CONSUMER ADVOCATE

From the Consumer Protection Section at the office of Ohio Attorney General Mike DeWine

IS YOUR PHONE SAFE FROM HACKERS?

Many mobile phones today are essentially mini-computers. They can be conveniently used to browse the Web, check e-mail, and make financial transactions.

But without proper security features, hackers may be able to use fairly simple technology to manipulate your phone and the information stored in it.

For example, they could change your control settings without your knowledge, or wipe out information stored in your phone.

According to "Stop. Think. Connect," a coalition of private companies, nonprofits, and government organizations to promote online safety, today's mobile devices require security software updates just like a personal computer or laptop.

Any devices that connect to the Internet, including smartphones, need protection from viruses and malware. To keep software updated, you may need to synch your phone with your computer.

The coalition also provides the following advice:

- Only give your mobile number to people you know and trust.
- Never give out someone else's number without their permission.
- If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.
- Get savvy about Wi-Fi hotspots. Limit the type of business you conduct using hotspots and adjust security settings to limit who can access your phone.
- When in doubt, don't respond. Fraudulent text messages, calls, and voicemails are on the rise.
- Requests for personal information or immediate action almost always indicate scams.
- Stay current on new ways to stay safe online. Check trusted websites for the latest information, and share what you learn with family and friends.

Continued on page 2

SCAM ALERT: ADVANCE FEE LOANS

Consumers throughout Ohio are reporting losing money to advance fee loan scams. In some cases, they send hundreds of dollars out of the country for loans that are nonexistent.

For example, a Central Ohio consumer received a call saying she qualified for a loan worth up to $5,000. In order to receive the loan, she first had to send $300 via wire transfer to India. She sent the money, but never received the loan. It was all a scam.

In an advance fee loan scam, con artists ask for upfront fees in exchange for a loan or line of credit. Victims often are asked to wire money to another country to secure the loan. After sending the money, however, victims receive nothing.

Continued on page 2

HIGH SCHOOL VIDEO CONTEST NOW OPEN

Ohio high school students can demonstrate their creative talents and have a chance to win scholarship prizes by entering the 2011 Take Action High School Video Contest.

To enter the contest, high school students may submit a 60-second video on Internet safety. Entries may come from individuals or teams of two students. In their videos, students must encourage their peers to be safe online using one of the following topics:

- Read the fine print.
- Free isn't always free.
- Too good to be true? It probably is.
- Research before you buy.
- Guard your personal information.

Videos must be submitted to the Ohio Attorney General's Office by December 15, 2011. Winners will be announced in early 2012.

The top three winning individuals or teams will receive college scholarships of $2,500, $1,500, and $1,000, respectively. To learn more, visit www.OhioAttorneyGeneral.gov/TakeActionContest.

Is your phone safe?

Continued

Be careful about the applications (apps) you download. Change your phone settings so that the phone automatically locks if it is inactive for a certain period of time. Establish a hard-to-guess password required to unlock it.

Buying online? Beware of payment scams

If you shop online, be skeptical of sellers that offer discounts in exchange for payment via wire transfer.

For example, a seller advertises a wedding dress for $3,000 but offers to lower the price to $1,500 if the buyer agrees to send the payment via wire transfer instead of PayPal. The buyer agrees and wires $1,500 but never receives the dress.

Scam artists may try to lure buyers away from the established payment mechanism so that they can more easily steal buyers' money.

They often prefer payment via wire transfer, because a wire transfer leaves very little paper trail, helping scammers get away with their ploys.

Scammers may use other tactics to trick buyers online. For example, they may "borrow" photos from a legitimate company's website, and then repost the photos to make potential buyers believe their (phony) offer is real.

Anytime you shop online, be very cautious and research the seller as much as possible. If a seller asks you to send payment via wire transfer, it's likely a scam.

Scam alert: advance fee loans, *Continued*

Since January 2011, the Ohio Attorney General's Office has received more than 100 complaints about advance fee loans or advance fee credit cards. While some of the complaints involve disputes against legitimate businesses, many represent scams.

Requests for wire transfers in exchange for a loan almost always signal a scam.

Signs of an advance fee loan scam include:

- Calls or e-mails offering loans
- Claims of "guaranteed" loans or lines of credit
- Demands for advance fees, such as a "bank processing fee"
- Requests for money sent via wire transfer
- Companies that fail to provide loan information in writing

In a related scam, consumers are contacted by "debt collectors" who demand payment on past-due loans. Consumers who receive these calls frequently say they had applied online for a payday loan but never received the loan and do not owe the money.

Sometimes the callers threaten consumers with arrest or jail time if they refuse to pay.

If you receive calls demanding that you pay a debt, tell the callers to provide written verification of the debt. If they refuse, don't trust them and don't send any money. The law requires debt collectors to provide verification that you owe a debt.

Scam artist hacks Facebook account, offers grant

A Southeast Ohio consumer reported that while she was chatting with her sister on Facebook, her sister said she had received a government grant.

The consumer's sister forwarded a link about the grant, and soon the consumer began chatting with an official who said he was from the Federal Government Humanity & Empowerment Program.

The official instructed the consumer to send $2,000 via wire transfer so that she could obtain a $150,000 grant. The consumer sent the money, but never received the grant. It was a scam. Her sister's Facebook account had been hacked.

In a typical grant scam, a con artist asks a consumer to wire transfer money in advance in exchange for the promise of a government grant. Despite the con artist's claims, there is no real grant and any money the consumer sends likely will be lost to the scammer.

Want updates?

- Receive the Consumer Advocate via e-mail by signing up at www.OhioAttorneyGeneral.gov/ConsumerAdvocate.
- Visit www.OhioAttorneyGeneral.gov for more information or to file a complaint about a consumer transaction.