FSCALT25B2015/3

Financial Services Commission
Mauritius

ALERT

Phishing Attempt by Dr. Lesetja Kganyago

The Financial Services Commission, Mauritius (the "FSC Mauritius") would like to alert members of the public of a phishing email from Dr. Lesetja Kganyago, ("Dr. Kganyago").

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, Dr. Kganyago acquaints that the recipient is listed as a beneficiary in the recent schedule for payment of outstanding debts incurred by the United Kingdom Lottery Promotion Council ("UK Lottery Council") pending since 2011 to 2015.

On 05 January 2015, Dr. Kganyago and Ban Ki-moon together with Dr. Edward Terry of UK Lottery Council, met with the Senate Tax Committee and it was decided by Dr. Kganyago to release all unclaimed funds back to the UK Lottery Council, for subsequent payment directly to the beneficiary.

The UK Lottery Council has instructed their fiduciary bank to credit the beneficiary`s winning amount directly in the latter`s ATM card to curb the Government tax.

The beneficiary is invited to contact Mrs. Liza Yolandi allegedly the person in charge of the foreign exchange department and to provide the latter with his personal details. Furthermore, the inheritor has to pay an amount of 4,500 for the fund transfer approval letter from the British High Commission. All information regarding the winning amount should be kept confidential and any double claim will lead to disqualification.

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 – Alert - Phishing Attempt by Mr Kassym – Jomart Tokayev and Alert - Phishing Attempt by Mr. Andrew Lincolm 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