Smart Tips on Using Internet Banking Services

Published by

- Hong Kong Monetary Authority

Supported by

- Communications Association of Hong Kong
- The Hong Kong Association of Banks
- Hong Kong Computer Emergency Response Team Coordination Centre
- Hong Kong Computer Society
- Hong Kong Police Force
- Joint Electronic Teller Services Limited
- Office of the Government Chief Information Officer

Major Safety Tips on Using Internet Banking Services

Login passwords – Set a password that is difficult to guess and different from the ones for other services. The login password should be changed regularly and should never be stored on computers, mobile phones or placed in plain sight. Keep the security token (if any) provided by your bank at a safe place.

Computers and mobile phones – Protect your computer and mobile phone for logging into your Internet banking. Avoid using public computers or public Wi-Fi to access Internet banking services.

Bank websites and Apps – Internet banking should be accessed by entering the bank's website address directly, or using a bookmark or an Internet banking mobile application (App). Never access your bank website or provide your personal information (including your password) through any hyperlinks or attachments embedded in emails or from websites.

Login process – Beware of any unusual login screen or process (e.g. a suspicious pop-up window or request for providing additional personal information) and whether anyone is trying to peek at your password. Log out immediately after use.

Messages from banks – Check your bank’s SMS messages and other messages in a timely manner and verify your transaction records. Inform your bank immediately in case of any suspicious situations. Banks will not ask for any sensitive personal information (including passwords) through phone calls or emails.

Major Tips on Protection of Your Computers and Mobile Phones

Passwords – Set difficult-to-guess passwords for your computer and mobile phone. Activate the auto-lock function.

Secure systems and software – Use the latest versions of operating system, Internet banking App and browser. Do not jailbreak or root your mobile phone or tablet.

Beware of computer viruses – Install and update promptly your security software. Do not download or open doubtful files, browse suspicious websites, or click on the hyperlinks and attachments in questionable sources (e.g. emails, instant messaging, SMS messages, QR codes). Download and upgrade your Apps from official App Stores or reliable sources only.

Network functions – Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) not in use. Choose encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection settings.

Reference: The Government’s Cyber Security Information Portal
(http://www.cybersecurity.hk)