Financial Services Commission
Mauritius

Alert on Phishing

In line with its objectives and functions, the Financial Services Commission, Mauritius (FSC Mauritius) is issuing this alert to enable members of the public to identify phishing messages.

What is phishing?

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.

How to recognise phishing attempts?

- They seem to come from a bank, a financial institution or a reputable organisation.
- They might include logos which appear to be official and other identifying information taken directly from legitimate websites.
- They might include convincing details about your personal history that scammers found on your social networking pages.
- They might appear to be from a prominent personality or someone occupying a position of high authority.
- They might ask the recipient to make a phone call or to reply to an email, message, and text in order to communicate personal information.
- They might include links to spoofed websites where you are asked to provide personal information.

Commonly used phrases in phishing attempts

- Verify your account

  If you receive an email message from any business asking you to send passwords, logon information or user names, Social Security numbers, or other personal information through email or to update your credit card information, do not respond. This is a phishing scam.

- You have won the lottery

  The lottery scam is a common phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often includes references to renowned companies or oganisations.

- If you don't respond within 48 hours, your account will be closed

  These messages convey a sense of urgency which may urge you to respond immediately. This is a type of phishing message.

- Masked web address/ illegitimate

  Phishing links may contain all or part of a real company's name and are usually masked. The links do not take you to the real address but usually to an illegitimate website.

  Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered by adding, omitting, or transposing letters. This is called "typo-squatting" or "cybersquatting."

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 e-mail 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.

The FSC Mauritius urges members of the public to exercise appropriate caution in respect of such phishing scam.

You may also wish to refer to the 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
E-mail: fscmauritius@intnet.mu

18 March 2014