Defensive Cyber Operations – National Guard (DCO-NG)

ARMY NATIONAL GUARD (ARNG)

Advisory

AD-18-06	**"Tax Season Scams"**	**26 Feb 2018**

RISK

Medium

AFFECTED SYSTEMS

All Users

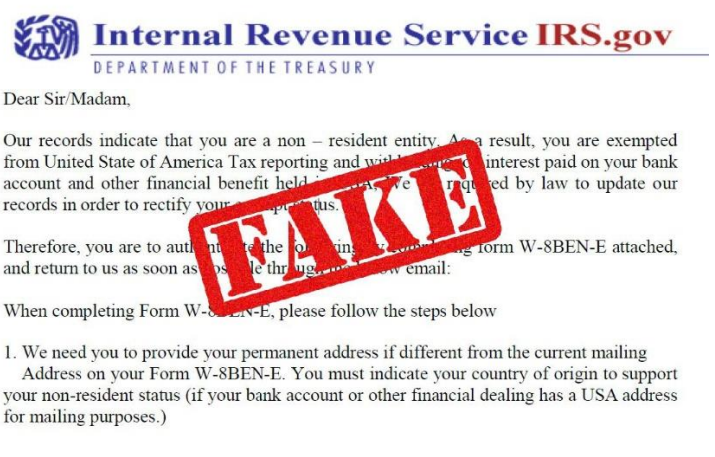
ISSUE

Providing useful and relevant information to the National Guard and its personnel is one of the many goals of the CSS-DCO. With the 2017 tax return season upon us, a surge in potential tax scams is likely to come with it. These scams come in many forms including fraudulent returns, phony calls, fake Internal Revenue Service (IRS) emails, as well as phishing schemes. These can lead to the theft of taxpayer money and/or personal data.

Fraudulent tax returns can be filed by malicious actors that have successfully acquired personal identifiable information (PII) from unsuspecting individuals. Typically the return is filed and the funds are sent directly to the malicious individual that filed. This year, however, the IRS is reporting that these malicious actors are now having the funds deposited into the account of the taxpayer and then calling the individual claiming to be from a collection agency acting on the behalf of the IRS. The caller states that the refund was deposited in error and asks the taxpayer to forward the money to their collection agency. Safeguarding your PII and filing your return as soon as possible will greatly reduce the risk of this happening as the IRS only accepts one tax return per Social Security Number (SSN).

Phone calls from individuals claiming to be IRS agents is another common tax scam used by malicious actors. These scams come in many varieties but usually, the malicious actor will call and explain that you owe taxes, fines or fees and convince you to make a payment over the phone. You can avoid being a victim of this scam by understanding that the IRS will never demand payment or call you without first mailing you an invoice. They will also never require a specific payment method, ask for a credit/debit card number over the phone, or threaten you for not paying.

Phishing is also widely used in tax scams. Phishing usually comes in the form of an email however, text messages can also be utilized. These phishing attacks are designed to appear as though they have come directly from the IRS. Tax season scams have become much more sophisticated over the years and some emails look official by including links to sites that look very similar to the official IRS website (IRS.gov). These scams can be avoided by understanding that the IRS does not initiate contact with taxpayers by email, text message, or social media.



Internal Revenue Service IRS.gov
DEPARTMENT OF THE TREASURY

Dear Sir/Madam,

Our records indicate that you are a non – resident entity. As a result, you are exempted from United State of America Tax reporting and withholding on interest paid on your bank account and other financial benefit held in the USA. We are required by law to update our records in order to rectify your status.

Therefore, you are to authenticate the following and complete form W-8BEN-E attached, and return to us as soon as possible through this new email:

When completing Form W-8BEN-E, please follow the steps below

1. We need you to provide your permanent address if different from the current mailing Address on your Form W-8BEN-E. You must indicate your country of origin to support your non-resident status (if your bank account or other financial dealing has a USA address for mailing purposes.)

FAKE

Defensive Cyber Operations – National Guard (DCO-NG)

ARMY NATIONAL GUARD (ARNG)

Advisory

MITIGATION

- Do not carry your Social Security card or any documents that include your SSN or Individual Taxpayer Identification Number (ITIN)
- Do not give businesses your SSN or ITIN just because they ask.
- Protect your financial information
- Check your credit report every 12 months
- Secure PII in your home
- Protect your personal computers by using firewalls, anti-virus software, updating security patches, and changing passwords for internet accounts on a regular basis
- Do not give personal information over the phone, through the mail, or on the internet unless you have initiated the contact and are sure of the recipient
- File your taxes as soon as possible

REFERENCES

"Tax Scams/Consumer Alerts"
https://www.irs.gov/uac/tax-scams-consumer-alerts

"Scam Alert: IRS Urges Taxpayers to Watch Out for Erroneous Refunds; Beware of Fake Calls to Return Money to a Collection Agency"
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

"Beware this year's dirty dozen tax scams"
https://www.msn.com/en-us/money/taxes/beware-this-years-dirty-dozen-tax-scams/ar-AAv4nHa?li=BBnbfcN&ocid=iehp

"Keeping Yourself Safe From Tax Scams Today"
https://turbotax.intuit.com/tax-tools/tax-tips/General-Tax-Tips/Keeping-Yourself-Safe-From-Tax-Scams-Today/INF26181.html

If you have any questions about this report, contact:
Defensive Cyber Operations – National Guard
ng.ncr.ngb.mbx.dco-ng-cnd@mail.mil
703-607-8455