Monetary Authority of Singapore
10 Shenton Way MAS Building Singapore 079117
Telephone: (65) 6225-5577

Annex B

What is phishing?

Phishing is a way of obtaining sensitive personal information such as one's banking account details, PIN, one-time passwords (OTP), credit card number, user ID or password through the Internet, in order to perform unauthorised banking transactions.

The most common phishing method is a spoofed email purporting to be from a financial institution, credit card issuer, service provider or a government agency.

The phishing emails typically contain URL links, which when clicked, direct the consumer to fake webpages (e.g. a login page) which mimic the websites of legitimate financial institutions. These fake webpages are often used by perpetrators to harvest the sensitive personal information belonging to consumers. The webpages may also contain malware aimed at infecting consumers' computing devices. Phishing emails may also contain malicious attachments that could compromise recipients' computing devices or systems.

Identifying tell-tale signs of phishing emails and guarding against phishing attempts

Below are some quick tips that can help members of the public identify potential phishing attacks.

- Misspellings
- Threats of dire consequences for not responding
- Unsolicited requests for sensitive information
- Promises of attractive rewards for replying or clicking on the URL
- Different URL displayed when you hover your mouse over links in the email
- Requests to open file attachments (e.g. .exe, .zip file types)

If you come across any of these tell-tale signs, do not reveal any confidential or personal information to the sender. Do not click on any links to external websites or open attachments in the emails purportedly sent to you by financial institutions or government agencies. If you are unsure of the authenticity of the email, contact the organisation that the email was purportedly sent from.