BANK OF MAURITIUS

Website: https://www.bom.mu

Communiqué
Fraudulent International Conference Scam Alert

Members of the public are hereby requested to exercise caution when replying to any unsolicited email inviting them to attend international conferences. These emails could be scams designed to trick individuals into giving out their personal details and banking information.

It is, therefore, important for members of the public to be aware of fraudulent internet correspondence, also known as 'phishing' – a type of fraud in which e-mail messages, instant messages and websites are used to deceive individuals into providing confidential, personal information, which can be used for credit card fraud and other serious violations of privacy. Phishing e-mails generally appear to be sent from legitimate organizations, asking users to either reply or link to a web page to update their personal information. They sometimes contain an organizational logo and even a physical address, but the web address, or URL, does not match that of the legitimate organization.

Members of the public are therefore cautioned against such emails and are advised not to give out any personal and banking information such as details of their bank accounts, card numbers, personal identification numbers etc., to unknown persons as they run the risk of being scammed or become a party to illicit transactions.

Members of the public are advised to take the following precautions to ward off any risk of being scammed :

- Be watchful to any unexpected e-mail, instant message, voicemail or fax.
- Check the veracity of information received by other means, for example, telephone or other relevant website or email addresses.
- Do **not** be fooled by an email that looks legitimate or appears to link to a genuine website. The legitimacy of the email must be checked before replying to it.
-- Do **not** give out personal, credit card or account details upon receipt of email requesting for personal and banking information.
- Do **not** reply to emails received from unknown sources.
- Do **not** respond to any e-mail, phone or fax instructions that prompt you to divulge your personal information.
- Do **not** click on any links in a suspicious e-mail; clicking on such a link may cause the download of key-logging or 'spyware' programmes onto your computer.
- Regularly log on to your online banking, credit card or other accounts and reconcile your statement balances to ensure that all transactions are legitimate.
- Use up-to-date anti-virus software – including spam filters and even 'anti-phishing' programmes, which are available to help screen out potential phishers on websites and e-mails.

A list of the different types of financial frauds is available on the Bank's website, https://www.bom.mu, under the menu "Financial education". Please do not hesitate to call us on our toll-free number **149** or send us an email on micell@bom.mu to report any potential scam or financial fraud.

15 December 2014