NEWS RELEASE

Cyber Monday Threats: Install Security Updates Now

Cyber thieves take advantage of unpatched vulnerabilities on computers, cell phones and other devices -- Dec. 8 free webinar to address this topic

PHOENIX, Ariz. (Nov. 21, 2016) – Christmas will come early to cyber thieves around the world on Cyber Monday, November 28 – one of the highest days of the year recorded for cyber crime. A recent study by EnigmaSoftware.com showed that in 2013 and 2014, malicious attacks on shoppers increased 40 percent on Cyber Monday compared to the average number of attacks on days during the month prior.

Michael Cocanower, founder and CEO of Phoenix-based itSynergy, said that number is probably even higher now as many brick-and-mortar retailers start to extend many of their Black Friday deals to Cyber Monday.

"Phishing scams and other techniques will be rampant, but one of the biggest threats relates to unpatched vulnerabilities in software programs. There is a common misconception that people can set their devices to 'automatic' and not have to worry about updates. That's where the danger lies…each product must be patched individually," he said.

Cocanower, who has been recognized nationally and locally for his IT expertise, conducts a free, monthly 15-minute webinar series, "Hacking the Human," on the second Thursday of every month. The next topic on Thursday, December 8 covers security updates, which Cocanower said is often misunderstood and neglected. Interested participants should register at http://www.itsynergy.com/webinar prior to the start of the webinar at 11:30 a.m.

When a criminal breaks into a network, one of the very first things on their 'To Do' list is to scan every machine for unpatched vulnerabilities they can exploit. If browsers, plugins, desktop apps and other programs on computers, cell phones, tablets and other devices don't have the latest security updates installed, clever thieves can easily break in.

"Bad guys are constantly looking for 'holes' to exploit software. When a vendor becomes aware of a hole that a bad guy is using, they issue an update to plug the hole," Cocanower said, adding that people don't realize that it isn't just software that needs patches. "Hardware devices, like medical devices, baby cameras, wireless routers, Nest thermostats and others need patches too. Almost every hardware device has some software embedded on it that allows it to do whatever it does. That software needs to be patched just as much as Apple iTunes or Windows does."

Cocanower offers these tips for getting current with security updates today:

1) **Do an inventory of all of the devices that need security updates.**

   Computers, tablets, cell phones, wireless routers, baby cameras, medical devices – anything that has software embedded to make it work needs to be updated. And, be vigilant about your cell phone. Both Apple and Google regularly release updates to their mobile software. Sometimes hardware manufacturers or cellular providers don't pass those updates along immediately, so it is important to remain vigilant about updating.

2) **Include devices used by employees working remotely.**

   Remote workers allow potentially sensitive or confidential information to reside on a PC which is outside of a company's control. Additionally, a company has to open a 'hole' in its perimeter defenses in order to allow users in.

   Some of the most sophisticated, security-conscious organizations implement an 'interrogation' of a remote/home computer when the employee attempts to connect remotely. If security patches aren't installed, the remote access system will 'quarantine' the remote/home system and not allow it to get access to network resources.

3) **Do an inventory of all of the software programs that need to be updated.**

   Examples include Chrome, Microsoft, Adobe Flash, Oracle Java, apps on your phone…the list is endless.

4) **Start getting into the habit of doing security updates regularly**.

   For businesses, a qualified IT firm can help manage this as it is too burdensome without automation. There are third party programs that help to keep all of the apps updated, such as Ninite, http://ninite.com. You also can go to the website of each individual vendor. Most applications have a 'check for updates' feature somewhere that you can use.

   Check with manufacturers of both software as well as hardware devices to ensure you have the latest updates. Larger software vendors, such as Microsoft and Apple, will have utilities installed that will allow you to easily check for updates. On a Windows PC, just type Windows Update into the search bar, and on Apple open the App Store app on your Mac, then click Updates in the toolbar.

The "Hacking the Human" webinars are geared towards non-technical end users in business at any level in the company. Each webinar provides useful tips to ward off cyberattacks and more complex social engineering schemes that result in theft and corporate espionage.

For more information, call itSynergy at (602) 297-2400 or visit www.itsynergy.com.

###

About Michael Cocanower

He has his black belt in the Kung Sul division of Hwa Rang Do, a Korean martial art, so it's fitting that Michael Cocanower's passion is helping small and medium-sized businesses defend themselves against malicious cyber intruders. A Phoenix native, Cocanower founded itSynergy in 1997, and under his leadership, the company has experienced exponential revenue growth. A long-standing Microsoft Partner, itSynergy provides strategic technology management services for small and mid-sized organizations on a fixed monthly fee. Cocanower has received numerous awards and widespread industry recognition throughout his career, including being named one of 20/20 Visionaries in *Channel Pro Network* magazine's May 2016 issue. The magazine regularly turns to him for input on current IT trends, and called him a "shrewd and articulate observer of the SMB market." In addition, the Arizona chapter of Entrepreneurs' Organization (EO) recently appointed Cocanower to the board of directors as membership chair.

Media Contact:
Sue Kern-Fleischer, PublicizeThis!, (602) 810-1404, sue@publicizethis.com