FINANCIAL INTELLIGENCE UNIT

FRAUD ALERT[1] – PHISHING SCAM
August 14, 2018

The Financial Intelligence Unit (the FIU) has been made aware of numerous "spear phishing scams" that are being perpetrated by cyber criminals and targeted towards the Belizean public. They are designed to compromise personal banking information, access accounts and credit cards and eventually siphon funds to criminal third parties.

Phishing is a form of fraud in which victims are contacted typically through electronic communication such as email or text message by someone posing as a reputable individual or entity, to lure them into providing sensitive data such as personal information, banking and credit card details and passwords, for malicious reasons. An attachment or links in the message may install malicious software (malware) on the user's device or direct them to a malicious website set up to deceive them into divulging sensitive data. To make phishing messages appear to originate genuinely from a well- known organization, they may include logos and other identifying information taken directly from the organization's website.

Persons in Belize have been receiving emails from several sources, suggesting that urgent action must be taken to prevent account loss and requiring the resubmission of personal information including account numbers, user IDs, access codes, PINs and passwords, etc. The purported sender might be your local bank, an employer or online media services such as Apple, Google, Amazon or Yahoo. In the hands of hackers, personal information may be used to carry out other criminal acts such as blackmail or fraudulent transfer of funds through online banking. There are increasing reports of breached online banking accounts and subsequent fraudulent online transfers.

On the other side, residents are being recruited via social media to harvest the proceeds of these crimes such as fraudulent online transfers and to repatriate the funds to criminal third parties, some of whom may reside overseas. The recruitment may be done in several modes, including offers to partake in surveys or to perform other jobs at home with a promise of substantial reward. Thereafter, the prospect will be asked to recover amounts deposited to their bank accounts and to pay themselves a commission and forward the bulk of the deposits to criminal third parties. It has been observed that recruits are directed to repatriate the stolen monies through remittance service providers.

[1] The Financial Intelligence Unit (FIU) issues this Alert in accordance with section 7(1)(d) of the FIU Act, requiring the FIU to take such measures as may be necessary to counteract financial crimes.

The FIU is working in concert with the Central Information Technology Office, elements of the Belize Police Department and the banking sector (and its supervisory authority the Central Bank) to address the resulting issues.

In the interim, we caution all persons that the offence of money laundering is committed if a person knowingly or having reasonable grounds to believe that any property represents any person's proceeds of crime and, nevertheless, such person acquires, possesses, converts, transfers, conceals or otherwise deals with such property. The FIU is in the process of investigating reports of such phishing schemes and the resulting fraud and will prosecute perpetrators and accomplices as appropriate.

The public is urged to exercise the following measures to reduce the risk of being a victim of phishing schemes:

- **Never reply to email messages that request your personal information.** Be very suspicious of any email message from an individual or organization that asks for your personal information, or one that sends you personal information and asks you to update or confirm. Financial institutions will never send a link in an email requesting a user to change login credentials including account name, password, PIN number, security questions, etc.
- **Do not click links in suspicious emails.** The link may not be trustworthy.
- **Further secure your personal information by upgrading security protocols including passwords.** Establish strong passwords which are alphanumerically designed.
- **Monitor your online accounts more frequently.**
- **Report suspicious emails.** Use your email's "report phishing" or "report spam" feature to report suspicious emails.

Finally, suspicious activity reports can be sent to the Financial Intelligence Unit by directing them to fiu.belize@fiubelize.org. In other circumstances, please call the FIU at 223-2729 and 223-0596 and ask to speak to one of our investigators.

Financial Intelligence Unit **4998 Coney Drive, Belize City** **(501) 223-2729**