Ohio Attorney General's
Consumer Advocate
Newsletter
OCTOBER 2017

October 2017

Scholarship Contest Accepting Entries

The Ohio Attorney General's ninth-annual Take Action Video Contest gives Ohio high school students the opportunity to learn about cybersecurity and a chance to win up to $2,500 in college scholarships.

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 cybersecurity topics:

- Privacy on your smartphone
- Social networking scams
- Creating strong passwords

The top three winning individuals or teams of two students 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.

The deadline to submit a video is Dec. 8, 2017. Winners will be announced in March 2018 during National Consumer Protection Week.

Visit www.OhioAttorneyGeneral.gov/TakeActionContest to view last year's winning videos, the official guidelines, and the 2017 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.

Protect Your Identity in the Wake of the Equifax Breach

There's no way around the headlines. Equifax, one of the country's three main credit reporting bureaus, suffered a data breach affecting some 143 million U.S. consumers. Despite this scary news, there are ways you can protect yourself.

Equifax said the information was compromised between May and July 2017 and includes names, social security numbers, birth dates, addresses and driver's license numbers. The data breach also included the credit card numbers of approximately 209,000 U.S. consumers.

"Data breaches involving Social Security numbers are especially serious," Attorney General Mike

DeWine said. “If your information has been compromised, take the time to understand what that means and how you can better protect yourself moving forward.”

To see if your personal information was impacted by the breach, visit www.equifaxsecurity2017.com. You will be prompted to enter your last name and part of your Social Security number, at which point Equifax will inform you if your information was involved in the breach.

Regardless of whether or not your information was accessed, Equifax is offering one year of free enrollment in “TrustedID Premier” for all U.S. customers if they enroll by January 31, 2018. TrustedID is a credit monitoring service that monitors all three major credit reporting bureaus, Equifax, TransUnion, and Experian, and provides consumers with copies of their Equifax credit report. You can sign up for this feature by visiting www.equifaxsecurity2017.com.

Tips for affected consumers include:

- **Check your credit report**. Monitoring your credit report can help you identify signs of potential identity theft. You are entitled to one free credit report per year from each of the three major credit reporting agencies. Visit www.annualcreditreport.com to access those reports. You can pull all three at once, or you can pull your reports throughout the year.
- **Place an initial fraud alert on your credit report.** Contact one of the three major credit reporting agencies — Experian, Equifax, or TransUnion — to place an initial fraud alert, which will stay on your credit report for 90 days. The alert is free and will make it more difficult for someone to open credit in your name.
- **Consider placing a security freeze on your credit report**. A security freeze essentially puts a lock on your credit so that most third parties can’t access your report. This helps protect you from unauthorized accounts being opened in your name. In Ohio, security freezes are permanent until you lift them. You can be charged a $5 fee per credit reporting agency to place or remove a freeze. Contact each credit reporting agency separately to place a freeze. Note that Equifax is offering a free “freeze” for one year with enrollment in their TrustedID program; however, this will not freeze your reports at Experian or TransUnion.
- **Beware of scams related to the breach**. Con artists may pretend to have information about the breach, or they may falsely claim to want to help you. Some calls or messages may be scams designed to steal your money or personal information. Don’t give out personal information to those who contact you unexpectedly (even if they say they want to help you) and be wary about clicking on links or downloading attachments in messages.
- **Monitor your bank accounts.** Look for suspicious activity. If you find errors, immediately notify your bank or credit provider.
- **When it’s tax season, consider filing early**. File your taxes as soon as you have all of the information necessary to file so there is less of a chance for someone to fraudulently file on

your behalf. This is especially important if you know your information has been compromised.

Signs of possible identity theft may include:

- Unexpected mail about accounts you did not open.
- Credit card charges you never made.
- Unexpected collection calls.
- Another person's name showing up in your background check or credit report.
- Credit reporting errors or a lower-than-expected credit score.

Victims of identity theft should contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioProtects.org. Please note that the Ohio Attorney General recommends checking your credit reports first, and then contacting the Ohio Attorney General's Office only if your information appears to have been misused.

When Caller ID Fails: Learn About "Spoofing"

Do you receive unwanted telemarketing or scam phone calls and wonder why your caller ID says many of them are right in your area code? It's called caller ID "spoofing;" a technology that is cheap and readily available to mask where the calls are originating.

Spoofing means scammers from other states or even other countries can spoof your caller ID to make you believe they are from, for example, a legitimate bank or government agency in your hometown. The Ohio Department of Health recently reported that scammers used caller ID spoofing to make calls appear as if they were coming from their office and a local health department. The scammers then requested personal information from the consumers.

Scammers may spoof the caller ID using an area code where they know the organization they are impersonating conducts business (such as a phony IRS agent using the 202 area code for Washington, DC). Calls may appear to be in your own area code and even use the same prefix as your own phone number.

According to the Federal Communications Commission (FCC), "Under the Truth in Caller ID Act, FCC rules prohibit any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongly obtain anything of value. If no harm is intended or caused, spoofing is not illegal."

The FCC requires telemarketers to display the phone number along with the company name, if possible. The phone number should be one that consumers can call back during regular business hours and ask to not receive future calls.

In addition to spoofed phone calls, news reports and recent complaints to the Ohio Attorney General's Office suggest scammers are sending phony bank text messages to convince consumers to disclose personal information. Consumers are instructed to reply or call an Ohio telephone number because of a problem with their account. The texts often appear to be from the "Huntington National Bank Help Desk" or the "Huntington Security Department." If the consumer returns the call, the scammer may try to get bank account or personal information like social security numbers.

Consumers can steer clear of scams by following these tips:

- Do not give out personal information, including account numbers, passwords, or social security numbers to unexpected callers claiming to be your bank, a government agency, or other legitimate business or organization. If you receive this type of call, hang up.
- If you think a caller may be legitimate, call the organization's telephone number as shown on your account statement, the back of your credit and debit cards, the company or agency's official website, or in the phone book.
- If you receive an unwanted robocall, do not push any buttons – even to "talk to a representative" or "opt out" – because that may only confirm to the caller that your phone number is valid and working. Instead of getting fewer calls, you may actually receive more.
- Place your landline and cell phone numbers on the National Do Not Call Registry (www.donotcall.gov, 888-382-1222) to help reduce telemarketing calls. Be sure to report any violations to the National Do Not Call Registry or the Ohio Attorney General's Office.

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.

Some Scams Targeting Apple Products and Users

October is National Cyber Security Awareness month, and the Ohio Attorney General's Office is warning users of Apple products that scammers are targeting them for personal information and money.

In one scam targeting Apple's iCloud users, con artists impersonate Apple's support team and call consumers to tell them their account has been hacked. Typically, these types of scammers will tell the consumer that allowing them access will restore their service. In reality, allowing them access will open the door to personal information that may be on your device or account.

In another scam, con artists that obtain stolen AppleIDs can reset the passwords and lock users out of their own devices. Typically, they will demand a ransom of about $100 in order for the

consumer to regain access. Another method of Apple ID theft occurs through legitimate-looking text messages that ask unsuspecting users to "confirm your Apple ID."

A consumer recently reported getting an email from Apple based on a recent purchase. The email said if the item was not ordered, the consumer needed to disclose her name and social security number. Fortunately, the consumer caught on to the scam and did not share her personal information.

Here are a few tips to avoid falling for these types of scams:

- *When in doubt, delete.* If you have received an unexpected link in a text message or email, delete it. If you think it might be official communication from a company you do business with, go to that company's legitimate website without clicking on the suspicious link.
- *Beware of fake web addresses* (URLs) that look similar to a real company's web address. Also, find out the real email address that is sending you a suspicious email. Doing this may be as simple as hovering over the email address to reveal the real sender.
- *Login and check your accounts* that contain personal information on a regular basis. Doing so will help you catch scams as quickly as possible. Also, be sure that you use complex, unique passwords or passphrases for each account.

If you think your Apple ID has been hacked, Apple offers resources to help. Keep in mind, scammers will target anyone on any device, including Android users.

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.