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

CHANGE OF BANKING DETAILS SCAM

ISSUED: MARCH 2021

1. Background:

Banking plays a significant role in the economy and especially in the movement of funds from person to person. Banking services are sadly also exposed to abuse to advance financial crimes. The Financial Intelligence Centre (FIC) has worryingly observed an increasing trend in what is commonly known as *"Change of banking details"* scams. 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 laundering 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 money laundering activities.

2. How do these fraudulent scams operate?

Scammers are increasingly enhancing the sophistication and complexity of their methods. There has been growth or increased use of the "change in banking details" scam.

Suppliers often share their banking details with clients for payment purposes. The scam is premised on fraudsters or scammers intervening between the communications of suppliers and their clients or customers or any two parties that are in a business relationship which may require movement of funds via banking platforms. A person or party would receive an email or letter informing them that the supplier has changed their bank account details. The correspondence would almost certainly include "new" or alternative banking details where funds should be paid to. Many a times, such communications request persons to update their records in order to ensure all future payments are directed to such "new" or alternative bank account. The details are, of course, fraudulent with the consequence that monies are paid to the fraudster and not the supplier or legitimate beneficiary. Individuals or businesses involved making bank payments or remittances are vulnerable to this scam. Below are some common fraud techniques used by defrauders[1]:

[1] https://www.datamills.co.uk/2018/12/beware-the-change-of-banking-details-email-scam

- The scammers may obtain innocent parties' usernames and passwords through phishing emails. Such can be used to hack into personal or business email accounts;
- Often, people would receive emails, letters or faxes supposedly from recognised suppliers;
- Such emails or other communication may look precisely like a genuine one from the supplier, using the right logos, layouts etc;
- The email may inform recepients of a change in bank account details and request that they update their records accordingly;
- The request for change in banking details may not be made via official correspondence or using the contact details that are within the known database of recepient; and
- As often observed, the recipient may pay funds to the said "new" bank account provided, assuming such change in banking details originate from legitimate party.

3. How do I protect myself from these Scams?

Ensure that to always confirm (either call or face-to-face engagement) any change in banking details with someone known by the party which is required to make such change. For example, This can be the CEO or payment officers, accountants of such supposed beneficiary;

In making the above-mentioned telephonic or face-to-face verification, it is enncouraged to estbalish contact by using the known contact details or such company or person, or the number listed in the telephone directoy, as oppsoed to the contact numbers availed on the communication which calls for changing of tbanking details;

Beware of identical email addresses. Scammers may add a full stop, replace one letter or the email may end with .com instead of .co.na;

Scrutinise all documents for spelling mistakes, errors, and suspicious changes made;

Maintain good relationships or constant contact/engagementwith existing suppliers. This helps to identify changes in communication patterns or any suspicious matters;

As a business owner, you may protect yourself by not placing your banking details on the invoices but rather providing them telephonically; and

For suppliers, it is not always advisable to avail or share banking details via email correspondences. If there are no other secured channels such as physical delivery of such details in writing, rather share banking information directly over the telephone.

REMEMBER

Falling victim to these scams undermines the reputation of such entities and business confidence as perceptions could arise that may suggest control shortcomings. To help minimize this risk, consider enhancing controls around payment systems and in the unfortunate event of such scams occurring, report such timely to the to the FIC or the nearest police station.