FSCALT25B2015/5

Financial Services Commission
Mauritius

ALERT

Phishing Attempt by Mrs Thérèse Konaté and Mr Michael O'Hara

The Financial Services Commission, Mauritius (the "FSC Mauritius") would like to alert members of the public of a phishing email from Mrs. Thérèse Konaté, ("Mrs Konaté") and Mr Michael O'Hara ("Mr O'Hara").

Phishing refers to emails, text messages, letters and phone calls that seem to emanate from legitimate businesses that trick people into disclosing their personal and banking information. These scammers are generally looking for information like your bank account numbers, passwords and/or credit card numbers, which they will use for their own benefit.

In this email, Mrs Konaté notifies the winning of an amount of 250 000 € through the Loterie Internationale Microsoft Corporation, an internet promotion programme.

The beneficiary is invited by Mr O'Hara, allegedly the director of operations of the Loterie Internationale Microsoft Corporation to contact Maitre Bernad Dardier and to provide the latter with his personal details within 45 hours. All the information provided will be kept confidential.

Mr O'Hara further acquaints that all winning amounts should be claimed within 10 days or otherwise the money will be credited to some health and medical organisations. All information regarding the winning amount should be kept confidential so as to prevent double recovery.

Furthermore, Mr O'Hara is soliciting lottery winners to invest part of the winning sum in the internet promotion programme.

The FSC Mauritius urges members of the public to exercise appropriate caution in respect of such emails and to avoid providing details of their bank accounts, credit card numbers, etc. in their own interest.

The following could be used as a guideline to "protect yourself" from phishing scams:

- ☐ Never send money or give credit card or online account details to anyone you do not know and trust.
- ☐ Do not open suspicious or unsolicited emails (spam)—ignore them.
- ☐ Do not click on any links in a spam email or open any files attached to them.
- ☐ Never dial a telephone number that you see in a spam email or SMS.
- ☐ If you want to access an internet account website, use a bookmarked link or type the address in yourself—NEVER follow a link in an email.
- ☐ Check the website address carefully. Scammers often set up fake websites with very similar addresses.
- ☐ Never enter your personal, credit card or online account information on a website if you are not certain it is genuine.
- ☐ Never send your personal, credit card or online account details through an email.

You may also wish to refer to:

- The FSC Mauritius Alert on a similar phishing attempt - Alert – Phishing Attempt by Mrs Helen J issued on 18 March 2014; and

- You may also wish to refer to the Social Media and Fraud Alert and Alert on Phishing issued by the FSC Mauritius on 11 July 2013 and 18 March 2014 respectively.

Financial Services Commission, Mauritius
25 February 2015

FSC House, 54 Cybercity, Ebene, Republic of Mauritius, 72201
Tel: (230) 403 7000 Fax: (230) 467 7172
E-mail: fscmauritius@intnet.mu, Website: www.fscmauritius.org