Ohio Attorney General's
Consumer Advocate
Newsletter
APRIL 2013

Consumer Videos Now Available

The Ohio Attorney General's Office now offers several new videos on consumer protection topics. Watch as Consumer Protection Section experts discuss home improvement, identity theft, and other issues, and check out the winning student videos from the office's 2012 Take Action High School Video Contest.

To view all Attorney General videos, visit the videos page of the office's website at www.OhioAttorneyGeneral.gov/Videos or its YouTube channel at www.youtube.com/user/OhioAttorneyGeneral.

In March, the Consumer Protection Section recorded a video tip of the day in honor of National Consumer Protection Week. The section also recognized the winners of the 2012 Take Action Contest, a scholarship competition open to all Ohio high school students in grades 9 through 12.

The office received 240 submissions from students of 50 schools in 26 counties. The three winning teams were:

- **First place:** Kayla Hanneman and Maclane Nugent, seniors from Pymatuning Valley High School in Ashtabula County. They will split a $2,500 scholarship for their video, "I Knew You Were Lion."
- **Second place:** Eric McGinnis and Jesse Braun, seniors from Normandy High School in Cuyahoga County. They will split a $1,500 scholarship for their video, "Please be Careful."
- **Third place:** Junior David Michael and senior Chance Davis of Dublin Coffman High School in Franklin County. They will split a scholarship of $1,000 for their video, "Stopping Scholarship Scams."

To view the winning videos and see a list of other finalists, visit the contest page at www.OhioAttorneyGeneral.gov/TakeActionContest.

Agent or Imposter?

Scammers have been posing as law enforcement officers for years, but current technology makes the scheme more convincing.

Several consumers recently reported phony debt collection calls from alleged BCI agents or other law enforcement officials within the Attorney General's Office. The calls are scams — no one from the Attorney General's Office will threaten you demanding that you pay a debt — but phony calls can be believable.

For example, a Delaware County consumer received a call from someone claiming to be from the Attorney General's Office. The caller told the consumer she would be arrested within 45 minutes if she did not pay the $1,300 she supposedly owed on a payday loan. The caller told the consumer to

buy a prepaid money card to pay the debt. Fortunately, a store employee stopped the consumer before she purchased the card, so she did not lose money.

Another consumer was not so lucky. She received a call from the "Law Enforcement Bureau of Criminal Investigation" and was told she owed $536.48 on a payday loan. Because the consumer was threatened with arrest, she bought a prepaid card and gave the scammer the card's number. She lost her money.

Although the imposter phone scam is not new, current technology can make the ploy more convincing. For instance, scammers can "spoof" or disguise the number that appears on an individual's caller ID. The call may appear to be coming from a local government entity with a local area code, but in reality, it could be coming from a scammer in another state or another country.

In Greene County, Clerk of Courts Terri A. Mazur recently warned residents that scammers were cloning (or spoofing) the Clerk of Courts' phone number. When consumers received one of the scam calls, the court's phone number appeared on their caller ID.

In one case, a Greene County resident received a call and saw the Clerk of Courts' phone number on his caller ID. When he answered the phone, the caller demanded that he pay money or risk being arrested. In the background, he heard the caller saying, "I'm talking to him now, so don't go to arrest him." In reality, the call was a scam.

If you receive a call from someone claiming to be a government official and that person is threatening to arrest or harm you, it is likely a scam. Follow these tips to protect yourself:

- Remember that the Attorney General's Office will not call and threaten to arrest you.
- Don't trust the number that appears on your caller ID. It may be a spoofed phone number.
- Don't give out personal or financial information to anyone who contacts you unexpectedly.
- When in doubt, hang up and call a number that you know to be legitimate, such as the Attorney General's Help Center, 800-282-0515.
- If you are receiving debt collection calls, ask the caller to send written verification of the debt. If you don't receive verification, you likely do not owe the debt.

To learn more, or to report a potential scam, contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.

AG Shuts Down Fraud Ring

In March, Ohio Attorney General Mike DeWine and Miami County Prosecutor Gary Nasal announced the guilty plea of the ringleader of a telemarketing fraud scheme that stole millions of dollars from thousands of victims across the country.

The plea was a major victory for the Consumer Protection Section's Economic Crimes Unit, which works with local law enforcement and prosecutors to investigate and prosecute consumer fraud of a criminal nature.

Victims in the case, many of them elderly, owned inexpensive, vacant land throughout the United States. Members of the telemarketing ring targeted the elderly victims, claiming they could sell their land. They told victims their land was worth up to 15 times its assessed value and that they had eager buyers who wanted to purchase the land.

Property owners were told to pay fees as high as $16,000 to guarantee the sale of the land for the inflated value. Other victims were told that a solar energy plant had agreed to purchase their land for the overstated price, but in order to finalize the sale, they had to pay closing costs. Ultimately, there were never any buyers, closings, or sales. In all, the enterprise defrauded people in 41 states out of more than $2.8 million.

Based in Miami County, the criminal ring began operating in 2007. It involved 18 individuals, and of those, 15 have been convicted so far.

The Economic Crimes Unit discovered the scheme and led the investigation with extensive cooperation from law enforcement agencies in Ohio and Florida, the Florida Attorney General's Office, and the U.S. Postal Inspection Service.

To learn more or to report potential fraud, contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.

'Spear Phishing' Scams Hit Close to Home

In a typical phishing scam, a con artist pretends to be an employee of your bank or a government agency and asks you to confirm account information by submitting your bank account number, password, or Social Security number. The scammer hopes you will fall for the scam and reveal personal information.

Spear phishing is a more targeted form of this scam. Instead of sending a general message asking for verification of your account information, the scammer crafts a targeted message, using information he has learned about you.

For example, a scammer may hack into your e-mail account and find information about your financial planner and accounts. The scammer then sends an e-mail to your financial planner (using your e-mail address) and asks the financial planner to transfer $9,000 to another account. If the financial planner complies with the request, your money will be lost.

According to the FBI, criminals need some inside information to make spear phishing scams seem legitimate. They may obtain information by hacking into a computer network or by finding information online through social networking sites, blogs, or other websites. With this information, they can send realistic e-mails to potential victims.

To avoid spear phishing scams, follow these tips:

- Create complex passwords. Use a variety of characters and make your passwords lengthy.
- Do not use the same password for multiple accounts. For example, do not use the same password for your e-mail account and your online banking account. Create a unique password for each account.
- Keep your security software up to date and use a phishing filter, if possible.
- If your e-mail account is hacked, contact your e-mail provider. If the hacker may have gained access to your personal information, contact the appropriate organizations, such as your bank.
- Do not share too much information online. Be mindful of the information stored in your e-mail account and how much sensitive information you transmit via e-mail or social networking.
- Be careful where you click. When in doubt, do not click on links contained in e-mail messages.

- Talk to your financial planner or bank about scams and what would happen if your accounts were hacked.

Report scams to the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.