Financial Intelligence Unit

Government of the Cook Islands

PO Box Avarua Rarotonga

Email: fiuhead@cifiu.gov.ck Mobile: (+682) 55 354

Public Notice - Increase in COVID-19 Scams

With the ongoing global pandemic COVID-19, cybercriminals are trying to capitalise on the crisis and we wish to warn the Cook Islands public that there will be an increase in COVID-19 online scams.

It is important that all individuals and businesses be extra vigilant and take additional protective measures against online scams. Many of these scams can be very sophisticated and look as though they came from legitimate sources or even individuals you may be related to or know.

The types of scams that have been seen in other parts of the world include:

Phishing emails

These may be emails with links or attachments included. Examples include:

- Links to COVID-19 statistics or information.
- Fake Health ministry alerts. For example, cybercriminals have sent phishing emails designed to look like they're alerts from the US Centers for Disease Control and Prevention.
- Fake health advice. For example, cybercriminals have sent emails that offer purported medical advice and some claim to be from medical experts near Wuhan, China.
- Workplace policy emails. These are phishing emails pretending to be from your work place with attachments or links relating to “new” disease management policies being put in place. If the attachments are clicked then malicious software is downloaded.
- Emails from scammers purporting to be a relative or friend needing urgent financial help as they may be stuck with travel restrictions, need money for supplies or medical bills.

Scams or fake ads

Be wary of ads or products that claim to offer treatment, protective equipment or cures for the coronavirus. The ads often try to create a sense of urgency — for instance, “Buy now, limited supply.” Clicking on such ads may result in downloading malware onto your device. In addition, you might buy the product and receive something useless, or nothing at all. Meanwhile, you may have shared personal information such as your name, address, and credit card number.

How to protect yourself

- Ensure your IT security systems are up to date.
- Be vigilant against what to look for to better identify phishing emails. Please check our FIU Scams webpage for further information.
- Only obtain information from legitimate sources eg. COVID19.gov.ck, Ministry of Health website.
- Businesses should proactively put in place payment verification steps within their account teams or personnel.
- If you receive requests from family, friends etc – check the request by calling them or someone close to them.

We are asking the public to report all scams (whether acted upon or not) to the FIU on fiuhead@cifiu.gov.ck or phone (682) 55 354.