Don’t be a Victim of Scams

By **Natasha Eddie Hivae**

Let’s talk about Scams. Recently we have learned that there is a scam conducted online to lure people into believing that they won a huge amount of money from the Central Bank of Solomon Islands.

Just last month, the Reserve Bank of Fiji also issued a statement to warn the general public on similar scam activities.

This scam activities in other words is called a “make money fast scams” or an “economic scam.” For this type of scam, cyber criminals will lure you into believing you can make fast and easy money on the internet.

This scamming method is quite simple and uses an effective approach. For instance, the scammers would normally address a basic need for money, especially when someone is in a difficult financial situation.

Using all sorts of techniques, the victim is lured into giving away personal information such as bank account numbers, passwords, and debit or credit card numbers with the promise of a monetary reward.

These fraudulent activities are often perpetrated in the name of legitimate business such as a bank (e.g. CBSI), telecommunication or internet service provider.

There is an increase of scam activities conducted in the Pacific Islands in the last couple of years.

According to the Solomon Islands Financial Intelligence Unit (SIFIU) there are many people in Solomon Islands that also fallen victim to a lot of scams in recent years.

Their reports have shown that the monetary loss incurred through fraudulent activities are in thousands or even millions of Solomon dollars.”

Furthermore, the number of monetary loss through scams could be higher as there are large number of victims out there that are not reporting the fraudulent activities due to fear of being identified or embarrassed.”

In 2007 several people in the Cook Islands have fallen victim to the internet and postal scams. One case that was known to the Financial Intelligence Unit is a person sending over NZ30,000 {US22,500} overseas from the Cook Islands.

According to their FIU, one of the victims was contacted by email saying that they have won or been nominated as the beneficiary of some millions of dollars and in return, they are simply required to pay some type of fee.

There are different types of scams conducted nowadays. With the increase of technology and internet rates made cheaper, criminals are using online platforms to conduct their activities and scamming is one.

Solomon Islands recently had our fair share of experiencing pyramid scams. The famous “One Link Pacifica” pyramid scheme was reportedly operating for months before the downfall of its operations leaving many people victims.

In 2017 the PNG Post Courier reported, more than 50,000 Papua New Guineans paid large some of monies as 'fees" to await a windfall of 'millions of kina' from Israel and the United Arab Emirates which was denied by the United Arab Emirates government.

These are classic examples of scam activities conducted in our neighboring countries and within Solomon Islands.

The SIFIU continues to carry out awareness programs in schools, communities, through radio programs and media releases to educate and warn Solomon Islanders about the risks associated with scams or other questionable schemes that are in operation out there.

So, what can we do to protect ourselves from Scams?

Some advice from SIFIU for the general public to take note of is to;

Protect yourself;

- If you have provided your account details to a scammer or someone unknown that is operating a questionable scheme, please contact your bank or financial institution **IMMEDIATELY**.
- **DO NOT** click on any links, make a reply or open attachments from emails claiming to be from your bank or another trusted organization and asking you to update or verify your details – **JUST PRESS DELETE.**
- Look for the **SECURE SYMBOL**. Secure websites can be identified by the use of "https:" rather than "http:" at the start of the internet address, or a closed padlock or unbroken key icon at the bottom right corner of your browser window. Legitimate websites that ask you to enter confidential information are generally encrypted to protect your details.
- Do an **INTERNET SEARCH** using the names or exact wording of the email or message to check for any references to a scam – many scams can be identified this way.
- **NEVER** provide your personal bank account details, debit/credit card numbers or online account details if you receive a call claiming to be from your bank or any other organization. Instead, ask for their name and contact number and make an independent check with the organization in question before calling back.

Finally think twice about what you say & do in an online environment. You could be the next target for scammers. By doing this, you are one step ahead of them.