SEPTEMBER EDITION
Chief of Police Dennis J. Mc Enerney
Volume 3, Issue 9

S.C.R.A.M. GAZETTE

Citizens Police Academy

Well you may have missed your opportunity to attend this years Citizen's Police Academy. But that doesn't mean you can't participate and follow along. Each week, we will be offering a virtual look into the Citizens Police Academy Class by using the hashtag #NPDCPA2016.

By utilizing Twitter, Instagram or Facebook you can follow along and participate as a Virtual member of the Citizen's Police Academy.

During class sessions you can post messages using #NPDCPA2016. Our staff or volunteers will then answer those questions as they come

This provides you with an inside view of the Niles Police Department's Citizen's Police Academy.

Our program starts on September 6th, at 6:30 pm and runs every Tuesday until November 15th.

This is your opportunity to get the insiders view, join us and send us your messages.

Hackers can steal your info in three easy steps when you use public Wi-Fi

Are you always on the hunt for open public hotspots to save on data costs? Or perhaps you 're on the road and need an internet connection to check on remote documents on your work laptop.

We have warned you before about how crooks can use public Wi-Fi networks to steal your data or even rig public charging stations to steal your data. It's quite simple and easy for determined hackers to set up fake public "honey pot" traps.

Yesterday, former top hacker turned cyber security consultant, Kevin Mitnick demonstrated to ABC's Four Corners how easy it really is.

53-year-old Mitnick was arrested in 1995 for the security breaches of more than 40 major corporations including Nokia, Motorola and IBM. He served five years in prison and is now one of the top white-hat security consultants in the industry.

In the Four Corners video, Mitnick showed how a hacker can steal data by setting up a fake Wi-Fi public hotspot with a legitimate-sounding name, like "Telstra Air" in an airport, as used in his example.

Once the victims unsuspectedly log into the fake Wi-Fi network, the hacker then sniff and record all the keystrokes coming from their devices, including usernames and passwords from websites they visit, such as banking information.

Mitnick says once this user information is stolen, hackers could then send out fake software updates to the target computers to install malware. If the malware is successfully installed, the hackers will gain full control of the infected computers.

He also said that these hacking tools are accessible to everyone on the internet, that even high school students can download and deploy them.

To summarize, here are the three steps that Mitnick demonstrated:

- Hackers set up their own fake public Wi-Fi with a misleading name.
- Upon logging in, the victim's keystrokes are recorded and stolen to obtain personal information.
- Hackers will send malware disguised as updates to the victim's computer. Once the malware is installed, the hackers gain full control of the computer without the victim's knowledge.

How to protect yourself:
When you do connect to public networks, encrypted data is essential to your online security. However, you can't always trust that the network is encrypting that data for you. Visiting SSL sites, or websites that begin with the letters H-T-T-P-S means that the data exchanged is being encrypted. But you still may want to take additional precautions. Here's how:

- Virtual Private Networks,(VPNs): You might not realize that it's easy to create your own private network. VPNs, can be created wherever you go if you have the right software. There are several apps that create VPNs, as well as online security software.

Next Presentation
SCRAM
9/23 @ 11 AM
"Internet Safety"

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

Connect with US!
WWW.NILESPD.COM

The FTC offers the top three ways to avoid fraud

The Federal Trade Commission offers tips regularly on not to become a victim of a scam. The FTC recently released a brochure that provides the top 10 ways to avoid fraud. The brochure is available online.

According to the FTC the brochure is a one-stop resource to help you spot imposters, know what to do about robocalls, and how to check out a scammer's claims.

Here are three things that can help you avoid scammers who try to call you:

1. **Hang up on robocalls.** If you pick up the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal and plentiful. Don't press 1, 2 or any number to get off a list or speak to a person. That just means you'll get even more calls.

2. **Don't trust your caller ID.** Scammers can make caller ID look like anyone is calling: the IRS, a business, government office and even your own phone number. If they tell you to pay money for any reason, or ask for your financial account numbers, hang up. If you think the caller might be legitimate, call back to a number you know is genuine – not the number the caller gave you.

3. **Talk to someone.** Before you give up money or information, talk to someone you trust. Scammers want you to make decisions in a hurry. Slow down, check out the story, search online – or just tell a friend. We find that people who talk to someone – anyone – are much less likely to fall for a scam.

For seven more tips to help protect yourself and loved ones from fraud, read on – or order your free copies of *10 Things You Can Do to Avoid Fraud* to share in your community. And if you spot something that looks like a scam, report it to the FTC.

Scary new malware puts millions of phones and tablets at risk

The ever-changing world of cybercrime consistently gets more and more sophisticated. The villainous cybercriminal will go to the extreme to get their hands on your personal information and steal your money. Ransomware attacks alone quadrupled in the first quarter of 2016 from the same period a year earlier.

Trojans, phishing emails, viruses and ransomware are just some of the scary attacks that you've read about on our site. Now, there's a first-of-its-kind attack that could infect millions of gadgets.

The new attack comes from mobile malware that can infect Android phones and tablets. It's a Trojan named Twitoor, and it coordinates with botnets by using the social media site Twitter. This is the first known Trojan to coordinate infected gadgets through social media site rather than a command-and-control (C&C) server.

A botnet, to refresh your memory, is a group of gadgets that hackers have quietly taken over. The hackers take control with a virus and then use the combined power of the gadgets to perform large-scale hacks or scams. The gadgets under control can even send spam messages without the owner knowing.

Once the malware is hidden on your gadget, it repeatedly coordinates with a Twitter account. That account then gives the Trojan instructions on what to do next. It will be instructed to either install secondary payloads or to switch to another command-and-control Twitter account.

The Twitoor app can not be downloaded from the Google Play store. That means it's most likely spread through malicious URLs or text messages.

Source: Komando.com