S.C.R.A.M. GAZETTE

2015 In the Review:

Scam protection and how to be safe in 2016

2015 had some very impressive scams that resulted in millions of dollars of losses for money for victims. The scammers used a variety of tricks, some old, some new to separate the victim from their hard earned cash.

Here are the top 10 of 2015:

1. **Internet merchandise scams:** You buy something online, but it is either never delivered or it is not what they claimed it was, or is defective.
2. **Phishing/Spoofing Emails:** Emails that pretend to be from a company, organization or government agency but ask you to enter or confirm your personal information.
3. **Fake Prizes, Sweepstakes, Free Gifts, Lottery Scams:** You receive an email claiming you won a prize, lottery or gift, and you only have to pay a "small fee" to claim it or cover "handling costs". The prize, of course, does not exist.
4. **Fake check payments:** You sell something online or through Craigslist and you receive a phony check, and instructed to wire money back to buyer. The check looks real… but after you try to cash it, you find out it is a fake. To make matters worse, you get arrested for passing a counterfeit check!

5. **IRS Tax Scam: The** Victim is called and told by the "IRS" that they owe back taxes and a penalty. They are asked to secure a credit card and make a payment or they will be arrested for the IRS.
6. **Jury Duty Warrant:** The victim is called by the "police" told that they failed to show up for jury duty and there is a warrant for your arrest. The victim is then asked to pay a fine via a secured online credit card.
7. **Computer Performance Scams:** Have you ever got that call from "windows"? You know the one that tells you your computer is running slowly and has a virus? When was the last time Microsoft called you ? When you call them it takes three hours of waiting before you get to speak to a live human. Microsoft will never call you!
8. **Grand Parents Scam:** This scam involves the victim being called from their "grand child" alleging to be in a foreign country under arrest and needing money. The victim is asked to wire money via Western Union or to get an online secured credit card to make a payment.
9. **Online Dating Scams:** These people portray attractive men and women and then claim they need your money to help in an emergency.
10. **Facebook Fake Friend Scam** – Have you ever got a friend request on Facebook from someone you already thought was your friend? If you hit accept, you may have just friended a scammer. The scam comes into play by having the con artist (fake friend) build an online relationship, and trust, and then He/she asks you to send money.

When in doubt, before you send any money or conduct any transaction contact the us at the Niles Police Department to verify if it is a scam. If you feel uncomfortable about it call a family member and ask them.

Next SCRAM Class

December 18

10 am

Holiday Safety

Niles Police

7000 W. Touhy Ave
Niles, IL 60714

847-588-6500

www.nilespd.com

Connect with US!

www.nilespd.com

Chip-and-PIN opens you up to fraud. Be aware of this scam!

You probably know by now that credit card issuers are sending out millions of new credit cards that are designed to be more secure than your current credit cards. They're called EMV (Europay, MasterCard, Visa) or chip-and-PIN cards that you can spot by the shiny computer chip embedded in it.

With the EMV cards, the chip records each transaction and assigns it a number. No transaction code can be used twice, so even if hackers steal it, it won't do them any good. These cards, which you insert into a reader rather than swipe, is doubly secure if your card also requires a secret PIN to get in, hence chip-and-PIN.

The Federal Trade Commission issuing warnings to card users like you. There are a huge number of these cards in the mail. In America, 120 million cards have already been issued but another 480 million are so will be delivered over the next couple of months.

The problem is twofold. Protect your mailbox because crooks can steal the cards. But scammers are also up to their old tricks, either sending phishing emails or calling you.

These scammers will email you links. If you click on them, it may infect your computer with malware or take you to a bogus site where they collect your personal information. If they call you, they'll say they're your card issuer and they need your information before they can send you an EMV card.

The FTC is warning every card user to take three steps to protect yourself from these scammers.

1. Your card issuer will not call you or send you email asking you to confirm your personal information. Delete those emails, and hang up on those calls.
2. Contact your card issuer if you've received emails or phone calls from scammers claiming to be the card issuer.
3. Don't open email links. The only time you should input your personal information is when you typed in a company's website address yourself.

Source: www.kimkomando.com

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data. As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Devices which remotely or automatically adjust lighting or HVAC
- Security systems, or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Entertainment devices to control music or television from a mobile device

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT Risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices.

What an IoT Risk Might Look Like to You?

Unsecured or weakly secured devices provide opportunities for cyber criminals to intrude upon private networks and gain access to other devices and information attached to these networks. Devices with default passwords or open Wi-Fi connections are an easy target for cyber actors to exploit.

Examples of such incidents:

- Cyber criminals can take advantage of security oversights or gaps in the configuration.
- Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting.
- E-mail spam attacks are not only sent from laptops, desktop computers, or mobile devices. Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail. Devices affected are usually vulnerable because the factory default password is still in use or the wireless network is not secured.

Consumer Protection and Defense Recommendations

- Isolate IoT devices on their own protected networks;
- Disable UPnP on routers;
- Consider whether IoT devices are ideal for their intended purpose;
- Purchase IoT devices from manufacturers with a track record of providing secure devices;
- When available, update IoT devices with security patches;
- Change any default password or an open Wi-Fi connection, change the password and only allow it operate on a home network with a secured Wi-Fi router;
- Patients should be informed about the capabilities of any medical devices prescribed for at-home use. If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor;
- Change all default passwords are changed to strong passwords. Do not use the default password determined by the device manufacturer. Many default passwords can be easily located on the Internet. Do not use common words and simple phrases or passwords containing easily obtainable personal information, such as important dates or names of children or pets. .

Fake Charities, how to navigate through the fog to find the real ones.

How it works: The end of the year is a prime time for charitable donations, and scammers try to take advantage. Fake charities are among the most popular holiday scams: scammers either misuse the name of a genuine organization, or make up their own.

What to do:

- Only donate to charities you know. If a new charity piques your interest, be sure to verify it on charitynavigator.org or through the Better Business Bureau.
- If you get a request via phone, call the charity back and ask if they can send you material about them to your address.
- Don't donate cash or use a wire transfer. Verify the organization's correct name and donate by check.
- Beware of charities that raise funds for local fire fighters or police. Check their authenticity before offering money.
- Ask how much of your donation will go for the cause. Some charities often spend the majority of their money for internal operational costs

4 TIPS TO FOLLOW IF YOU'VE BEEN VICTIMIZED:

1. File a police report. File a report about the fraud or scam so you can prove to your bank and credit reporting companies you've been scammed.
2. Tell your credit card company and bank. If you are the victim of identity theft or some other financial scam, contact the fraud department at your credit card company and bank.
3. Report the fraud to the three credit reporting companies. Each credit reporting company has a fraud unit: Equifax: (800) 525-6285; Experian: (888) EXPERIAN or (888) 397-3742; TransUnion: (800) 680-7289.
4. Gather evidence. In addition to the police report, save what you can related to the suspected fraud. Having items such as letters/emails of solicitation, prospectuses, cancelled checks, cash receipts, receipts for cashier's checks or money orders, bank statements, investment statements, or medical statements could help you get your money back or protect yourself from further victimization.