Fake Website Scams! Scam Alert 6/28/17

Posted on 06/28/2017 by Jane Margesson | AARP Maine | Comments: 0

Little blue pills, spilling from a bottle. Could they be those “Special Pills”? Only you can say. This image became my second flame on Saturday, January 7th, 2006. It also was my 5,000th download on August 10th, 2006.

6/28 SCAM ALERT

Scammers are creating fake websites that look like known and trusted news sites to sell “brain booster” pills. They post bogus articles about the pills with endorsements from people like Stephen Hawking and Anderson Cooper (neither has endorsed any such product). The site then links you to the sales page for the pills where you can place an order with a credit or debit card. The scammers claim the pills will lead to an increase in concentration and memory recall, but there is no evidence to support these claims, according to the Federal Trade Commission. It’s always a good idea to consult with your doctor before purchasing health products.

Be a fraud fighter! If you can spot a scam, you can stop a scam.

Report scams to local law enforcement. Contact the AARP Fraud Watch Network at www.aarp.org/fraudwatchnetwork for more information on fraud prevention.

New ransomware attacks

A new form of ransomware is making its way around the world and infecting thousands of computers.

The new malware reported Tuesday is more dangerous and can cause more damage than the WanaCry ransomware that made an appearance last month. Called “Petya/NotPetya” users receive a notice to reboot their computer at which point the system locks. Supposedly you can fix the problem by paying the ransom of $300 in bitcoin but experts report that the email address for payments has now been shut down and mail is being returned to the sender.

Users should look for a warning box that appears and says “You are about to be logged off” and “windows will shut down in less than a minute.”

When the user reboots their computer, they will see what appears to be the system checking the disk with a list of files/programs. According to experts, some users have been successful in preventing the encryption if they turn off the computer at that point. The final notification from the malware is a screen that tells them their files have been encrypted and to pay the ransom.

Maine Identity Services reminds you to keep your security software and operating system updates current and be careful when opening email attachments or visiting new websites. Please make sure that you are backing up all needed data to an appropriate cloud or device.

Maine Identity Services, LLC provides data breach and identity theft assistance to individuals, organizations and law enforcement personnel through its books, seminars and police materials. For more information about the company and its products, visit www.meidhelp.com or email: info@meidhelp.com .