AUGUST EDITION | Chief of Police Dennis J. Mc Enerney | Volume 3, Issue 8

S.C.R.A.M. GAZETTE

Text Message Scams

A common scam is to send text messages, that may appear to be from legitimate sources such as banks or your cellular company. The message says you need to update your profile information and then provides a link to a website. The URL may even include the name of your bank.

Once you click on the link, it takes you to a form that appears to be on the bank's website. The page will then ask you to "confirm" your identity by entering your name, user ID, password and/or bank account number. **Do not do it!** Taking the time to log in to your online bank account through a secure network is a lot easier.

Here's a general rule of thumb for avoiding these types of scams:

- Do not click on any link in any email or text message that you were not expecting. If there's a question and you think there's a legitimate message or notification intended for you, go directly to the official website of whatever business it is and check for any notifications there.
- If your bank needs you to update your profile, you should be able to find that information by logging in to your account separately through the official site -- or by calling your bank directly.
- Just hit delete! Ignore instructions to confirm your phone number or visit a link. Some scam texts instruct you to text "STOP" or "NO" to prevent future texts. But this is a common ploy by scammers to confirm they have a real, active phone number.
- Read your phone bill. Check your phone bill for services you haven't ordered. Some charges may appear only once, but others might be monthly "subscriptions."
- Know your rights. Real commercial text messages must provide a free, easy way for you to opt out of future communication. Learn more here.
- Know how to combat spam texts. In the U.S., forward the texts to 7726 (SPAM on most keypads). This will alert your cell phone carrier to block future texts from those numbers.

Ransomware continues to spread

Ransomware continues rise and cause fear amongst the general public, yet many people fall for this scam.

Hackers are becoming bolder in attacking computer systems and demanding payment. They are not just targeting bi -name corporation. Ransomware can happen to anyone, anywhere or anytime.

Hackers have become extremely adept at tricking you to click on their links, or open an infected attachment. They could be a familiar email from what you might think is your banking institution or from some well-known brand, like Apple or Disney.

Because of the high volume of data breaches and hacks that your personal information may have become compromised. Many companies are ill equipped to prevent hacking on their systems, as a matter of fact an Accenture report revealed that one in four consumers have been hacked without know it.

Because we conduct business or access different sites utilizing email addresses it opens the door for hackers to target your inbox. They utilize links within emails or attachments to target you with malware. Once the malware is installed, there is almost no way to remove it, locking you out of your system. Your only option, short of a complete wiping out of your hard drive is to pay a fee to the hacker.

But the newest way to target us is through our mobile devices, including our cellphones and tablets.

One your mobile device is infected with malware the screen locks up and the display may have obscene pornography. The hackers claim they are from a law enforcement organization and will give the potential victim just 72 hours to pay the “fine” or they will report them to the Department of Homeland Security.

The best way to protect yourself is to prevent the attacks from ever getting through. Here are some helpful tips:

1. Stop Ransomware—Keep your operative system and web browser up to date is critical. Know how to install the latest updates for Windows.
2. Prevent it from running—If a malicious ransomware hits your inbox, you can in fact prevent it. Don’t click anything that looks suspicious.
3. Have a backup plan– if malicious ransomware bug happens, its not over. Most security company can clean them out and decrypt your files. For new ransomware you need to back-up your data, protect it on an external drive or cloud system.

National Night Out
August 2, 2016
5:30 pm
Oak Park

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

Connect with US!

WWW.NILESPD.COM

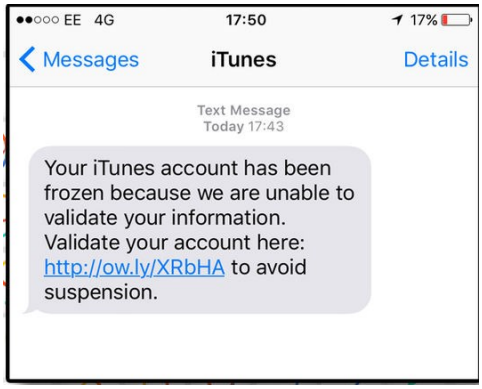
The IRS doesn't want your iTunes cards

If anyone tells you to buy iTunes cards to pay the IRS, qualify for a grant, get a loan or bail out a family member, say "No." They're trying to scam you. The only place to use an iTunes card is at the iTunes store, to buy online music, apps or books.

People have told the FTC about scammers who called and demanded iTunes cards as "payment." Bogus "IRS agents" told people they owed back taxes and would be arrested soon, unless they bought an iTunes card and gave the code to the "agent." Phony "government grant" officers called and promised a big payout, after the person bought an iTunes card and read the code to the "grant officer." Other fraudsters told people their grandkids were in jail and the only way to help was — you guessed it — to buy an iTunes card and read the code over the phone. All the stories were false.

There's a reason scammers insist on getting iTunes cards: Once you tell a scammer the code from the back of an iTunes card, he takes control of the value on the card. He can use the code or sell it. After a person redeems the code, you can't get your money back.

If you gave someone the code from an iTunes card and you think it was a scam, call Apple Support at 1-800-275-2273 right away (you may have to spend some time on hold). Tell them what happened and ask if they can disable the card. Also, go back to the store that sold you the card and talk with their customer service staff. And if you hear from someone who wants you to send an iTunes card, please tell the FTC.. If you gave someone the code from an iTunes card and you think it was a scam, call Apple Support at 1-800-275-2273.



Some safety tips that iTunes will never ask your for email:

- Social Security Number
- Mother's maiden name
- Full credit card number
- Credit card CCV code

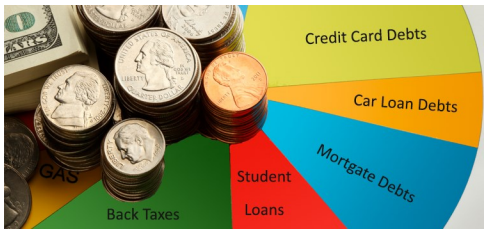
"Phishers" create elaborate websites that look similar to iTunes, but their sole purpose is to collect your account information. Often, a fake email will ask you to click on a link and visit one of these phishing websites to "update your account information."

Debt Relief and Credit Repair Scams

Debt relief service scams target consumers with significant credit card debt by falsely promising to negotiate with their creditors to settle or otherwise reduce consumers' repayment obligations. These operations often charge cash-strapped consumers a large upfront fee, but then fail to help them settle or lower their debts – if they provide any service at all. Some debt relief scams even tout their services using automated "robocalls" to consumers on the Do-Not-Call List.

Auto loan modification scams falsely promise that they can reduce consumers' monthly car loan or lease payments to help them avoid repossession. The FTC also works to make sure consumers get a fair deal in the auto marketplace.

Credit repair scams also frequently target financially distressed consumers who are having credit problems. These operations lure consumers to purchase their services by falsely claiming that



they will remove negative information from consumers' credit reports even if that information is accurate.

•The following tips may help you avoid scams:

- Fraudulent debt relief companies will often make claims of being able to negotiate a one-time settlement with creditors that will reduce a consumer's principal by fifty percent or more. The Consumer Federation of America, an association of non-profit consumer organizations, warns that such a promise is a virtual impossibility.
- If you have trouble making credit card payments, immediately call the creditor to work out a payment plan. If that is unsuccessful, a non-profit credit counseling service may be able to help you. These services may charge a small fee, but the cost will be substantially less than using a debt relief company. An excellent resource for locating a local credit counseling service is the National Foundation for Credit Counseling, atwww.nfcc.org.
- If a company offers a "one size fits all" solution, what they are really offering is a "no size fits anyone" problem. Legitimate credit counseling services tailor a consolidation plan to each consumer's individual needs.
- Do not be afraid to ask questions. Demand that the company disclose set-up and maintenance fees, and that these fees be set in writing. According to the Consumer Federation of America, consumers should not pay more than $50 for the set-up fee and $25 for monthly maintenance of the account.
- Do not rely on the company's website. Conduct your own searches of the company – the Better Business Bureau and state consumer protection agencies are excellent resources.