



Financial Services Commission
Mauritius

Alert - Phishing Attempt by Mr Kassym – Jomart Tokayev

The Financial Services Commission, Mauritius (the “FSC Mauritius”) would like to alert members of the public of a phishing email from purportedly Mr Kassym – Jomart Tokayev (Mr Kassym”), the ex-Director General of the United Nations Organisation (“UNOG”).

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, the UNOG claims to have been authorized by the newly appointed United Nation Secretary General, and the governing body of the UNITED NATIONS Monetary Unit, to investigate the unnecessary delay on the payment of the beneficiary’s Inheritance funds since corrupt officials of the Bank are trying to divert the funds into their private accounts. The beneficiary is informed that his inheritance funds, amounting to USD\$1, 20,000,000 have been credited in his favour through ATM VISA CARD.

The beneficiary is urgently requested to contact Mr Brian Robertson, allegedly the Director of the ATM Payment Department of the HSBC Bank Plc UK and to provide the latter with his personal details for the delivery of the ATM Card.

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 Mr. Andrew Lincolm](#) issued on 18 March 2014;
- The FSC Mauritius [Social Media and Fraud Alert](#) issued by the FSC Mauritius on 11 July 2013.

Financial Services Commission, Mauritius

FSC House

54 Cybercity

Ebene

Republic of Mauritius

Tel: +230 403-7000

Fax: +230 467-7172

Email: fscmauritius@intnet.mu

18 March 2014