Having trouble viewing this email? www.mignolet.com

Like

MIGNOLET
BUSINESS RESEARCH CONSULTANTS, INC.

10 Tips for a safer Tax Season

Tax Refund Fraud

10 tips - online banking safety

For more than three decades Jean Mignolet has served in law enforcement and private investigation, managing all aspects of general investigative business. She specializes in in-depth background investigations, and is the top choice of attorneys, corporations, small business owners and individuals who require all types of investigative services.

For further information visit: www.Mignolet.com

Contact us at: investigators@Mignolet.com or call us at: 954-523-8737

Jean,

It's tax time so I've decided to dedicate this issue to banking and IRS Fraud. Even my mother and close friends have been victims of ID theft with the subsequent IRS return fraud.

The good news is that my brother, Neil Karadbil, an Assistant US Attorney with the Southern District of Florida and his team successfully convicted two defendants for their participation in a stolen identity tax refund scheme resulting in millions of dollars in fraudulent activity.

A copy of this press release may be found on the website of the United States Attorney's Office for the Southern District of Florida at http://www.usdoj.gov/usao/fls.

Jean Mignolet

A reminder that prior issues of the newsletter are viewable from my website.

Quick Links

Our Website

Services

Join Our Mailing List!

Fraudulent Tax Returns net nearly $4 billion for Cybercriminals

Consumers face risks during tax season and their identities need protection when filing their tax returns, especially online. Almost 93% of returns are filed online, creating a crucial need for cybersecurity.

The top five cities for the most fraudulent tax returns are Chicago, Detroit, Atlanta, Houston, and Miami.

Once our tax information is online, it remains there FOREVER. More than 125 million tax returns were filed online in 2013, twice the number filed in 2012.

Cybercriminals have derived strategies to manipulate tax returns for personal gain, including FRAUDULENT RETURNS and IDENTITY THEFT.

Last year the IRS gave away almost $4 billion in fraudulent tax
refunds. Cybercriminalscreate illegal file returns in their name and often receive those

10 TIPS FOR SAFER ONLINE BANKING

It's convenient and most of us do it; online banking. However, now we ask ourselves what is the risk of being compromised by hackers and those who illegally access our accounts due to identity theft.

The most important thing that you can do is monitor your account(s) closely. More than two million people per year have money stolen from their bank accounts, losing on average close to $1,200 or more.

Of course, you don't have to be online to become a bank fraud victim. Crooks gain access to your account and debit card details through a variety of "old school methods".

Even when I tried to stop my health insurance company from debiting my bank account since I had switched insurance companies I was told that my payee had to agree to stop withdrawing the insurance premium amount. This is an ACH (Automatic Clearing House) debit which most companies prefer than having bank checks automatically sent via the mail.

Here are some helpful guidelines to assist you in keeping your financial life safer:

*** You need to log into your account(s) to closely monitor your balances and payments often;**

*** Refrain from doing your online banking transactions in public areas or on public networks because access is more readily available to cybercriminals;**

*** Avoid clicking on links to your bank in an email. It's much safer to go to the actual website and login. Do NOT**

returns on pre-paid cards which readily convert into cash.

Here is a list of some of the specific ways in which tax refunds may be compromised:

1. Identity theft;

2. Phishing - the use of fake IRS messages and letters, mostly using recent text messages and social media channels to get information;

3. Return preparer fraud - which is encompasses a variety of crimes from identity theft to false statements and refund skimming, perpetrated by people who prepare your return for you;

4. Hiding income offshore - The IRS continues to work with the Department of Justice to track down tax evaders and take legal action;

5. "Free Money" scams - Beware...there are a number of schemes that falsely claim you can file a return without documentation and receive refunds even if your income is so low that you don't normally file;

6. Impersonation of charitable organizations - This happens frequently and the scam is extremely plausible. A typical version of this scam might be a call to victims of natural disasters, claiming to be from the IRS, offering to help them file loss and refund claims. Be alert. This is most likely an attempt to gain access to

log in from your Google searches or other searches go directly to the actual website or page. The email could be a fake that appears genuine. Clicking links could lead to a spoof bank site phishing for your sign-on details. Even if it is legitimate, the best practice is to go to the website itself.

*** Check to see that all sites are secure by looking for the "https" at the beginning of the website address. The "s" verifies that is *secure* ("s").**

*** Change all your passwords regularly, and be sure that your antiviral software is up to date. Malware can capture passwords when you key them in if your antiviral software doesn't prevent that from happening so constantly update.**

While this is a fairly comprehensive list that when followed can help you travel a much safer online/financial road, be aware that nothing is 100% hack proof these days.

Crooks have become more sophisticated and computer technology has changed. Therefore, law enforcement and financial protection organizations have added more recommendations to bolster your online banking defenses and it's a good practice to question what your bank or institution might be using just so you can sleep better at night knowing you are safer than the day before.

If you are banking on your hand held devices, please try and follow these tips:

*** If you use a mobile device for your banking, make sure it's properly protected against physical theft. That puts the responsibility on you to keep your device(s) close to you at all times. Some devices have alerts that will tell you buzz, ring, chime or sing out (your choice of music) to let you know that you have left it behind.**

Do not set up automatic logins to any accounts because it's much easier for a hacker to access your information. Take the extra 20 seconds to log in each time you log on.

Do *password protect* your device(s) so thieves can't access it at all. Each device is different so when you purchase it ask

Social Security numbers. Callers may also pose as an aid service and charge fees.

7. False or inflated income and expenses - his may be for a various reasons, such as minimizing taxable income, or maximizing potential income for refundable credits such as Earned Income Tax Credit;

8. False 1099 Refund claims - This is a long-running scam in which people file a Form 1099 Original Issue Discount with the belief that this will secure refunds based on the notion that the U.S. government has a secret account in your name, which is accessible via this technique.Of course, it's not. **Beware of people offering to help you get your hands on this non-existent money.**

9. Frivolous arguments - False 1099s are just one of numerous misplaced beliefs that there are ways of securing refunds to which you're not justifiably entitled.

10. Falsely claiming zero wages - This is usually done by filing a "corrected" W2 or 1099 canceling previously filed documents, so as to imply that you didn't earn a cent. People who practice this face a $5,000 penalty, in addition to payment of outstanding taxes.

11. Disguised corp ownership - This is a complex series of tricks using specially set-up companies to hide earnings and claim fictitious

how to password protect it, or if you already have a device and you haven't done so, call the manufacturer or go to the local store and ask how. This includes laptops, tablets, cell phones, iPads, and any other mobile device you are using.

DO NOT store passwords for sensitive accounts on your devices or in your browsers no matter what you are using. There are password managers where you can store all of your passwords, but for better safety, I would simply put them in a safe place where no one can get to them. This is a personal option.

There are a number of password managing products such as Scambusters which includes Last Pass (free), KeePass (free) and RoboForm (paid-for and free versions).

Whether you utilize a password managing product or simply have another system, be sure to generate difficult passwords that are not easy to figure out.

Here are a few more tips:

*** Always *log out* after using your online account(s). Do not simply hit the "close" buttons that are on your menu bar. By logging out you are assuring that you have CUT OFF immediate access to your information. This prevents a hacker or possibly a burglar from gaining access.**

Most banks and some other accounts online will automatically log you out after a brief period of time due to inactivity - each one is different - maybe 5 minutes, maybe more or less. DO NOT COUNT ON THAT. Log yourself out *each and every time.*

*** Some banks offer extra security through what is known as "two factor authentication" which is exactly what it states. You must enter your ID, password, and then some other form of verification before you can access your account. One bank I know has 3 factors that you must get through before you can gain access to your account.**

The extra step might be a text message to your phone with a specific site key or with others you may have to answer personal questions.

deductions.

12. Misuse of trusts - This is another series of complicated structures designed to hide assets or avoid tax payment.

After a legitimate user files his or her tax return online, cybercriminals compromise the system and steal personal and identifiable information typically included in a return, such as names, banking accounts and social security numbers.In the first half of 2013 alone, 1.6 million taxpayers were affected by identity theft.

Another form of identity theft results from fraudsters utilizing social networks to spot potential targets. They collect taxpayers' information which is used to accurately complete a return.

Cybercriminals gather personal details such as a user's number of children, marital status, and employer to piece together a person's identity, which can help them claim the correct number of dependents and estimate an annual salary in order to file a fraudulent return.

The launch of a new IRS mobile app this year poses additional risks for tax return fraud.

The app provides information on a user's refund status and tax records, as well as a portal that allows taxpayers to download their returns as far back as 2009.

Banks are offering other additional security codes and passwords to make it tougher for criminals to access your information. To learn more about two factor authentications, see this Wikipedia entry: http://en.wikipedia.org/wiki/Two-step_verification

*** Arrange for your bank to send your balance and transaction notifications either daily or in intervals to let you know what activity is going on with your accounts.**

Be certain that you are working with a properly constituted bank because just as criminals can set up fraudulent online stores, they can also set up BANKS THAT REALLY DON'T EXIST.
If you are just starting out with online banking and setting up a new bank, be CERTAIN that
you read the US Federal Deposit Insurance Corporation (FDIC) "About Us" section on a bank website. It will show its history, official name and main office (corporate headquarters) address. The bank should also be covered by FDIC insurance to ensure your funds are properly protected.

The FDIC logo should be easily located on the webpage but if this is a bank that you have not heard of or properly researched, note the FDIC logo can certainly be duplicated/forged.

A good practice is to visit the FDIC's site and search the name of the bank to ensure its credibility. Here's the link: http://research.fdic.gov/bankfind/

If a bank isn't registered with the FDIC it doesn't necessarily mean it's a scam, however, it would be highly unusual and I would go with another bank that is. If it's an overseas bank that doesn't have FDIC protection for your funds and it folds, your funds will fold with it.

You can contact the FDIC toll free at 1-877-275-3342 to check the validity of a bank.

Finally, THE GOLDEN RULE, whether you bank online or at a physical bank, NEVER NEVER NEVER provide your personal account details in response to any messages,

Despite the convenience factor for consumers, these tools make it easier for cybercriminals to illegally obtain more personal and identifiable information than was previously available.

The key issue is that whatever you have put out there in the way of personal information will always be there for cybercriminals to access.

You can relieve some of the fear of it by knowing that there is usually a way to prevent these problems. Additionally, the IRS is trying new and improved strategies to prevent these crimes, and the more diligent you are about your information, the safer you will be.

including SMS texts, emails or pop-ups.

One of the popular scans is that you may be told your account is frozen, systems are being upgraded or all sorts of stories designed to convince you to disclose the information. REMEMBER, BANKS DO NOT WORK THAT WAY - NEITHER SHOULD YOU.

Now you're set for safer online banking --
but don't let your guard down!

HAPPY HOLIDAY