FINANCIAL INTELLIGENCE UNIT
FRAUD ALERT
March 18, 2022

The Financial Intelligence Unit (the FIU) is aware of numerous "phishing scams" that are being perpetrated by cyber criminals and targeted towards the Belizean public. Phishing scams are designed to compromise personal banking information, access accounts and subsequently steal customers' funds.

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.

The FIU notes that persons have been receiving emails purporting to be from their local banks and stating that they are required to update their bank account information and/or migrate to new online banking security settings. Following the instructions received, victims would have divulged sensitive banking credentials. In the hands of phishers, personal information is used to carry out fraudulent transfer of funds via online banking. There are increasing reports of breached online banking accounts and subsequent fraudulent online transfers.

On the other hand, residents are being recruited via social media to harvest the proceeds of these crimes, and remit or transfer the value to criminal third parties, some of whom may reside overseas. The recruitment may be done with an online job offer to conduct evaluation of online gift card sales, which entails going online and purchasing online gift cards such as Google Play and iTunes with funds sent to their accounts. The person is instructed to keep a small payment from the sum received for each evaluation. It has also been observed that recruits are directed to transfer the bulk of stolen funds to third parties' accounts, or through remittance service providers.

The FIU advises the public that a person who knowing or having reasonable grounds to believe that property which represents the proceeds of crime, converts or transfers that property for the purpose of concealing or disguising its illicit origin or conceals or disguises the true nature, source, location, disposition or movement with respect to ownership of that property, or acquires, possesses, uses or otherwise deals with that property , or participates in, or aids and abets or facilitates any of the previously mentioned, commits the offence of money laundering, pursuant to section 3 (1) of the Money Laundering & Terrorism (Prevention) Act, Chapter 104 of the laws of Belize (Revised Edition 2020). The FIU is conducting investigations into these reports of phishing schemes and will pursue prosecutions of perpetrators and their accomplices. Account holders who permit their accounts to be misused to enable the transfer of illicit proceeds may be subject to the freezing of their accounts and subsequent prosecution to recover the proceeds of crime.

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 therefore urges the public to exercise the following measures to reduce the risk of being a victim of phishing schemes:

- Do not reply to email messages requesting your sensitive banking information. Be very suspicious of email messages from individuals or organizations asking for your personal information or sends your personal information to you requesting that you update or confirm it. Be reminded that, financial institutions do not send links to customers' emails requesting users to change login credentials such as, account name, password, PIN number, security questions, etc.

- Do not click on links in suspicious emails. The link may not be trustworthy.

- Secure your personal information by upgrading security protocols including passwords and create strong passwords, which contain alphanumeric and special characters.

- Monitor your online accounts frequently.

- Report suspicious emails by using your email's "report phishing" or "report spam" features.

Finally, suspicious activity reports can be reported to the FIU at telephone number 223-2729.