Beware of Scams

Bank South Pacific (BSP) is warning the general public to beware of scams via emails, phone calls and letters.

Phishing (hoax emails) has increased in recent times due to the availability and access to modern means of communication such as the internet and emails.

While these means of communication make life easier for the user by a simple click of the button, they also provide opportunities for criminals and con artists who attempt to acquire sensitive information such as usernames, passwords, PIN numbers and credit card details by pretending to be a trustworthy entity.

Perpetrators send out legitimate-looking emails in an attempt to gather personal and financial information from recipients. This is normally carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website that look and feel almost identical to the real website. Typically, the messages appear to come from well-known and trustworthy email addresses.

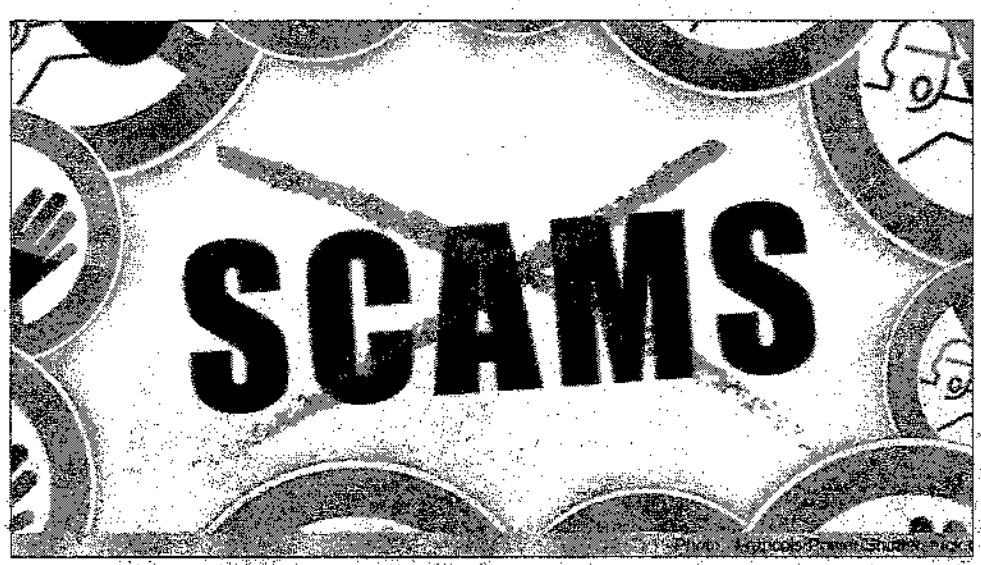

Image: BBB

Already many unsuspecting and gullible people world-wide, including Vanuatu, have fallen victim to hoax emails by responding and acknowledging such.

Organisations around the world, both financial and non-financial alike, have reported hoax emails that misrepresent their organisation have been sent to customers and many have fallen victim to clicking on the link or file attachment then unwittingly disclosing confidential details.

Spot the hoax and "do not bite"

As a general rule of thumb, always read carefully emails, before engaging. If you suspect that the email sent is suspicious and may be a hoax or is a hoax, always contact the company being impersonated directly and immediately.

If you get an email claiming to be from a reputable business but asking for private information, do not reply, nor submit personal information or click on any links contained in the email.

Hoax emails usually ask you to update, validate, or confirm personal information, often with a false sense of urgency such as: "We are updating our accounts and need information fast." "An unauthorised transaction has recently occurred on your account." "You may lose your account if you don't update your information. "Or "Please click here to verify your information."

What is BSP doing to protect customers?

Customers are reminded that BSP will never send an email request to its customers to verify, update or give their information or personal details. This is to educate our customers that at BSP we will never, never communicate with them via email to update or disclose their personal information or details pertaining to their Internet Banking passwords or account details.

At BSP like any other financial institution, we ensure that client and customer information is treated and shared via proper processes and protocols. The bank has a stringent policy of nondisclosure regarding matters of information security and deals with customers accordingly.

BSP was made aware of the threat of hoax emails by staff who received them and advised senior management who have since then put in place various means of protecting customers.

Customers are advised that this issue is an ever present threat for all people who send and receive internet email. You would have seen customer notices providing advice and guidance on the hoax email threat.

Many of our customers have been vigilant and cooperative in sending suspected hoax emails to the BSP hoax email address, where each email sent replied, the hoax email examined and a response to eliminate the threat to customers is developed and implemented.

As stated, the best advice is to ignore any type of unsolicited email requesting your action to click on a link or attachment.

Protecting personal and sensitive information such as bank account details, bank card PIN numbers and credit card numbers is important as disclosing it to someone else will result in you losing your money in your bank account or other important information.

Please contact BSP on 678 22084 or email: *hoax@bsp.com.pg* for verification with any questions relating to hoax emails or if you are unsure of what to do.