April 16, 2018

GENERATIONAL
WEALTH MANAGEMENT
A Registered Investment Advisor

Re: The Most Common Tax Scams of 2018 and How to Protect Yourself

As the 2018 tax season reaches a climax amid the flurry of late filings, tax scams have become increasingly more prevalent. It's phishing season for scammers attempting to lure unwary taxpayers into handing over their personal information, their money, or their identity.

Phishing—coined in 1996 by hackers stealing America Online accounts—is an Internet scam involving the use of deceptive email messages intended to dupe people into providing their personal or confidential information.

Scammers attempt to get credit card numbers, Social Security numbers, and user names and passwords to accounts by sending emails (phishing) designed to appear they're from trustworthy sources.

Here are this year's most common scams:[1]

Oops. That refund wasn't yours. Send it back now!

You completed your taxes early. A few weeks later, your refund is deposited into your account. Some time later, you get a call saying the refund was a mistake. Return the money immediately.

The big red flag here is the caller. The IRS doesn't call taxpayers demanding payment.

The caller in this case poses as a representative of a debt collection agency. Callers say they are acting on behalf of the IRS and the refund was made in error. They then tell the taxpayers to forward the money to the "collection agency."[2]

Another version of the scam involves automated messages of recorded voices saying you will face criminal fraud charges, an arrest warrant, and a blacklisting of your Social Security number. The message gives you a case number and a telephone number to call to arrange returning the refund.

Unfortunately, the flip side to this scam is the thief may have successfully arranged for the IRS to deposit a fraudulent refund into your account. If that's the case, you will have to refund the money with interest. But still, the IRS won't call you to demand you return the money.

According to the IRS, taxpayers filing electronically will have their returns rejected if another one with their Social Security number has already been filed. Taxpayers should then file a paper return and follow the agency's Taxpayer Guide to Identity Theft.[3] They should also send Form 14039, Identity Theft Affidavit.

Hello. We know who you are. Now, pay up or else!

Your telephone rings. It's a "tax official" from the IRS. You know you're in trouble. The caller says you've underpaid your taxes. And that's a big mistake. The caller is a "representative" of a collection agency working on behalf of the IRS. The caller demands you pay the difference now to avoid further trouble later.

This scam targets mostly immigrants, non-native English speakers, or hearing-impaired people who have to rely on special dictation software or other devices.

Scammers in this case use personal information they've been able to steal from you to give the erroneous perception that they're legitimate, which makes this scam more alarming.

By understanding what the IRS won't do,[4] you can better protect yourself against scams. Here are some pointers:

- The IRS won't call to demand payment with a specific payment method (a prepaid debit card, gift card, or a wire transfer). The agency first mails you a bill if you owe taxes.
- The IRS won't threaten to have you arrested by local police or other law enforcement agencies for not paying your tax bill.
- The IRS will not demand payment without providing you an opportunity to question or appeal the amount the agency says you owe.
- The IRS will not ask for credit or debit card numbers over the telephone.

If it looks like the IRS, if it sounds likes the IRS, it must be the IRS, right? Not so fast.

Scammers and identity thieves are becoming more sophisticated in their attempts to steal your money and your identity. You may receive an email from the "IRS"—even after you've filed your taxes. So, what's the big deal with opening the email? After all, the agency may just be seeking additional information or asking for clarification on an issue, right?

Typically, “IRS” requests are variations of the phrase: “You are to update your IRS e-file immediately.” Recall the definition of phishing as the “fraudulent use of deceptive emails.”

You open the email only to discover you’ve downloaded malware into your computer. Malware uses “computer viruses, worms, Trojan horses, and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting, or deleting sensitive data, altering or hijacking core computing functions, and monitoring users’ computer activity without their permission.”[5] In other words, you open the email, you open yourself up to identity theft.

The IRS makes first contact most of the time through regular mail delivered through the United States Postal Service. The agency will “call or come to a home or business, such as when a taxpayer has an overdue tax bill, to secure a delinquent tax return or a delinquent employment tax payment, or to tour a business as part of an audit or during criminal investigations. Even then, taxpayers will generally first receive several letters (called ‘notices’) from the IRS in the mail.”[6]

How do you protect yourself from phishing? Here are 5 tips to help keep your information, identity, and finances secure.

1. Don’t open phishing emails.
2. Don’t open emails from unknown senders.
3. Don’t click on hyperlinks or attachments from unknown senders.
4. Beware of emails promising gifts or money in exchange for participating in surveys or for providing confidential information.
5. Delete spam from your email.

A note on requests for donations from “charity” organizations: Legitimate and reputable groups never ask for confidential or personal information by email. Before deciding to donate to a charity from an email solicitation, thoroughly investigate the organization or nonprofit. You can report scams and phishing attempts to the Treasury Inspector General of Tax Administration at 800-366-4484.

As always, we are committed to protecting your identity and your financial future. Feel free to contact us if you have any questions about the information in this letter or any other financial matters.

Kind Regards,

The Team at GENERATIONAL WEALTH MANAGEMENT

Footnotes, disclosures, and sources:

Securities offered through First Allied Securities, Inc. A Registered Broker/Dealer. Member FINRA/SIPC. Advisory Services offered through First Allied Advisory Services, Inc. and Generational Wealth Management, Both Registered Investment Advisors. Generational Wealth Management is not affiliated with First Allied Securities and/or First Allied Advisory Services, Inc.

These are the views of Platinum Advisor Strategies, LLC, and not necessarily those of the named representative, Broker dealer or Investment Advisor, and should not be construed as investment advice. Neither the named representative nor the named Broker dealer or Investment Advisor gives tax or legal advice. All information is believed to be from reliable sources; however, we make no representation as to its completeness or accuracy. Please consult your financial advisor for further information.

We have not independently verified the information available through the following links. The links are provided to you as a matter of interest. We make no claim as to their accuracy or reliability.

Opinions expressed are subject to change without notice and are not intended as investment advice or to predict future performance.

---

[1] https://mic.com/articles/188047/tax-fraud-2018-income-tax-return-refund-scams-2017-to-beware-fake-irs-refunds-realistic-emails-phone-calls-phishing - .o4Y0DjiFW

[2] https://www.irs.gov/newsroom/scam-alert-irs-urges-taxpayers-to-watch-out-for-erroneous-refunds-beware-of-fake-calls-to-return-money-to-a-collection-agency

[3] https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft

[4] https://www.irs.gov/newsroom/tax-scams-consumer-alerts

[5] http://searchsecurity.techtarget.com/definition/malware

[6] https://www.irs.gov/newsroom/how-to-know-its-really-the-irs-calling-or-knocking-on-your-door-0