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

SOCIAL MEDIA SCAMS

ISSUED: FEBRUARY 2020

1. Background:

Social media platforms provide avenues that enables users to participate and share content, including multimedia content[1] usually online. Popular networks such as Facebook, Twitter, WhatsApp and Instagram provide an easy platform for one to instantly reach millions of active users all over the world. These benefits equally carry certain risks. Lately, the Financial Intelligence Centre (FIC) has observed a worrying increase in what is known as "Social Media Scams". This refers to criminal activities, operated on social media platforms, which are designed to trick innocent victims out of money, assets or even personal details.

The FIC has a duty to enhance public awareness with regards to known fraudulent schemes that the public could be exposed to. It is against this background that the FIC presents this communication.

2. How do these scams operate?

Social media has completely changed the way people interact and many people's lives have become very public as they share a variety of personal content online. Social media also offers several features that criminals may find attractive. Social media gives fraudsters the ability to hide their true identities by creating illegitimate (or fake) profiles and accounts, impersonating trusted sources. Social media also gives criminals the ability to reach many people with ease and at low cost. Below are some common techniques used by social media fraudsters:

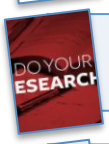
- Fraudsters claim to be genuine online sellers on social media sites such as Facebook. Consumers pay for goods, which then turn out to be counterfeit, poor quality or the goods are simply never delivered to the buyer;
- Fraudsters create illegitimate (or fake) profiles with which they make contact with individuals and lure them into an online relationship. They take time to build trust, then ask consumers to send money or share personal details;
- Fraudsters post false advertisements, news articles or messages to tempt consumers into investing in alternatives such as cryptocurrency (bitcoin). Consumers end up losing their investments or have their personal details stolen;
- Fraudsters hack into someone's social media account, then send messages to their contacts claiming to be in desperate need of help and asking them to send them money; and
- Fraudsters post products, services or rental properties advertised at very low prices, the seller insists on partial payment in advance, to reserve the place or the goods. Usually, the buyers who pay do not receive goods or receive goods which are not of the advertised quality.

[1] For example, text, audio, video, images, graphs and animations

3. How do I protect myself from social media scams?

Use strong, unique passwords that are not easy to crack;

Do not respond to any unsolicited messages;



Perform a thorough research on the investment opportunities offered on social media prior registering your personal details with them or handing over any money;

Do not pay a deposit or any partial payments before you have inspected the goods in person;

Do not avail all personal information on your social media profile such as your phone number and home address or banking details;

Be careful of individuals you meet through social media sites, especially if they promise romance, or get rich schemes; and

Set your profiles to private and restrict your social media contacts to people you know personally. In you are already a friend to someone on scoial media, be careful not to accept additional friend requests from existing friends.

Case Study 1:

John came across an advertisement on Facebook for a luxurious vehicle for sale. The set price for the vehicle is unbelievably low and the price is also negotiable. John immediately called the seller (Maria) and they agreed on the price for the vehicle. John then made a payment to the value of NAD 50,000.00 into account of Maria. Immediately, Maria withdrew all the funds and she deactivated the account. John never heard from Maria, nor received the vehicle he purchased. Maria's mobile number is unreachable.

Case Study 2:

Julia, a pensioner in Namibia started engaging Thomas on Facebook who lives in Congo. Although the two have never met in person, they have been communicating through various social media platforms for the past few months. Julia believes that she has found true love in Thomas, she is convinced that he is the man of her dreams. One day, Thomas reached out to Julia requesting for urgent financial help. He assured her that it is a loan, and he will pay her back every cent once he comes to Namibia. Julia transferred a total of NAD 500,000.00 into Thomas bank account in Congo. Initially, the local bank in Namibia placed a hold on the transfer, however, Julia requested the hold to be removed for such funds to go to the beneficiary. Upon receipt of the funds, Thomas immediately withdraws all the funds, he deactivated his bank account, and he was never in contact again. Julia never heard anything from Thomas since then, and she never got her money back.

REMEMBER

Although social media platforms allow us to connect with others, the platforms can also pose a threat if we are not cautious. Scammers are increasingly using these platforms to target consumers, and anyone can become a victim. However, if one falls victim to these scams, they should report it immediately to the FIC or nearest police station, and they should alert their bank immediately to stop facilitating any direct payments/deductions from their account to such schemes.