Ohio Attorney General's
Consumer Advocate Newsletter

NOVEMBER 2014

Attorney General DeWine Warns Ohioans of Scams on Social Media

While many scams begin with a phone call or door-to-door visit, others attract potential victims through postings on popular social media websites and apps.

Consumers need to be skeptical of 'too-good-to-be-true' pitches, and offers on social media are no exception. As we use more methods to communicate, scammers will try to take advantage of us using those same technologies.

For example, earlier this year, a Dayton resident reported a "money flipping" scam in which the scammer offered consumers a chance to "flip" an investment of a few hundred dollars into thousands of dollars. The scammer claimed to have successfully flipped his own money and wanted to share his success with others. Using the Instagram social media app, the consumer read about a way to pay $150 and get paid $5,000 virtually overnight; he fell victim to the scam and lost $150 after he paid but received nothing in return.

In addition, scammers can take advantage of consumers who post vacation plans or other personal information on social media. After the scammers see the information, they can use it to devise an "emergency" scam, such as needing money to get out of a foreign jail or to fix their automobile that has just broken down during their trip

Another example of social media scams occurs when an online account is hacked by a scammer and used to send out "emergency" messages to a consumer's network of friends or contacts asking for money.

In almost all social media scams, the scammer asks for payment through methods that are difficult to trace, including wire transfers or the purchase of a prepaid money card.

Consumers can protect themselves by following these safety tips:

- Know that if it looks too good to be true, it probably is. Any quick way to make a huge, guaranteed profit without any risks is likely a scam.

- Be wary of any attempts by a stranger to get you to use a wire transfer service or purchase a prepaid money card.
- Conduct online searches based on what information you know about the potential scammer, such as the person's name, online user ID, email address, and phone number. Try searches using keywords from the posting and words such as "scam" or "complaint."
- Know that strange or unexpected social media postings that appear to be from friends could be the result of a scammer hacking into those friends' social media accounts. Before sending money, always verify the friend actually sent the post and not an imposter. Try calling a mutual friend at a trusted phone number to check out the legitimacy of such a posting.

Consumers who suspect a scam or organizations wishing to schedule a cybersecurity presentation should contact the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

Attorney General DeWine Announces National Settlement with AT&T Mobility

Ohio Attorney General Mike DeWine, along with other state attorneys general and federal agencies, recently announced a national settlement with AT&T Mobility LLC to resolve allegations that it placed unauthorized third-party charges on consumers' cell phone bills in a practice known as "mobile cramming."

As part of the settlement, AT&T Mobility has agreed to pay $105 million, of which $80 million will be used for consumer refunds.

Hundreds of thousands of Ohioans may be affected by the settlement, which was reached by the attorneys general of all 50 states and the District of Columbia, as well as the Federal Trade Commission and Federal Communications Commission.

"We urge consumers to check their cell phone bills for unauthorized charges," Attorney General DeWine said. "Phone bill 'cramming' can be a costly problem — small charges, undetected by consumers, can add up over time. This settlement provides restitution for AT&T customers who have experienced unauthorized third-party charges on their cell phone bills, and it helps prevent these charges in the future."

Consumers who have been "crammed" often complain about charges, typically $9.99 per month, for "premium" text message subscription services (also known as "PSMS" subscriptions) such as horoscopes, trivia, and sports scores, that the consumers have never heard of or requested.

The attorneys general and federal regulators allege that cramming occurred when AT&T Mobility placed charges on consumers' mobile telephone bills for these services without the

consumers' knowledge or consent. Last fall, AT&T Mobility and the three other major mobile carriers — Verizon, Sprint and T-Mobile — announced they would cease billing their customers for commercial PSMS charges.

Under the terms of the settlement, AT&T Mobility is required to provide $80 million in funds to be used to pay refunds to consumers who were victims of cramming. The funds will be administered by the Federal Trade Commission.

Consumers can submit claims under the AT&T Mobility cramming refund program by visiting www.ftc.gov/att. On that website, consumers can find information about how to obtain a refund. If consumers are unsure about whether they are eligible for a refund, they can visit the claims website or contact the Claims Administrator at 1-877-819-9692 for more information. Claims will be accepted until May 1, 2015.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

Avoid Falling Victim to Health Insurance Scams

Planning to make changes to your health insurance? Make sure you don't stumble into a scam.

Scam artists operate year-round, but during open enrollment periods, when individuals can make changes to their health insurance plans, consumers may be more vulnerable to scams involving insurance or medical products.

One Ohio consumer received a call from someone offering an insurance policy. The caller asked for the consumer's Social Security number, which the consumer provided. Later the consumer realized the call was a potential scam, and he did not know the name of the company offering the policy.

Another consumer received a phone call that was displayed as an "alert." Thinking it was a weather alert or Amber Alert, the consumer picked up. It was a recorded call that prompted the consumer to press a button to contact his health insurance company about authorization for a pain relief product. The consumer hung up the phone, finding the call deceptive.

An unexpected request for personal information, such as your Social Security number, Medicare number, or credit card information, is usually a sign of a scam. Rather than

providing information over the phone, ask for written information or hang up and contact an organization using a phone number you know to be legitimate.

If you want to contact a government agency or insurance provider online to learn about your options, make sure you reach the organization's official website. For government information, official websites include Healthcare.gov, Medicare.gov, and Insurance.ohio.gov. (Look for the ".gov" at the end of the web address.)

Look out for websites that have similar but different names than official websites. These websites may show up when you perform an Internet search for a government agency or insurance provider, but in some cases the websites are operated by scam artists or other untrustworthy organizations.

Watch for signs of a scam including:

- Unexpected requests for your personal information.
- Someone who says you must act immediately.
- Claims that new Medicare or insurance cards are being issued.
- Telemarketing calls that violate the Do Not Call Registry.
- Automated or "robo-calls" offering insurance plans or medical products.

To avoid potential health insurance scams, follow these tips:

- Guard your personal information.
- Don't respond to unexpected or suspicious phone calls.
- Never pay fees for help to understand your insurance options.
- Make sure your security software is up to date to help protect yourself online.
- Use a phishing filter if possible. A phishing filter works to detect whether a browser is going or about to go to an illegitimate website address.
- When in doubt, don't click on links or attachments contained in emails.
- Check out an insurance agent or navigator with the Ohio Department of Insurance before giving out personal information.
- If you receive any suspicious calls claiming to be from a government agency or health insurance provider, hang up and dial the agency or insurer using a phone number you know is legitimate.

- Don't trust callers who claim new Medicare or insurance cards are being issued and you must provide your information.

Ohioans who want help detecting a potential scam should contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov. For insurance information, contact the Ohio Department of Insurance at 800-686-1526 or www.insurance.ohio.gov.

Don't Get Caught in a 'Spear Phishing' Scam

The next time you check your email inbox, look carefully — it might contain a targeted message that a con artist designed just for you.

In a typical phishing scam, a con artist pretends to be an employee of a 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 account information, the scammer crafts a targeted message, using information they have learned about you.

A common way that scammers are able to obtain the information needed to conduct spear phishing campaigns is through data breaches. For example, if a large retailer suffers a data breach, the scammer may use the information obtained in the breach to later target their customers in a spear phishing attempt.

After obtaining the information, the scammer might send consumers an email that appears to be from the retailer that was breached, stating that the customer must resubmit his username, password, and other personal account information. Although the email appears to be from the retail store and even uses official-looking logos, the email is actually from a scammer who knows customers will be more likely to open the email if it appears to be coming from a trusted company with whom they have an existing relationship.

Spear phishing can also result from the hacking of consumers' personal email accounts. For example, a scammer may hack into e-mail accounts and find information about those consumers' financial planners and investment accounts. The scammer then sends e-mails to those financial planners (using the consumers' personal e-mail addresses) and asks the financial planners to transfer thousands of dollars to another account. If the financial planners comply with the request, consumers' money will be lost.

In order to make a spear phishing scheme seem legitimate, scammers need some inside information. 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. A phishing filter works to detect whether a browser is going or about to go to an illegitimate website address.

- 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.

- Think before you click. When in doubt, do not click on links contained in e-mail messages or pop-up messages.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.