SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

21 May 2025

Circular to licensed corporations

Phishing detection and prevention

In view of recent reports on phishing attacks that caused financial losses for clients, the Securities and Futures Commission (**SFC**) issues this circular to remind SFC-licensed corporations (**LCs**) of the expected standards relevant to phishing detection and prevention, as well as the requirement to notify the SFC under the Code of Conduct[1].

Several LCs have reported to the SFC that their clients received phishing short message service (SMS) messages with embedded hyperlinks purportedly sent by the LCs. After clicking the embedded hyperlinks, the clients were lured into entering their account login details[2]. Unauthorised transactions were subsequently conducted over the accounts of the clients, potentially involving market manipulation, and led to financial losses for the clients.

Expected standards

In February 2025, the SFC highlighted key observations from its cybersecurity review and set out expected standards in the Circular to licensed corporations - Cybersecurity review of licensed corporations[3]. Once again, LCs are reminded:

1. not to send electronic messages (such as emails or SMS messages) with embedded hyperlinks that direct clients to their websites or mobile applications to undertake transactions;

2. not to ask clients to provide via hyperlinks sensitive personal information, including login credentials and one-time passwords;

3. to send clients regular cybersecurity alerts and reminders, including security reminders against phishing attacks; and

4. to implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts.

LCs should (a) inform clients that LCs will not ask clients to provide via hyperlinks sensitive personal information, including login credentials and one-time passwords, and (b) remind clients not to disclose their account login information to any unverified websites, even if they look genuine.

[1] Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission
[2] These included login names, biometric IDs, passwords and/or SMS one-time passwords.
[3] https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC7

Where an LC has received any client enquiries about phishing SMS messages or emails with an embedded hyperlink to a website or application resembling that of the LC, or has been notified that the client has been defrauded by such phishing, the LC should remind the affected clients to report the incidents to the Police where applicable and alert other clients of the incident as soon as practicable.

In addition, according to paragraph 2.1 of Schedule 7 of the Code of Conduct, LCs which offer internet trading should put in place proper risk management and supervisory controls, including: 1) automated pre-trade controls that are reasonably designed to prevent the entry of orders not in compliance with regulatory requirements, and 2) post-trade monitoring to reasonably identify any order instructions and transactions which may be manipulative or abusive in nature.

Notifications to the SFC

Under paragraph 12.5(e) of the Code of Conduct, LCs are required to report to the SFC immediately upon any material failure, error or defect in the operation or functioning of its trading, accounting, clearing or settlement systems or equipment. Furthermore, under paragraph 12.5(f) of the Code of Conduct, LCs are also required to report to the SFC immediately upon any material breach, infringement or non-compliance of market misconduct provisions set out in Part XIII or Part XIV of the Securities and Futures Ordinance that it reasonably suspects may have been committed by its clients, giving particulars of the suspected breach, infringement or non-compliance and relevant information and documents.

Intermediaries Division
Securities and Futures Commission

End

SFO/IS/015/2025