FEBRUARY EDITION Chief of Police Dennis J. Mc Enerney 2017—Volume 4, Issue 2

S.C.R.A.M. GAZETTE

Tax Season means Tax Scams, be aware of the risk

CHICAGO – January 23, 2017 - The IRS has announced that the start date for the 2017 Tax season is January 23rd. The IRS will begin accepting tax returns for 2016, both filed electronically and those filing paper returns.

Again, in 2016 tax scams led the list of the top ten; and with the IRS predicting more than 153 million returns to be filed, that is fertile ground for tax scammers. The IRS continues to increase its efforts against refund fraud, which includes identity theft. As a result of these aggressive efforts to combat identity theft from 2011 through November 2013, the IRS has stopped 14.6 million suspicious returns, and protected over $50 billion in fraudulent refunds.

However, IRS impersonation is on the rise. The U.S. Treasury Inspector General for Tax Administration recently projected that victims collectively have paid more than $50 million to scammers posing as IRS officials since October 2013. The average amount lost is $5,200.

TIPS FOR AVOIDING TAX SCAMS:

Hang up on fake calls: The IRS will not call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill. The IRS will not require a specific payment method or ask for credit or debit card numbers over the phone. **Lastly, the IRS will not threaten to bring a local police and have you arrested for not paying. You can report it at: "IRS Impersonation Scam Reporting" on irs.gov or call 800-366-4484.**

Don't open e-mail attachments or click on links: For emails – Don't open any attachment, forward it to the IRS to phishing@irs.gov and then delete it. The IRS doesn't initiate contact with taxpayers by email to request personal or financial information. All contact is via U.S. Post Office.

This year the scams consumers are most likely to see: (A special thanks to the Internal Revenue Service for helping compile information to help combat fraud.)

- **Fake CP2000 Notice** – A relatively new scam, be on guard against fake emails purporting to contain an IRS tax bill related to the Affordable Care Act. Generally, the scam involves an email that includes the fake CP2000 as an attachment. (The CP2000 is a notice commonly mailed to taxpayers through the United States Postal Service. It is never sent as part of an email to taxpayers.)
- **Paying the "federal student tax"** – The IRS warns the public about bogus phone calls from IRS impersonators demanding payment for a non- existent tax, the "Federal Student Tax." The scammers try to convince people to wire money immediately to the scammer.
- **Tax-related ID Theft** – The Federal Trade Commission reports that since 2009 tax or wage-related fraud has been the fastest-growing way that identity thieves misuse victim's information. Protection recommendations include never carrying your Social Security card, protecting your personal computer with anti-virus software, and being extremely careful with your personal information.
- **Tax relief scams** – Consumers who owe back-taxes, sometimes out of desperation, readily fall victim to claims from scammers that they can free taxpayers from having to pay the IRS. They claim to be able to settle the debt for pennies on the dollar. These shady businesses and individuals charge exorbitant up-front fees ranging from $3,000 to $25,000. Consumers who are having trouble paying their taxes should: Contact the IRS or state comptroller.

Source: BBB Chicago

Netflix Scam, don't fall for this phishing expedition!

Hackers might be after you just because you love Luke Cage and Stranger Things. A new phishing scam is targeting Netflix users with an email requesting that you update your user information.

As detailed by the cybersecurity firm FireEye, once the user clicks through, they're taken to a site that looks exactly like a typical Netflix login page. They're banking on you being so excited to watch there favorite shows that you don't notice that a few things are amiss.

Once you've logged into the fake site, it'll request you update your credit card information, personal details, and your social security number. ***Netflix does not require your social security number, so anytime you see Netflix asking for it, that's a red flag that something's not right.***

Once you've handed over your personal information, the site redirects you to the Netflix homepage, making the whole scam feel pretty legit.

FireEye also notes that it's a unique scam in that the "phishing pages were hosted on legitimate, but compromised web servers." The site also uses techniques that help it get around standard phishing filters.

The firm notes that as of Jan. 9, the sites they were monitoring connected with this scam were no longer operational. But to be safe, don't hand over personal information after receiving an email like this from Netflix.

In fact, don't trust anyone who emails you. If your mom emails and asks what your birthday is, it's a trap. Tell her nothing.

But seriously, don't trust a Netflix email that is asking for your social security number.

Source: Thrillist.com

Next Presentation
02/13 @ 11 AM
"Telemarketing Scams"

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

Connect with US!

WWW.NILESPD.COM

Your private web activity is not as private as it seems

Web browsers, online tracking companies, and advertisers always claim that they only collect and analyze anonymous data and non-personally identifiable information. The browsing histories that are collected by these entities, or so they say, cannot be tied to any specific user they assure us and does not pose a threat to our individual privacies.

But is this true? Can't this "anonymous" browsing data be easily deanonymized and traced back to a specific user by merely linking it to something as prevalent as social media activity?

This is the question a group of researchers from Standford and Princeton sought to answer with a paper titled "De-anonymizing Web Browsing Data with Social Networks" set to be presented at the 2017 World Wide Web Conference in Perth, Australia.

In this study, they conducted simulations and strategies that can prove how network adversaries, or someone with malicious intent, can de-anonymize browsing histories by simply matching them with specific social media profiles like Facebook or Twitter.

"An adversary can thus de-anonymize a given browsing history by finding the social media

profile whose 'feed' shares the history's idiosyncratic characteristics," the paper states.

Their strategy included the correct matching of a simulated history of 30 Twitter browser links to a correct Twitter profile with a more than 50 percent success rate and the correct matching of 400 recruits' donated browsing histories at a 70 percent success rate.

"Our approach is based on a simple observation," the paper continues." Each person has a distinctive social network, and thus the set of links appearing in one's feed is unique."

They further stress that since their matching attempts to locate the right profile includes over 300 million Twitter candidates, it is "the largest scale demonstrated de-anonymization to date."

Their unmasking technique is feasible for any entity with access to browsing histories such as third-party trackers, government surveillance spies, internet service companies and public Wi-Fi snoopers. They note that any social media site can be used for this de-anonymization strategy, as long as each user's social media subscriptions can be named, the social media content is public and the user visits enough links from the social media site.

With this study, the group states that they are making three key contributions to the study of web de-anonymization. First, they have developed a general theoretical framework for de-anonymization. Second, they have successfully implemented and evaluated social media and browsing de-anonymization and third, they have created an experiment for testing their strategy on real browsing histories.

However, the group admits that their results are proof-of-concept and their sample of 400 users is not representative of the entire population.

One thing is for sure, though - social media site activity linking is just another tool that can be used to unmask even the older most private and anonymous data that's being collected on the web.

Source: Kimkomando.com

Gmail phishing scam is even fooling tech-savvy users

According to security expert Mark Maunder, the CEO of a WordPress security plugin called Wordfence, the hacker will first send you an email that includes an attachment. When you click on it, you're directed to what looks like a Gmail login page, according to Fox 59.

However, it's a fake. If you enter your email and password, you're giving your login credentials to hackers who then have complete access to your emails.

Sounds easy enough to avoid, right? Not exactly—the email looks like it comes from one of your contacts. It may even have a subject line that looks authentic. The hackers, who've likely compromised your contact's account, will even rename the attachment to something that appears plausible.

Once your account is compromised, scammers will use your contacts to send more emails in attempts to obtain new login credentials.

Even the URL redirecting you to login to your Google account looks authentic:

Fake login page: data:text/html,https://accounts.google.com/ServiceLogin?

Gmail login page: https://accounts.google.com/ServiceLogin?

The fake login box looks like the one you'd really use.

To combat this tactic, security experts say Gmail users should enable two-factor authentication, which gives you an extra layer of security. Unless the scammers have access to your phone, they won't have the access code to get into your account.

Experts say you should also look for the "lock" icon next to the address bar denoting a secure website. While it's not a foolproof method because scammers sometimes host their pages on secure servers, it's a commonsense step to take.

If you think you've already fallen for the scam, you should change your Gmail password immediately. For more information about the scam, go to this website.

Here's the response Google sent about the scam:

"We're aware of this issue and continue to strengthen our defenses against it. We help protect users from phishing attacks in a variety of ways, including: machine learning based detection of phishing messages, Safe Browsing warnings that notify users of dangerous links in emails and browsers, preventing suspicious account sign-ins, and more. Users can also activate two-step verification for additional account protection."

Source: wgntv.com news 9 Chicago

2017 Presentation

February 13	**Telemarketing Scams**
March 15	**Sweetheart Scams**
April 17	**Home Repair Scams**
May 17	**Financial Exploitation**

All presentations start at 11 a.m.