MARCH EDITION | Chief of Police Dennis J. Mc Enerney | Volume 3, Issue 3

S.C.R.A.M. GAZETTE

Home Alarm Scams

An alarm company is conducting door to door scams telling homeowners that they are affiliated with their alarm company.

The subjects may entice a homeowner to sign a new five year contract by stating the following:

- Their current alarm company went out of business.
- The need to update their security equipment or their contact information.
- The contract change may save them money.

If you have fallen, victim to this scam you are asked to file a police report immediately.

To prevent this scam from happening to you, we offer these quick tips:

- Before signing any contracts or changing of services. Call your current company to confirm, use the phone number on the paperwork you already have. Speak to a family member, or contact your local police department to determine if it may be a potential scam.
- If they do come to your door. Ask them for a business card with their company name, their name and phone number on it. If they represent themselves with a business card from your home alarm company you should call the telephones number on your billing statement to verify this is a verified contractor or employee your legitimate alarm service.
- Sales agents who push their way into your home, or refuse to leave. It's always safer to say no to someone on your doorstep before they come in, rather than trying to get a salesperson out of your home. Firmly tell the person no. If they continue to pressure you, close the door and call the police.
- High-pressure or scare tactics. Limited time offers, and pressure to "act now" to protect yourself from supposed crime sprees in your neighborhood are often signs of a scam. Report it immediately and do not sign any contracts without fully understanding the terms and conditions of the "offered deal".

SCAMS—Plague community members

The Better Business Bureau has released some of the top scams that occurred in 2015 in the hopes to warn people what to look out for this year.

Top Heartbreak Scam: Catphishing: Total Loss=$15.62 Million

People lost the most money to this type of scam last year. Scammers work to gain their victim's trust, while never meeting face to face.

CONSUMER TIP from the BBB: Do not give out personal information or send money to someone you have never met. Be wary of sob stories and reasons why they won't meet you in person.

Top Prize Scam: Fake Lottery Winnings: Total Loss=$6.597 Million

This scam works when people convince their victims they have won a prize in the U.S. lottery, but they have to pay a fee to collect it. If you did not enter the lottery, you have not won.

CONSUMER TIP from the BBB: Most legitimate airline, hotels and vacation booking agents do not participate in telemarketing promotions, solicitations or unsolicited prize giveaways. Before giving out any personal information to "claim" a prize, ask to see the details of the prize in writing and carefully read the fine print. Some vacation prize giveaways may cost you more than you are willing to pay.

Top Subscription Scam: Free Trial Traps: Total Loss=$2.982 Million

This scam works when consumers are asked to sign up for a free trial of a service and have to pay a nominal fee. Once the scammers have your credit card information then you are enrolled in paying a monthly expensive subscription.

CONSUMER TIP from the BBB: Read all terms and conditions and be sure to read reviews of a company before signing up for anything.

Top Imposter Scam: Spear Phishing: Total Loss=$5.826 Million

Be on the lookout for fake websites and emails that look like services we use all the time. When people click on insecure links they can be duped into signing up for something and losing money.

CONSUMER TIP from the BBB: Only shop on secure and legitimate websites. Do not follow any questionable links and if you are online shopping, make sure to look for a 'lock' symbol in the URL.

Top Emergency Scam: Fake Relative Needs Cash: Total Loss=$1.952 Million

Someone can quite easily find out a little information about you through social media. They then call you up and use that information to pretend they are a relative and they need money to help them out of a problem.

CONSUMER TIP from the BBB: Do not send money to someone you don't know.

NEXT SCRAM CLASS
April 13, 2016
At
11 a.m.
Niles Senior Center

Niles Police Department
7000 W. Touhy Ave
Niles, IL 60714
847-588-6500
www.nilespd.com

Connect with US!

www.nilespd.com

PROTECT YOUR SMART TV FROM HACKERS

One of the hot gift items this past December was an Internet-connected "smart TV," but what many new owners don't realize is that these TVs can be hacked -- just like a computer or smartphone.

How the Scam Works

When you use your smart TV to browse the Internet or connect through apps, scammers can take advantage of security holes to gain access to your device. On some TVs, the apps aren't as secure as those on your smartphone.

Once they hack your TV, scammers can access the camera and voice controls. They can use this to spy on your home (to time a break in) or listen in on conversations. Scammers can also gain access to information on the machine, such as usernames and passwords, or even computers on the same network.

Smart TV hacking isn't really a big issue yet. But as more people purchase these TVs, con artists are bound to find ways to use them for scams. This just happened with smartphones a few years ago.

Tips to keep your smart TV secure:

- Treat your TV like a computer. Your smart TV is a computer, so use the same common sense you would for keeping your laptop safe. For example, don't visit suspicious websites or click on strange links.
- Keep your TV system up-to-date. Manufacturers will do their best to patch security holes. System updates are annoying but vital for protecting your device.
- Use firewalls. Any device that connects to the Internet should be guarded by a firewall, and your smart TV is no exception. Be sure to use your smart TV's built-in firewall settings and a router with an enabled firewall.
- Secure your network. Be sure your home's wireless network is secure by having proper passwords and up-to-date software.
- Watch the camera. Assume your TV's camera and microphone are turned on. If you are concerned, cover the camera with a piece of tape.

SAVE THE DATE—UPCOMING ACTIVITIES

April 13—SCRAM Presentations—Identity Theft

11 am at Niles Senior Center

April 30—National Drug Take Back Day

10 am to 2 pm at the Niles Police Department

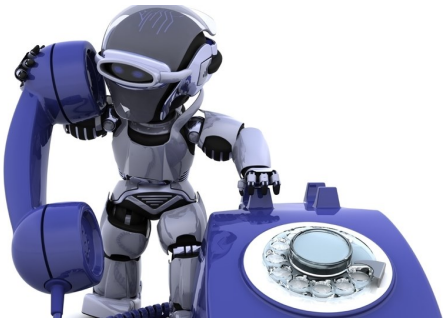
May 11—SCRAM Presentation—Ruse Entry Burglary

11 am at the Niles Senior Center

Phony calls about health insurance

Robocalls can be more annoying than a lingering head cold. Recently, some people got robocalls that seemed to be about health insurance and the Health Insurance Marketplace, but the calls were a con. The callers were phishing for personal information. People who work in the Marketplace don't make cold calls, and they never ask for personal information. If you get a call like this, hang up.

The phone numbers showed up with a local area code. The recorded message sounded urgent: "You need to buy health insurance or face a fine. To learn more, press 1." A person who works in the Health Insurance Marketplace got the call and knew it was fishy, so she pressed 1. The operator claimed to 'work with the law,' and asked for the person's full name, date of birth, phone number, income information and Social Security number. The person who got the call knew it was nonsense, so she hung up and contacted the FTC.



If you get a recorded sales call, but you didn't give the caller written permission to call you, the call is illegal. Don't press 1 to speak to the operator or get your name taken off the list, and don't give any personal information. If you respond, you'll probably get more calls. If you want information about health insurance in your state, visit HealthCare.gov. If you get a call like this, please report it to the FTC.