FijiFIU

Fiji Financial Intelligence Unit

FIU ALERT & INSTRUCTION NOTICE #: 14/2018

[Sections 25.1(h) & (o): Financial Transactions Reporting Act]

6 December 2018

TO: FINANCIAL INSTITUTIONS & MEMBERS OF THE PUBLIC

RISE IN EMAIL COMPROMISE & EMAIL SPOOFING CASES IN FIJI

The Fiji FIU would like to advise commercial banks, financial institutions, businesses and members of the public to exercise caution when handling email payment instructions for import trade transactions and large value personal outbound foreign remittance transactions.

The Fiji FIU has noticed a continuous rise in cases of individuals and businesses falling victim to email compromise and *spoofing* scams.

Since 2014, 39 businesses and individuals have lost funds totaling $5million in foreign remittance transactions to cybercriminals through email compromise scams. Only $169,000 was recovered.

Email compromise involves the cyber attacker often utilising social media platform and online social engineering techniques to trick internet users to unknowingly install malware such as *keylogger*, computer virus, worm, *Trojan Horse* and Spyware onto their computers, workstations or wireless devices. This is an effort to compromise and steal personal sensitive information such as email and other online account login credentials.

Once the cyber attacker gets access to the account, they can then monitor emails, intercepting those that contain an invoice or a payment instruction to the commercial bank. Therefore, the cyber attacker then changes the payment instructions on a chosen invoice or intended transaction and allows it to be processed usually with the funds going straight into a bank account of a cybercriminal syndicate instead of the intended and rightful beneficiary.

Email *spoofing* is the creation of email messages with a fake or look-alike email sender address to mislead the recipient about the origin of the message. Cases reported to the Fiji FIU show that look-alike email addresses were used between local business entities and their overseas suppliers regarding orders for import of goods. Cases also involve non-trade related personal foreign remittance transactions.

Recent case examples reported to the Fiji FIU in 2018 on email compromise and email *spoofing* cases include:

In March 2018, an email account of a local bank customer was compromised and a fraudulent payment instruction was sent to the local bank. Approximately FJ$575,000 was transferred to a foreign bank account belonging to a cybercriminal syndicate.

In September 2018, in a case involving cyber money laundering, FJ$556,000 was fraudulently transferred from a local business bank account to an offshore "incorrect" bank account number. In this case the foreign supplier's business email was compromised.

In October 2018, proceeds of approximately FJ$27,000 from sale of investment shares of a local investor who is residing abroad, was remitted to a cybercriminal's bank account in another country as a result of email compromise of the investor.

In October 2018, an estate property settlement proceeds totaling approximately FJ$845,000 was remitted to the foreign bank account of a cybercriminal who pretended to be the beneficiary of the estate. It appears that email accounts of the beneficiary and local party were compromised.

You may also refer to Fiji FIU's Press Release No. 9/2014 that was issued on 17 April 2014 and FIU Alert Notice #: 6/2014 that was issued to commercial banks on 11 August 2014 on "Email Spoofing".

Any suspicious overseas trade transaction or large personal remittance that could be linked to email compromise and spoofing scams should be immediately reported as a suspicious transaction report to the Fiji FIU.

Commercial banks and remittance service providers are required to conduct enhanced due diligence for suspicious payment instructions.

Business customers engaged in overseas trade should also be made aware of alternative and safer modes of instructing commercial banks for international trade payments.

This alert notice is intended for wider circulation to members of the public and business community as well as to industry associations, clients and customers of financial institutions.

Should you need any further clarification or information, please contact Mr. Avaneesh Raman on telephone 322 3279 or email avaneesh@rbf.gov.fj.

Razim Buksh
Director