30 Sep 2004

Precautionary measures against fake e-mails or websites (superseded by TM-E-1 of Supervisory Policy Manual)

Our Ref: B1/15C
B9/29C

30 September 2004

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Precautionary measures against fake e-mails or websites

The HKMA has issued a number of circulars and a guidance note since 2003 covering some suggested precautionary measures for handling fake bank websites and e-mails. In view of the increasing number of reported fraudulent bank websites and e-mails recently, I am writing to reiterate the importance of putting these precautionary measures in place to guard against such fraud.

One frequently used tactics by fraudsters is to send e-mails to members of the public purporting to be sent by an Authorized Institution (AI). These e-mails normally request bank customers to make connection to a fake bank website via an embedded hyperlink and to trick bank customers into revealing sensitive account and personal information such as Internet banking login names and passwords. In this connection, we believe that it would be helpful to mitigate customers' risk if the following safeguards are introduced:

a. do not send e-mails to your customers with embedded hyperlinks to the transactional websites;
b. inform your customers directly (e.g. through issuing personal e-mail alerts, displaying alert messages prominently on your institution's transactional website, or including similar statements in the monthly bank statements) that your institution or its agents/business partners will not:
    i. send e-mails with embedded hyperlinks to transactional websites to its customers; or
    ii. ask for sensitive account and personal information such as user IDs and passwords via e-mails.
    iii. Customers should be reminded that they should contact your institution immediately if in doubt; and

c. put a high priority for implementing two-factor authentication to further strengthen the security controls for retail Internet banking services. Meanwhile, AIs are expected to continue to review and enhance their security measures before the two-factor authentication is in place, including enhancing fraud monitoring and reporting mechanism, and lowering the maximum limit for unregistered third-party fund transfers through Internet banking where appropriate.

The HKMA will continue to monitor the trends of internet banking fraud, and work closely with the banking industry to consider other possible preventive and detective measures.

If you have any questions on this letter, please feel free to contact Mr Shu-Pui Li at 2878-1826 or Mr James Tam at 2878-8043.

Yours faithfully,

Y. K. Choi
Executive Director
Banking Supervision

Last revision date : 01 August 2011