使用網上銀行的主要保安提示

Major Safety Tips on Using Internet Banking Services

一、登入密碼－設定難以猜破及與其他服務不同的密碼，並定期更新。切勿記錄密碼在電腦、手機或當眼位置。如銀行有提供保安編碼器，便需妥善保管。

1. 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.

二、電腦及手機－保護用以登入的電腦及手機。避免透過公用電腦或公共無線網絡登入。

2. 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.

三、銀行網址及 App－應透過輸入銀行網址、書籤或網上銀行流動應用程式(App)登入。切勿透過電郵、網上的超連結或附件登入或提供個人資料(包括密碼)。

3. 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.

四、登入過程－檢查登入網頁及過程有否異樣(如出現可疑的彈出視窗、被要求提供額外的個人資料)及是否有人窺看密碼，並在使用後馬上登出。

4. 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.

五、銀行訊息－及時查閱銀行發出的手機短訊及通訊，並查核交易紀錄。若發現可疑情況，應立即通知銀行。銀行一定不會以電話或電郵，要求提供任何敏感的個人資料(包括密碼)。

5. 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.

保護電腦及手機的要點

Tips On Protection Of Your Computers And Mobile Phones

一、鎖機密碼－設定難以猜破的鎖機密碼及自動上鎖功能。

1.Passcodes for mobile phones – Set a passcode for your mobile phone that is difficult to guess. Activate the auto-lock function.

二、安全系統及程式－使用最新版本的操作系統、網上銀行 App 及瀏覽器。切勿用 Jailbreak (越獄)或 Root 機等手法改裝手機及平板電腦。

2.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.

三、提防電腦病毒－安裝和及時更新保安軟件，切勿瀏覽可疑網站，或開啟可疑電郵/手機短訊的超連結及附件。只從官方應用程式商店或可信的來源下載及升級應用程式。

3. Beware of computer viruses – Install and update promptly your security software. Do not browse suspicious websites or click on the hyperlinks and attachments in suspicious emails/SMS messages. Download and upgrade your Apps from official App stores or reliable sources only.

四、網絡功能－關閉無需使用的無線網絡功能(如 Wi-Fi、藍芽、NFC)。如需使用 Wi-Fi，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。

4. 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.

五、參考:香港政府的網絡安全資訊站 (http://www.cybersecurity.hk/tc/index.php)

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