Michigan AGENT

A publication of the Michigan Association of Insurance Agents
July/August 2016

THE $18 BILLION INSURANCE ECONOMY

Michigan's P/C Carriers Grew 3.3% in 2015

PLUS:

- The Misclassification of Employees: 6 Factors to Consider in Determining Independent Contractor Status
- Defending Your Agency Against Ransomware & Other New Threats

Michigan AGENT

July/August 2016

EDITORIAL

Kari Quimby, CIC
Editor
517-327-8037
kquimby@michagent.org

CONTRIBUTORS

Jerry Fetty
jerry.fetty@smartservices.com

Lynne D. Mapes-Riordan
lynne.mapes-riordan@bfkn.com

Amy Skidmore
amy@Aartrijk.com

Charles Wasilewski
charles@Aartrijk.com

ADVERTISING AND PRODUCTION

Jennifer Burnett
517-327-8030
jburnett@michagent.org

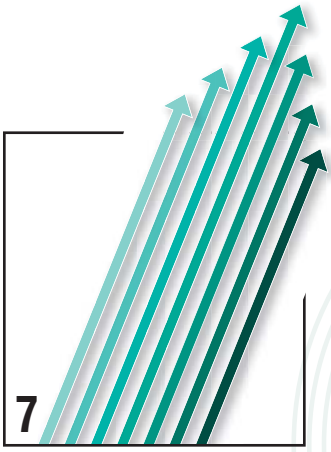
www.michagent.org

Michigan AGENT is published bi-monthly by the Michigan Association of Insurance Agents.

Postmaster: Send Address changes to 1141 Centennial Way, Lansing, Michigan 48917.

Printed in USA

Contents



ETC.

Camp YAC 2016 Highlights: The Power of Teamwork ... 22

The Mission of the Michigan Association of Insurance Agents is to advance the critical role of insurance and essential services provided by independent agents. We vigilantly advocate for a positive legislative and regulatory environment, assist in enhancing our members' business and professional skills, promote ethical conduct, and encourage a healthy insurance environment.

Defending Your Agency Against Ransomware and Other New Threats

By Jerry Fetty, SMART I.T. Services

There are now over a million variants of viruses on the Internet, affecting all operating systems and devices. We refer to them by many different names, and they have many different delivery methods: spyware, Trojans, worms, and phishing. More recently, ransomware has been on the front pages. But regardless of what you call them, these malicious programs, pop-ups, and emails are becoming more and more complex, making it harder for everyday users to decipher what is legit and what is harmful.

The hackers who produce these viruses are also getting more sophisticated.

For example, one recent study found that 80%-plus of malware comes from legitimate websites. Our company has even seen numerous examples of carrier and agency resource websites that have malicious code embedded within them.

Another group of hackers actually uses patches to help them spread viruses. They do this by waiting until a new patch for a software is released. Because many careless companies take weeks or even months to install new patches, the hackers will take the new patch, reverse engineer it to find out what flaw it is fixing, then develop a virus to exploit that flaw on those who delay updating their software.

Though the complexity of some of these schemes has changed, the goal of both old and new viruses is generally the same: to trick you into installing malware on your computer, potentially compromising personal and company data, while making your computer run slow.

I like to compare it to the old vampire movies in which the vampire could not enter a home unless invited in. Disguising himself as an honorable gentlemen, the vampire was able to trick the unknowing person into opening the door. In a similar way, that is what happens with viruses. The user of the system is deceived into clicking on the bait, and by doing so authorizes the malicious code to be installed and executed on the operating system.

For example, you may have heard of CryptoLocker, which is a ransomware Trojan that targets computers running Microsoft Windows. It first surfaced in September 2013, and attacks from various sources, such as under the guise of being a legitimate email attachment (fake resumes are very popular these days). When activated, the malware encrypts certain types of files stored on local and mounted network drives. The malware then displays a message which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid voucher) is made by a stated deadline, and threatens to delete the private key if the deadline passes. If the deadline is not met, the malware offers to decrypt data for a significantly higher price in Bitcoin.

How to Protect Yourself on the Internet

Fortunately, there are some steps your agency can take to significantly reduce the threat that viruses such as

Continued on page 34

Ransomware pose.

- ***Have an Acceptable Usage Policy in Place***. At our company, we have a very simple policy that states people are only allowed to do what pertains to their business function while at work. We found over time that the more detailed we tried to get with a policy, the more holes people tried to punch into it. So keep your acceptable use policy simple.
- ***Training***. One of the best preventative steps you can take is training your employees on how to recognize and deal with potential threats. For example, all your employees should know what virus software your agency uses. If they all know you use McAfee, they won't be fooled by a pop-up that alerts them that Windows Defender has identified a malicious virus on their computer. All your employees should know who to contact about any suspicious or questionable emails or pop-ups. New employees should be clear about the agency's security policies. (If you want to provide some basic training for your employees, we recommend our 30-minute webinar on this topic. http://bit.ly/28Mfne6)
- ***Keep Your Web Browsing Safe***. Don't lower your web browser settings. When an agency runs into problems at a carrier website, sometimes the first thing the carriers tell them to do is lower their security settings, and that is just not safe. You should call your IT people instead. A good agency IT company should know the web settings you need to make that specific carrier's website work, while keeping your agency safe.
- ***Have a Good Internet Monitoring and Filtering System***. We get into a lot of discussions with agents on this, particularly because agents do not want to come off as Big Brother with their employees. We understand that, but these monitoring systems have become very sophisticated in recent years, so they can be set to block the bad stuff, without preventing the mid-level concerns, such as online shopping.
- ***Get a Single Product to Cover Anti-virus and Malware Protection***. Although you can purchase separate products for each of these, we recommend you buy a product that covers both. When a different company is dealing with either viruses or malware, they individually are not concerned with causing problems for the other company's products. If two different products are both trying to block certain things, it can cause trouble such as lock-ups, scanning issues, or slowness.
- ***Be a Skeptic***. This is a trickier one. If we could provide everyone a single piece of advice on how to avoid a virus, it would be this: be skeptical. If a pop-up doesn't look right, or an email looks funny, don't click on it.
- ***Avoid Certain Sites***. This includes:
  - *Online chat* (unless you are online with tech support)
  - *Gambling/Gaming Sites*. Both are notorious for being magnets for malware and viruses.
  - *Illegal Download Sites*. No one should be accessing these sites for "free" music or movies.
  - *Social Networking Sites*. While it is understandable and acceptable that a person or two in your agency needs to have access to social media for professional reasons, most employees will use it only for personal reasons. The danger is not so much with the social media site, but the links in them that, when clicked, can connect you to a server that will download a virus to your system.
  - *Pop-ups*, especially ones that look like an anti-virus software. Your anti-virus program is not going to typically just pop up and start a scan.

Most times, the entire image that pops up is linked to a malicious website, so clicking anywhere on it (even the "X" or the Close or Cancel buttons), will bring you to that site.

Finally, here are some tips if you or someone in your office gets a pop-up that you suspect is not legitimate:

- Never click the "X" to try and close the program. Most times, the entire image that pops up is linked to a malicious website, so clicking anywhere on it (even the "X" or the Close or Cancel buttons), will bring you to that site.
- Use ALT+F4 to close the window. This is a Windows shortcut that tells the system to close the window in front of the user. If there are several windows that popped up, you may have to do this several times.
- If the pop-up still doesn't go away, shut off your computer, and call your IT company. ■

Jerry Fetty is founder and CEO of MAIA Platinum Partner SMART I.T. Services, Inc., an Information Technology service company that specializes in helping independent insurance agencies increase their productivity and profitability by harnessing the power of technology. He can be reached at (586) 258-0650 or jerry.fetty@smartservices.com.