consumers to trace or reverse the charges. Whether it's a wire transfer, a reload card, or a gift card, avoid using these types of payment methods when conducting a transaction with a stranger to protect yourself from scams.

Some con artists also use fake checks, trying to pass off a counterfeit business or cashier's check as legitimate. The scammer devises a clever story to trick consumers into depositing the worthless but legitimate-looking paper check in order to convince the consumer to wire funds or provide prepaid cards in return. For example, a con artist may "hire" a consumer for a job and then send the consumer a (phony) check for \$200 more than expected. The con artist asks the consumer to return the extra money right away by sending a wire transfer for \$200. Again, the request for a wire transfer is the consumer's clue to end the conversation.

The Federal Trade Commission (FTC) recently amended the Telemarketing Sales Rule to prohibit telemarketers from accepting certain payment methods often used by con artists. For example, the rule

bans telemarketers from requiring payment through a wire or money transfer, which allows the transfer of cash from a consumer in one location to a person or business in another location. Western Union and MoneyGram are examples of companies that provide these “cash to cash” services.

Under the revised telemarketing rule, other banned payment methods include certain cash reload mechanisms like MoneyPak, Vanilla Reload, and Reloadit, which essentially act as prepaid debit cards. Once the card and/or PIN numbers are given to someone else, that person can wipe all the money off the card. (Major providers of cash reload products now use a “swipe reload process,” which the FTC says is a safer method not affected by its new ban.) The rule also prohibits telemarketers from using “remotely created checks” to withdraw money directly from consumers’ bank accounts.

Consumers who question the legitimacy of a telemarketing call can check the Ohio Attorney General’s website to see if the caller is registered as a telemarketer in the state. However, there are exceptions regarding who needs to be registered in Ohio. Consumers also can look up charities on the website to see if a call is coming from a charitable organization registered with the Ohio Attorney General’s Office.

If you have questions or if you suspect a scam, contact the Ohio Attorney General’s Office by calling 800-282-0515 or visiting www.OhioProtects.org.

Know Your Consumer Rights – Repairs and Services

If you own a home or motor vehicle, you likely have paid for repairs or services in the past, or you may be planning to pay for repairs or services in the future. To make the most of your money, understand your rights as a consumer.

Ohio’s Consumer Sales Practices Act helps protect consumers from unfair and deceptive sales practices, including those involving repairs and services. Under Ohio’s Repairs and Services Rule, consumers have certain rights, such as:

- **Right to a verbal or written estimate.** Upon request, Ohio consumers have the right to a verbal or written estimate for repairs and services that will cost more than \$25 (or more than \$50 for motor vehicles). The estimate must include a description of the work that will be done, the anticipated date of completion, and the expected cost.
- **Authorization for cost increases of more than 10 percent.** In general, if a repair will cost more than 10 percent of the original estimate, the business must get the consumer’s authorization for the additional cost. Information concerning other related charges, such as pickup and delivery or diagnostic work, also should be made available to the consumer.
- **Itemized list of tasks performed.** If the customer requests it, the business must provide an itemized list of the tasks it performed. Additionally, the business must return all replaced parts, unless there is an agreement with the consumer to reuse or rebuild them or to send them to the manufacturer according to the warranty.

Before you hire someone to perform repairs and services, ask family and friends for recommendations. Gather information about businesses and how they have handled consumer complaints from the Ohio Attorney General's Office and the Better Business Bureau.

For vehicle repairs, verify that the repair shop is licensed with the Ohio Board of Motor Vehicle Repair. Before deciding which repair shop to use, consider getting at least three estimates from different repair shops to compare prices, services, and guarantees. Ask about guarantees up front and get all guarantees in writing. Remember: if a guarantee is not put in writing, it is not a guarantee.

Also, make sure the shop will honor any warranties and find out what the warranty will cover. Ask if the facility uses new, reconditioned, or spare parts, and keep copies of all estimates, invoices, work orders, receipts, guarantees, and warranties.

Be sure to read future issues of the "Consumer Advocate" for more articles in the "Know Your Consumer Rights" series. To report a scam or unfair business practice, contact the Ohio Attorney General's Office by visiting www.OhioProtects.org or call 800-282-0515.