S.C.R.A.M. GAZETTE

The Niles Police Department has a New Chief of Police

The Niles Police Department has a new Chief of Police. Chief Luis C. Tigera was appointed by the Village Board and Mayor Andrew Przybylo in June and formally took command of the department on July 1st.

Chief Tigera brings with him 37 years of law enforcement experience. Chief Tigera was formerly the Chief of Police in Broadview, Illinois from July 2011-April of 2017. Prior to that Chief Tigera was the First Deputy Director of the Illinois State Police from 2009-2011, Second in Command of the agency.

Chief Tigera held the rank of Region 1 Commander (as a Major) from 2008-2009. Region 1 covers, the Illinois State Police Districts 2 and 15, Investigations Zone 1 and the Protective Services Unit.

Chief of Police Luis C. Tigera

From 2004-2008 Chief Tigera was the Deputy Administrator (as a Major) for the Illinois Gaming Board. This unit provided the Illinois Gaming Board with enforcement, investigative presence to uphold the integrity of gaming in the State of Illinois

From 1985-2004 Chief Tigera held various positions in the Illinois State Police including the rank of Trooper, Sergeant, Master Sergeant and Lieutenant.

Chief Tigera started his career in law enforcement at the Niles Police Department in June of 1980. He held positions such as Public Service Aide, Communications Dispatcher and Reserve Officer until he left to join the Illinois State Police in 1985.

Chief Tigera looks forward to the opportunity to work in Niles, to build new community programs, to improve programs currently already in place and increase the high regard that the public has for the Niles Police Department.

The National Night Out is August 1st, Join us!

The 2017 National Night Out Against Crime and Drugs is scheduled for August 1, 2017 from 6:00 p.m. to 9:00 p.m. It will be held at Oak Park which is located at the corner of Main street and Ottawa street.

This years event will be highlighted by a police K-9 demonstration with the debut of our new K-9 Officer Ace and his handler Officer Christopher Koch.

We will also be highlighting our Impaired / Distracted Driving Course,

Dunk-A-Cop, NIPAS Emergency Services Team equipment demonstration, youth activities, family games, food and more.
The National Night Out is an annual community-building campaign that promotes police-community partnerships and neighborhood camaraderie to make our neighborhoods safer, more caring places to live.

National Night Out enhances the relationship between neighbors and law enforcement while bringing back a true sense of community.

If you need information about this years event contact Commander Robert Tornabene at 847-588-6505.

Next Presentation
9/13/2017
11 am
Confidence Scams

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

Connect with US!

WWW.NILESPD.COM

WannaCry-style Ransomware Now Targeting Smartphones

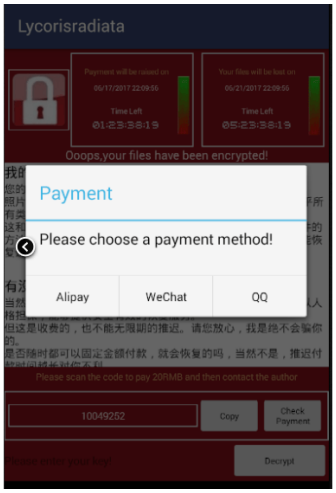
The recent global outbreaks of the WannaCry and Petya/GoldenEye ransomware variants shook the tech and business world. Traditionally designed as a for-profit malware scheme, ransomware encrypts important files on computers and demands a ransom to give you access to them again.

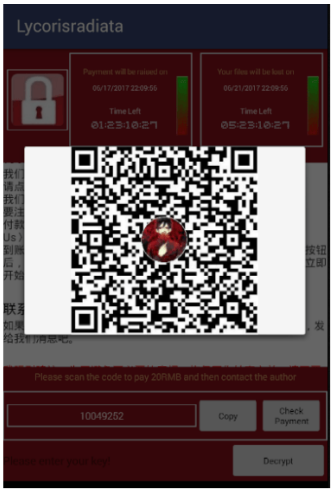
These cyberattacks mainly targeted outdated and unpatched Windows machines which were utilizing outdated software. But now cybercriminal have began targeting mobile platforms, such as Android devices.

Trend Micro researchers have uncovered a new variant of the SLocker Android ransomware and it's said to be copying the look and interface of WannaCry.

SLocker is one of the oldest Android screen locker and file encrypting ransomware around. It tricks its victims to pay the ransom by impersonating various law enforcement agencies like the FBI or the "Cyber Police." This strain of malware even crossed over to Android-powered smart TVs in the form of Flocker.

This ransomware variant are fake game guides, video players, and other apps that trick would-be victims into installing it. The sample captured by Trend Micro was disguised as a cheating tool for the game King of Glory. All apps originate from China.





Once installed, the icon for the malicious software looks nothing out of the ordinary since it appears like a regular game guide or cheating app. When it runs, it changes its name and icon and alters the infected Android gadget's wallpaper.

The ransomware then checks if it's been installed on the gadget before. If not, it then proceeds to search for certain text, pictures and video files (must be larger than 10 KB and smaller than 50 MB) on the gadget's storage and encrypts them.

Once the files have been encrypted, the victim is then given three options to pay the ransom, which curiously still led to the same payment destination. Thankfully the cybercriminals were arrested in China, however this should be a warning to all mobile users.

PROTECT YOUR MOBILE DEVICE

With the ever-growing threat of ransomware, you need to take precautionary steps. Here are suggestions that will help:

- Avoid downloading and installing apps from "Unknown Sources." - Only download apps from the official Google Play app store and make sure you check user reviews, too, before installing.
- Back up data regularly - this is the best way to recover your critical data if your computer is infected with ransomware.
- Make sure your backups are secure - do not connect your backups to computers or networks that they are backing up.
- Never open risky links in emails - don't open attachments from unsolicited emails, it could be a phishing scam. .
- Have strong security software - this will help prevent the installation of ransomware on your gadget.

Summer Cooling Centers Information

During hot summer weather, the Niles Family Fitness Center and Niles Senior Center are open as cooling centers during regular operating hours if relief is needed. The Fitness Center is 5:30am-10:00pm Monday through Thursday, 5:30am-9:00pm Friday and 7:00 am—5:00pm Saturday and Sunday. The Senior Center is open 8:30 am-5:00 pm Monday through Friday. Please call the Niles Police at 847-588-6500 after hours or **in an Emergency, call 9-1-1.**

Summer Crime Prevention Tips

Summer brings warmer weather, longer days and the possibility of an increase in burglaries and other types of crime.

The Niles Police Department is asking for renewed diligence from our residents to help prevent the occurrence of these incidents. There are many simple things you can do to keep yourself from becoming a victim.

Vehicles:
Keep vehicles locked with the windows up at all times, when they are not occupied. Remove all valuables including purses, wallets, cellular phones, MP3 players, GPS systems, laptop computers, sports equipment, etc. when vehicles are parked. Many vehicles also contain an automatic garage door opener, which would allow a burglar easy access to your garage/home. Park your vehicles in a locked garage when possible and keep the keys inside your home.

Homes:
Keep all doors closed and locked. This includes garages, sheds, and patio doors. Burglaries from open garages, sheds, and residences are more prevalent in the summer months, and sometimes even occur when the homeowner is present.

Summer vacation plans:
Stop delivery of mail and newspapers, or have a trusted neighbor pick them up. Set inside lights on a timer to turn on during the overnight hours. Set your burglar alarm, and have a neighbor watch your residence while you're on vacation. Make sure to leave contact information with them on how to reach you by telephone, while you're away. Inform them to contact the Broadview Police Department immediately, if they encounter any suspicious activities.

If you do not have a neighbor to look after your home while you're away, contact the Niles Police Department at (847) 588-6500 or go online to https://www.vniles.com/188/See-It-Report-It. Officers will check the premises periodically to make sure everything is secure.

New Medicare cards are on the way

Changes are coming to your Medicare card. By April 2019, your card will be replaced with one that no longer shows your Social Security number.

Instead, your card will have a new Medicare Beneficiary Identifier (MBI) that will be used for billing and for checking your eligibility and claim status. And it will all happen automatically – you won't have to pay anyone or give anyone information, no matter what someone might tell you.

Having your Social Security number removed from your Medicare card helps fight medical identity theft and protect your medical and financial information. But even with these changes, scammers will still look for ways to take what doesn't belong to them. Here are some ways to avoid Medicare scams:

- Is someone calling, claiming to be from Medicare, and asking for your Social Security number or bank information? **Hang up. That's a scam. First, Medicare won't call you.** Second, Medicare will never ask for your Social Security number or bank information.
- Is someone asking you to pay for your new card? That's a scam. Your new Medicare card is free. Is someone threatening to cancel your benefits if you don't give up information or money? Also a scam. New Medicare cards will be mailed out to you automatically. There won't be any changes to your benefits.

Upcoming Events
National Night Out
August 1,2017
Oak Park (Main & Ottawa)

Don't forget to join us for the National Night Out at Oak Park, on August 1, 2017 from 6 pm to 9 pm. Bring a friend, family member or neighbor to send a symbolic message to crime that you don't want them in your community

Scams in the name of charity

Scammers are creative, cunning and cruel — and they often mix in a little truth to spice up their big lies. This scheme shows just how low they can go.

Government imposters claiming to be with the FTC, or another agency like the fictitious "Consumer Protection Agency," are calling to inform people they have won a huge sweepstakes from the Make-a-Wish Foundation, a well-known charity for very sick children. To get the money, the callers say, the "winner" must first pay thousands of dollars to cover taxes or insurance on the prize. The call may even come from a 202 (Washington, DC) area code to appear credible — since the headquarters for the FTC and most federal agencies are in DC.

This is just a scheme using the well-known names of Make-a-Wish and the FTC to rob thousands of dollars from people. Once you wire money or send banking information, you will never see your money again.

Here are a few facts and tips to protect yourself and others:

- If someone asks you to wire money or provide your bank account information over the telephone, it's a scam.
- Anytime you have to pay to get a prize, it's a scam.
- The FTC doesn't oversee sweepstakes and no FTC staff is involved in giving out sweepstakes prizes. We do, however, go after sweepstakes scams like this one.
- If an FTC case results in refunds, you can find the details at ftc.gov/redress.
- The Make-a-Wish Foundation has information about this specific scam on its fraud alerts page.
- If you encounter this or other scams, report it to the FTC at 1-877-FTC-HELP or ftc.gov/complaint.
- Talk to your friends and family about scams. Visit FTC.gov/PassItOn to find out how.

Source: FTC.gov

Top Five Chicago and Northern Illinois Summer Sizzling Scams: BBB Offers Tips on How to Avoid Them

Fraudsters often change their tactics with the seasons, and continue to come up with new schemes to scam businesses and consumers. With the official start of Summer, local data just compiled from BBB Chicago and Northern Illinois Scam tracker shows the hottest summer scams to watch out for in our region. Better Business Bureau has been able to pinpoint the top five summer scams in the Chicago region so you know what to avoid.

BBB president and CEO, Steve J. Bernas says, "We know that scams are cyclical, as an example, every summer we see an increase in employment related scams. With our new data, we are able to better gauge the impact of those scams and others."

Number one on the list this summer:
Tax collection scams - Commonly known as the IRS Scam - 50% of all reported scams and inquiries fall under this category. While tax scams are nothing new, the various schemes fraudsters are coming up with are new. In the latest twist, the Internal Revenue Service is warning people that scammers have added reference to the automated Electronic Federal Tax Payment System (EFTPS).

Here's how it works:
Scammers claiming to be from the IRS are calling victims and telling them they've sent out two certified letters in the mail that were returned as undeliverable. They use this new twist to seem more legitimate because the IRS mails letters to communicate with taxpayers. If you receive a phone call saying mail sent to you from the IRS was undeliverable and your address is still the same as the last tax return you filed, then it's probably a scam.

The IRS (and its authorized private collection agencies) will never:
Call to demand immediate payment using prepaid debit cards, gift cards or wire transfers.

- Threaten to have you arrested.
- Demand that taxes be paid without giving the taxpayer the opportunity to question or appeal the amount owed.

Other scams on the top five list are:
2. Government Grants - Fake calls and notifications saying you have an accepted grant.
3. Employment - Identity and money theft is common attack on job seekers
4. Tech Support - Scareware, Ransomware, and false tech support calls
5. Online Purchases - Everything from fake ads to bogus websites and merchandise

Source: BBB Chicago