Consumer Council of Fiji
www.consumersfiji.org
CONSUMER COUNCIL OF FIJI

HEAD OFFICE
4 Carnavon Street
Private Mail Bag
GPO, Suva
Phone - General Office: 3300792, 3310183
Chief Executive Officer: 3305864
Fax: 3300115 | Email: complaints@consumersfiji.org

LAUTOKA/West
Suite 4 Popular Building
Vidilo Street
PO Box 5396, Lautoka
Phone: 6664987 | Fax: 6652846
Email: consumerltk@connect.com.fj

LABASA/North
Level 1, Lot 41 Raza Properties Ltd
Nasekula Road
PO Box 64, Labasa
Phone: 8812559 | Fax: 8812559
Email: colbs@connect.com.fj

18 April 2015 **FEATURE**

Avoid Phishing Scams

"Congratulations! You've won! We just need your Social Security number to process your prize! Plus, you need to send us a processing fee! Don't worry! You'll love your prize!"

It may be a dream come true when you receive such emails or text messages. But wait a minute – doesn't it sound 'too good to be true"? Don't you think, you need to be suspicious, especially, if it is asking for a processing fee?

Well, unfortunately, a lot of people fall for this type of messages everywhere in the world including Fiji.

Phishing e-mails trick people into sending money or providing personal information such as usernames, passwords, credit card details, and other personal details to unauthorized individuals who hijack their information and use it to commit identity theft.

Some consumers end up losing their hard earned cash at the hands of the scam artists who lure them with phishing messages such as "You have won the lottery".

The scammers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately. They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.

Still the most common form of phishing, emails from phishers impersonating bank employees or other legitimate parties asking the recipient to click on a link to enter sensitive data remain a threat. Typically, links will appear to be valid, but will actually direct the user to a forged website. Phishers count on users mistaking the fake site for the real one, and entering login information, credit card numbers, bank account information and other valuable data.

Often, these emails will include a logo for the impersonated company or agency and may even contain some legitimate links to seem more convincing. In the past, many of these emails featured blatant "tells", such as a generic salutation – "Dear customer," or something similar – and even contained grammatical or spelling errors in the body of the text.

To make these phishing email messages look even more legitimate, the scam artists use graphics that appear to go to the legitimate websites but actually take you to a phony scam site or possibly a pop-up window that looks exactly like the official site.

Here are a few phrases that are commonly used in phishing email scams:

"Verify your account"

Businesses should not ask you to send passwords, logon information or user names, Social Security numbers, or other personal information through email. If you receive an email message from Microsoft or any other business asking you to update your credit card information, do not respond: This is a phishing scam.

"You have won the lottery."

The lottery scam is a common phishing scam known as advanced fee fraud. The lottery scam often includes references to big companies, such as Microsoft. There is no Microsoft Lottery!

You can avoid getting hooked by a phisherman by not:

- responding to e-mails, mail, telephone solicitations, raffles or contests from unknown entities
- e-mailing personal or financial information including credit card or bank account numbers, passwords, Social Security numbers, etc. Most Internet e-mail is NOT secure
- replying to e-mails or pop-up messages requesting personal or financial information
- clicking on links in unsolicited messages which can connect to suspicious websites
- updating personal information online in response to e-mailed requests
- cutting and pasting a link from an unsolicited message into a Web browser, as these links can be made to look like they go to one site, but are actually redirected to another to mine information
- responding to calls from alleged companies which use a recorded message and ask you to call a phone number to update account information.

Consumers must be cautious and avoid disclosing their personal details, bank account numbers, PIN numbers and passwords to anyone they don't trust.

Remember: Consumers must be suspicious of any email with urgent requests for personal financial information.