



Fiji FIU

Fiji Financial Intelligence Unit



---

## ***PRESS RELEASE***

---

<b>Press Release No</b>	<b>: 33/2011</b>	<b>Phone</b>	<b>: (679) 331 3611</b>
		<b>Fax</b>	<b>: (679) 330 2094</b>
<b>Date</b>	<b>: 22 November 2011</b>	<b>E-mail</b>	<b>: <a href="mailto:info@rbf.gov.fj">info@rbf.gov.fj</a> or <a href="mailto:info@fijifiu.gov.fj">info@fijifiu.gov.fj</a></b>

---

### **BEWARE OF INTERNET HACKING AND EMAIL SCAMS**

The Fiji Financial Intelligence Unit (FIU) would like to warn and advise members of the public to exercise extreme caution when using their email accounts due to a number of scam email cases being brought to the attention of the FIU.

The Director of the FIU, Mr. Razim Buksh said that recent cases involve hackers gaining access to email accounts and sending out mass emails to the victim's contacts from the contact list. The email message is sent without the knowledge of the email account holder. These emails claim that the victim is robbed or stranded overseas for various make-believe reasons. The hackers make an appeal in the email message and the recipients, (who are either the victim's friends, relatives, or work officials), are requested to send a sum of money in the name of the victim. The hackers usually request that the money is urgently sent abroad to pay for hotel bills and air tickets to return home.

Mr. Buksh advises the general public to be wary of any email requesting you to send money abroad, even if the email appears to come from a trusted or known contact. Internet users and email account holders are also advised to thoroughly verify any requests for remittance of funds for whatever reason and not disclose their login and password information and bank account details to others. Such email should be ignored and deleted immediately.

Mr. Buksh advises the general public to refer to the following guidelines if in doubt: -

#### **How to determine if your email account has been hacked**

Your email account may be compromised if: -

1. You are no longer able to log into your email account because your password has changed; or
2. Your sent folder contains messages that you have never sent; or
3. Your email contacts inform you that they have been receiving spam messages from your account.

## **What to do if you suspect that your email account has been hacked**

- 1. Immediately change your password or request the administrator of your email system to change your password if you are unable to log into your account.**

Many E-Mail services and providers, such as *hotmail* and *G-Mail*, will have links that may be used to request a password change. Choose a strong password. A 'strong' password will be at least 6 characters long and contain a combination of uppercase and lowercase letters, numbers and special characters such as %, \$ and +.

- 2. Change the password for ALL your other online accounts.**

Please note that many users often use the same password for multiple accounts such as email, social networks and even internet banking. This practice is strongly discouraged. Furthermore it is recommended to err on the side of caution and to assume that ALL your accounts have been compromised.

- 3. Change your 'security question' and 'answer' for your accounts.**

Some email services require the setup of a Security Question that can be used to verify your identity. It is common practice for hackers to change this in order to regain access to your account if they are locked out.

- 4. Verify that you are the owner of your alternate email address.**

The alternate email address is where new passwords are sent in the event of a password reset request. It is common practice for hackers to change this in order to regain access to your account if they are locked out.

## **How can you prevent hackers from gaining access to your email account?**

1. Choose a 'Strong' password.
2. Install a reputable anti-virus software.
3. Change your password at regular intervals.
4. Avoid giving your email address to every site that asks for it.

Mr. Buksh also advises the general public to ignore unsolicited email that offer large investment proposals, winning of lottery awards, job offers, and other "get rich quick" schemes.

Mr. Buksh said that the FIU will continue to monitor all financial transactions to ensure that Fiji's financial system is safe and remains protected from cybercrime activities.

**Financial Intelligence Unit**