NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

When Computer Trouble Pops Up, Scammers Offer "Help"

Release Date: **October 24, 2016**

Media Contact: **Jerad Albracht, 608-224-5007**
Bill Cosh, Communications Director, 608-224-5020

MADISON – *A Wisconsin consumer's computer screen turned black. A pop-up message told her to call Apple tech support and provided a phone number. A quick call and $299 later, the problem was fixed.*

Another consumer had a full-page ad appear on her screen, then her computer froze. She contacted a tech support company using the phone number in the ad and gave them remote access to her system. They unfroze the system, set her up with a Gmail account and charged her nearly $450 for their services.

A third consumer's computer froze when a flashing screen appeared and a loud alarm activated. She called the number on the screen for help. The support representative removed the flashing screen and alarm for a fee.

Three similar stories. All three are ripoffs. These examples demonstrate the recent blending of two types of extortion: ransomware and tech support scams.

Ransomware – where malware locks down a computer – involves an on-screen demand for an anonymous payment in order to free up the system. Tech support scams typically involve a phone call out of the blue to a potential victim from a conman claiming to be with Microsoft or a major tech firm. The caller warns the consumer about a (non-existent) virus on their computer and promises to fix it for a fee.

These newer hybrid pop-up windows serve the purpose of pushing a call center number out to unsuspecting computer users.

Calling the number listed on the pop-up is a fruitless and dangerous proposition:

- For one, there is no virus or problem that prompted these pop-ups. Even if there were a technical issue on your system, a tech support company (especially a representative from a major company like Microsoft) would never call to warn you about it.
- Secondly, the person you call will ask for your credit card or bank account information to charge you for their "services." Don't give out your credit and bank account information to someone you don't know or trust – especially a random scammer.
- The last and most dangerous reason not to call is that the "tech support rep" will request remote access to your computer in order to "fix" the problem. Turning over control of your system gives a stranger access to all of your files and sensitive information and opens up your system to whatever malicious software they wish to install.

Instead of calling the number in the pop-up:

- Disregard the warnings in the message. A virus has not actually been detected and you have done nothing to cause an issue.
- Manually shut down your browser or close it using Task Manager on a Windows system (hit the Ctrl, Alt and Delete keys simultaneously) or Force Quit on an Apple system (hit the Command, Option and Esc keys simultaneously).
- If forcing the browser closed is not an option, shut down the system and restart.
- Clear your website history and cache.

(MORE)

- If you face further issues, contact a trusted local tech support business for assistance.
- File a complaint with the Bureau of Consumer Protection at datcp.wi.gov.

More information on these types of operations and additional safety tips can be found on both the Microsoft and Apple websites.

For additional information, visit the Consumer Protection Bureau at datcp.wi.gov, call the Consumer Protection Hotline at 800-422-7128 or send an e-mail to datcphotline@wisconsin.gov.

Connect with the Bureau of Consumer Protection on Facebook at www.facebook.com/wiconsumer.

###