



E-mail Address

ZIP code

GET UPDATES



BRIEFING ROOM

SERVICES

CONSUMER

ENFORCEMENT

LEGAL

ABOUT

CONTACT

Briefing Room > News Releases > December 2009 > Cordray Warns Ohioans of New H1N1 Scam

NEWS RELEASES

Cordray Warns Ohioans of New H1N1 Scam

12/1/2009

(COLUMBUS, Ohio)—Posing as the Centers for Disease Control and Prevention (CDC), scammers have found a new angle in the effort to exploit fears driven by the spread of the 2009 H1N1 influenza virus, sometimes called "swine flu." Attorney General Richard Cordray today urges Ohioans to beware of an e-mail which carries a computer virus that may infect your computer and provide a stranger with access to your personal information.

The bogus e-mail announces the launch of a "state vaccination H1N1 program" and encourages the user to create a personal vaccination profile. It provides a link to a Web page that looks similar to the CDC site. Within the page are downloadable instructions for creating your personal vaccination profile.

Cordray warns that by downloading the instructions, visitors are downloading a virus onto their computers.

"Any time you receive an e-mail from someone you are not familiar with, I strongly recommend avoiding the provided links," said Cordray. "Clicking on that link can unleash downloadable viruses capable of capturing your personal information and sending it back to the scam artist."

Because of these potential phishing attacks and e-mail scams, Cordray encourages consumers who are interested in H1N1 influenza virus information to visit the U.S. Department of Health & Human Services informational Web site at www.flu.gov or the Ohio Department of Health informational site, www.flu.ohio.gov. Cordray also offers the following tips to help Ohioans avoid phishing scams:

- **Contact the institution yourself:** Don't respond to unsolicited requests for your personal information. Instead, contact the organization at a phone number or a Web address you know to be correct.
- **Don't click on links in e-mails:** Be cautious about opening any attachments or downloading any files from e-mail messages. Links and attachments can make your computer vulnerable to viruses.
- **Look for warning signs:** Misspelled words or a lack of personal greetings may signal fraud. However, the presence of a personal greeting or a lack of errors does not guarantee legitimacy. Always be skeptical.
- **Use spam filters, anti-virus software, anti-spyware software and a firewall:** Update your security software regularly. The software can help stop your computer from accepting unwanted files that can be sent via phishing e-mails.
- **Don't give out personal information via e-mail:** E-mail is not a secure method of transmitting personal information. A bank or governmental agency will never request personal information via e-mail.
- **Monitor your accounts:** Review credit card and bank account statements as soon as you receive them. If you find unauthorized charges, immediately notify your bank or credit card provider.
- **Report phishing scams** to the company or organization the scam artist is impersonating and to the Ohio Attorney General's Office.

Report this phishing scam or any other scam to the Attorney General's Office at www.SpeakOutOhio.gov or by calling (800) 282-0515.

Media Contacts:

Kim Kowalski: (614) 728-9692
cell: (614) 893-6018
Ted Hart: (614) 728-4127
cell: (614) 743-2286

SEARCH

PREVIOUS RELEASES

[December 2009](#)

[November 2009](#)

[October 2009](#)

[September 2009](#)

[August 2009](#)

[July 2009](#)

[June 2009](#)

[May 2009](#)

[April 2009](#)

[March 2009](#)

[February 2009](#)

[January 2009](#)

[All News Releases](#)

Media Room

[More information for members of the media.](#)