Trojan Horse Attack on Internet Banking Services

You may have the experience of receiving fishy emails purported to be from your friends asking you to open a file or to provide personal data, but your friends later confirmed that the emails were not sent by them. In such cases, most likely your friends' computer had been infected with a Trojan Horse, and if you did follow the instructions in the emails, you might have become a victim too.

Recently a number of suspected Trojan Horse fraud cases, chiefly relating to business or corporate internet banking services, were detected in Hong Kong. It is believed that computer users, when logging on their internet banking account, were lured into inputting their logon credentials (e.g. logon ID, password, and one-time password (OTP) generated from the security device) to a fake web page. The information so "stolen" was then used by fraudster to initiate fraudulent fund transfer transactions despite two-factor authentication was required, as OTP was already disclosed to the fraudster.

The use of Trojan Horse for internet fraud has been around for some years. Where computer users fail to protect their computers from malwares such as Trojan Horse, fraudsters will still be able to do the trick, regardless of the level of internet security provided by banks. Here the HKMA would like to remind bank customers that it is very important to vigilantly protect their computers to safeguard against internet banking fraud.

In view of the recently detected fraud cases, I will try to address certain issues related to Trojan Horse in the form of questions and answers.

Q1. How could Trojan Horse be used to pose risks to internet users?

A1. Through the use of Trojan Horse planted in an internet user's computer, a fraudster can capture screen displays and keystrokes, steal information stored in or even take control of the user's personal computer.

Q2. What precautionary measures could be taken to avoid becoming a victim of Trojan Horse attack?

A2. Internet users should stay vigilant when using their computers in order to minimise the chance of being infected with Trojan Horse or any other malwares, or at least to detect them if the computers are already infected. If customers find the website of the bank suspicious or encounter unusual logon screen, they should **NOT** enter any information (including user ID, password and OTP) to the website and should report to the bank immediately.

Q3. How could an internet user detect whether a Trojan Horse has been installed in his/her personal computer?

A3. Internet users should install anti-virus software and personal firewall in the personal computers. It is also important to keep the software up-to-date to cater for any new alerts identified. Other good habits include:

- be very cautious about opening attachments in e-mails from unfamiliar sources, and avoid visiting or downloading software from suspicious websites
- never access your internet services such as internet banking through hyperlinks embedded in emails, internet search engines, suspicious pop-up windows or any other doubtful channels (customers should connect to a bank website through typing the authentic website address in the address bar of the browser or by bookmarking the genuine website and using that for subsequent access)

- don't disclose logon passwords or OTP to any person through any means such as e-mail, over the phone or in person
- review your transaction records regularly and verify transaction details on the notification (e.g. SMS message) sent from the bank, and report to your bank immediately if you notice any suspicious transactions in your bank accounts or discover any suspicious web page
- follow the security tips published by your banks when conducting internet banking transactions

Q4. Does the Trojan Horse attack also applicable to the transaction signing security tokens (i.e. a security token equipped with numeric keypad on the device – see the pictures below)?

A4. A transaction signing security token will require user to input transaction specific information (e.g. the beneficiary's account number) into the token in order to generate a unique OTP for authenticating that particular transaction. However, fraudsters may trick an internet banking customer into entering certain numbers (which is likely the account number controlled by the fraudster) into the transaction signing security token to obtain an OTP and thereafter make a fund transfer from the victim's account to theirs. It is therefore important for internet banking users to note that in general banks' internet banking logon process will **NOT** require customers to enter into their security token any numbers displayed on the customers' computer screen. That means, if customers come across an internet banking logon page which requests them to input specified numbers into their transaction signing security token to obtain an OTP then they can assume that it is not a genuine bank website and should report to their banks promptly.

Q5. Given the increasing risk of internet banking frauds, is it still safe to use internet banking?

A5. Internet banking services in Hong Kong are safe to use so long as both the banks and the customers have taken appropriate precautionary measures.

Security device with transaction signing function

Henry Cheng
Executive Director (Banking Supervision)
24 April 2013