Republic of Namibia

Financial Intelligence Centre

FINANCIAL INTELLIGENCE CENTRE (FIC)

P.O.BOX 2882, Windhoek

Tel: + 264 61 283 5100, Fax +264 61 283 5259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

NOTICE 01 of 2019

URGENT NOTICE TO ALL ACCOUNTABLE INSTITUTIONS, REPORTING INSTITUTIONS & THE PUBLIC

Security Alert: Be on the lookout for Phishing emails

01 February 2019

1. Introduction

This Notice is not issued in terms of any specific section of the Financial Intelligence Act, 2012 (Act No. 13 of 2012) as amended (FIA), but serves as a security alert to Accountable and Reporting Institutions (AIs and RIs), and the general public, to warn against phishing emails appearing to have been sent from email addresses belonging to Financial Intelligence Centre (FIC) employees.

2. Phishing emails appearing to emanate from FIC employees

All Accountable and Reporting Institutions (AIs and RIs), as well as the general public, is hereby warned that there are emails circulating which appears to have been sent by FIC employees stating things like ***"the usual payment of …(amount)….is made to your account. Please confirm payment was received. Thank you for doing business with me/us"***, or similar wording.

Kindly note that the FIC is not a commercial institution and does not do business or trade with any person or institution locally, regionally or internationally; and would not send out emails containing the above-mentioned or similar wording. These are considered phishing emails.

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in an email or other communication channels. The attacker uses phishing emails to, amongst others, distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.

Should you receive an email (either containing a link or an attachment or without any links or attachments) which appears to be from the FIC, kindly first confirm that the sender's email address is indeed correct. You may find that the sender's email address contain the name of an FIC employee, but not the rest of that employee's official email address, e.g. Frans@smtp06.serve.net.mx; while the content or signature to the email contains the correct email address of the FIC employee, e.g. Hilia.Frans@fic.na.

Example of a phishing email:

From: Frans@smtp06.serv.net.mx

Sent: 30 January 2019 09:00PM

To: robinhood@standardbank.com.na

Subject: COMET SIGNS PAYMENT

Attachments: REC 900273457256253.doc

A payment of U$ 6000.00 was made into your account to pay for invoice 51297454581527. Please confirm payment was received.

As always, thank you for your business.

Frans, Hilia
420 – 7970 -8020 O 420-797-8865 F
Email: Hilia.Frans@fic.na

When in doubt, please do not open the email, download any attachments, click on any links within the email or reply to the email. It is advisable to rather inform your IT department to investigate and confirm whether the email is not a phishing attempt and, at the same time, immediately alert the FIC.

Finally, please take note that the FIC primarily make use of the message board functionality on the goAML Web Portal to communicate with the regulated populace.

Should you have any questions in this regard, you may contact the FIC Helpdesk at email helpdesk@fic.na

---

Further information
Enquiries can be directed to the FIC Help Desk by:
Email to **helpdesk@fic.na**
Tel: + 264 – 61 283 5100
Fax: +264 – 61 283 5259