Republic of Namibia

Financial Intelligence Centre

P.O.BOX 2882, Windhoek

Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

TAX-RELATED SCAMS

ISSUED: APRIL 2022

1. Background:

Over the years, several people have lost significant funds and their personal information to tax-related scams. Criminals are aware that filing tax returns may be complicated to some. It has been observed that taxpayers unwilling to personally file returns resort to working through third parties. They are therefore more vulnerable to scammers who could trick them into sharing their confidential personal and financial information.

Fraudsters use these schemes as a way of illicitly soliciting funds from members of the public through deceptive, dishonest and fraudulent means. These scams often result in huge financial losses for victims. The losses from such scams prejudice persons and often result in Money Laundering (ML) activities. Laundering activities generally have the potential to undermine the integrity of our financial system. The FIC is sharing this publication to help contribute to efforts geared towards combatting such activities.

2. How do these fraudulent scams operate?

Scammers are increasingly enhancing the sophistication and complexity of their methods. There has been a growth the number of tax-related scams deployed to advance fraud. Most people are familiar with typical tax-related scams wherein an unsolicited email may request persons to provide sensitive information, usually to those involved in identity theft. However, criminals continue to change their strategies and recent trends suggest that criminals are also sending SMS communications requesting sensitive or other private information. With these schemes, criminals simply call, send SMSes or emails under the disguise of some legitimate business or operation, usually requesting the recipient or taxpayers to provide personal information or click on a malicious link. Information directly availed through this means can be used to advance tax related scams or fraud. Clicking on malicious links equally results in unduly availing scammers access to otherwise confidential personal information or platforms that may contain such information.

Below are some common techniques of tax-related scams[1]:

[1] https://www.lifelock.com/learn/identity-theft-resources/irs-tax-scams-to-watch-out-for

1. ***Tax-related identity theft:*** *This type of scam occurs when scammers steal your personal information such as income tax number, address, birthdate/identification number and other significant information and use such to file an income tax return in your name. Criminals may organise this criminal practice to steal your tax return;*

How do you know when you have been a victim of tax-related identity theft?
You may try to file your return online only to have the online application rejected indicating that a tax return connected to your income tax number has already been filed;
You receive a notification indicating that your online tax account has been created in your name while you have never signed up for such an account; and
Receiving a tax-related transcript by mail that you never requested.

2. ***The refund recalculation scam:*** *Taxpayers may want the maximum tax refund possible when filing or submitting their income tax returns. Criminals are aware of this and are likely to take advantage. Criminals may contact taxpayers, either by email or text, affirming that they recalculated their income tax refund and that the said taxpayer is due to receive more funds than he or she may have anticipated. Such email may request the taxpayer to click on a link. If one clicks on such, you may be directed to a web page that would request for your personal information. If the taxpayer provides this information, the scammers will use such to access his or her online bank and credit card accounts or apply for credit cards and loans in such victim's name or try other organised crimes that would have a negatively impact the taxpayer's finance; and*

3. ***The Taxpayer Advocate scam:*** *These are criminals who pretend to be a taxpayer's assistants from legitimate institutions. In this scam, con artists call taxpayers using a number that appears to be from the legitimate institution. Sometimes these calls are made by a human being or robocalls that request taxpayers to return a call. When taxpayers answer such calls or return same, scammer request personal information. Once scammers have this information, they may use it to steal the taxpayer's identity, which can be further used to commit other fraudulent activities.*

3. How does one protect him or herself from these Scams?

Safeguard your tax number and other personal information. Never share personal or financial information to anyone who send you emails requesting this information.

Stay abreast of the latest security threats and if possible, use the latest security which can effectively block unwanted access to malicious sites and spam mails as well as detect malware.

Taxpayers and businesses should exercise caution. Never open links or attachments that come from unexpected or suspicious senders, especially when they claim to be from officials or agents of government Institutions.

Ensure that your computer and other devices are secure. When a software update is available, try to install it. Software updates often eliminate any potential or new security threats.

Verify the sender's contact details to ensure it matches that of the institution it purports to belong to.

Call institution directly if doubtful to verify information. Legitimate institutions do not request account updates or login information via texts or mails.

Visit the sender's legitimate website independently rather than providing information in the message.

REMEMBER

If you become a victim of a tax-related scam, or through any other fraudulent activity, immediately file a Suspicious Transaction or Activity Report with the FIC at the Bank of Namibia or report same to the Namibia Revenue Agency (NAMRA). Alternatively, you may contact the nearest police station to initiate a criminal investigation.