



# 網路金融交易趨勢與安全

華銀作業管理部 林國音

近年來網際網路蓬勃發展，金融機構也各自發展出網路銀行、網路ATM，以擴大客戶服務及市場需求為目的，而從早年簡單的ID、Password（帳號、密碼）即可使用，到近年OTP、iKey、晶片金融卡...等相繼出籠，無非是為了提高交易安全，以因應越來越多元、越趨近於現實的網路環境。『使用網路金融交易』成為大家又愛又擔心的議題，愛的是簡便、省時、快速、靈活，而又擔心其安全性，萬一那天電腦中毒自己動了起來，自動轉帳怎麼辦？免驚啦！本文告訴您正確的觀念 -

## 網路金融交易勢不可擋！？

您曉得使用「線上金融交易」有多少人嗎？

依據創市際市場研究顧問公司(www.insightxplorer.com)於2006年12月，針對台灣地區網友進行一項金融服務使用行為調查顯示，目前持有金融商品的網友，「網路銀行」的使用率為34%，而「網路ATM」的使用率為32.6%。

而本行去年底網路銀行交易金額已達約台幣2.3兆，而網路ATM的交易量與實體ATM比率已達12%。





究結果，25-29歲為線上轉帳主要使用族群，30.6%的網友曾使用線上轉帳，26.9%網友曾利用網路ATM進行轉帳；另外有52.7%的網友表示未來願意使用線上轉帳，並且以24歲以下、女性族群最具成長潛力。這些跡象均顯示

出，隨著年輕網友消費能力的成長茁壯，網路金融交易將是一股不可擋的趨勢。

「網路銀行」、「網路ATM」等網路金融服務，對客戶及銀行的效益如下：

表 1 「網路銀行」、「網路ATM」對客戶及銀行的效益

好處	客戶	銀行
24小時、全年無休、不受地點限制的營運與服務	【提高客戶滿意度】 客戶無論在公司、在家裡只要電腦能夠連上網路，都可以使用本行網路金融服務，可以省去等候及交通時間，全方位的服務可提高滿意程度。	【增加本行金融商品的銷售機會】 由於不受時間、地點的限制，所以本行金融商品的銷售時點亦不會受到時空的限制。
自助式的交易	【提供財務電子化，降低客戶作業成本及臨櫃等候時間】 個人、企業帳務總覽，即時掌握資料調度，與企業戶的內部系統結合、資金收付容易，亦符合越來越多網路族群的喜好逛網路如逛街行為模式。	【降低本行營運與作業成本】 由於客戶可以自行完成金融交易及上線申請，節省臨櫃作業、繕打的人工營運成本。
結合企業財務系統	【降低人工作業成本及減少錯誤發生】 與企業戶的財務系統結合，整批資金預約調度，且有完整的編輯、核定、放行機制，並減少人工繕打的錯誤。	【藉由電子化建構非價格競爭門檻，可避免同業價格競爭】 當電子化交易對客戶服務的價值大於費用折扣的價值時，價格削減的競爭不一定可取得優勢。

推廣網路金融的三大關鍵 - 安全性與使用習慣

針對未使用過「網路銀行」服務的網友探詢沒有使用的原因，發現「擔心

資料安全」(58.3%)為最主要的原因，其次則是「比較習慣親自至銀行辦理相關服務」(37.1%)。

網路金融服務節省了實體的營運成

本，並且增加對於客戶的行銷管道，不少金融業者也都大力推展。而「網路金融的安全性與使用習慣」是推廣網路服務時兩大關鍵。

## 認識與控制風險，才能獲得機會與效益

### 為何要先認識風險？

網路金融交易是趨勢亦存在風險。事實上風險無所不在，機會與風險是一體兩面，逃避風險不如去認識風險，如在混沌之初人類不使用及學習控制火燭，也沒有如今日的進步，所以我們應隨著世界的腳步，一同與客戶紮實地踏出穩健的步伐 - 「認識與了解網路金融交易的風險」，才曉得如何去控制風險。

「風險存在於一切事物中！無論你做或不做，風險依舊存在！」

艾爾本 & 羅邁可

### 認識網路金融交易的風險 - 什麼是惡意程式

目前網路上造成安全上的威脅大致分為「電子郵件病毒」、「蠕蟲」、「特洛伊木馬程式」、「垃圾郵件」、「間諜程式」、「網路詐欺」等，其散播及型態各有所不同，但都有可能對個人資料及金融交易造成威脅。

### 電子郵件病毒

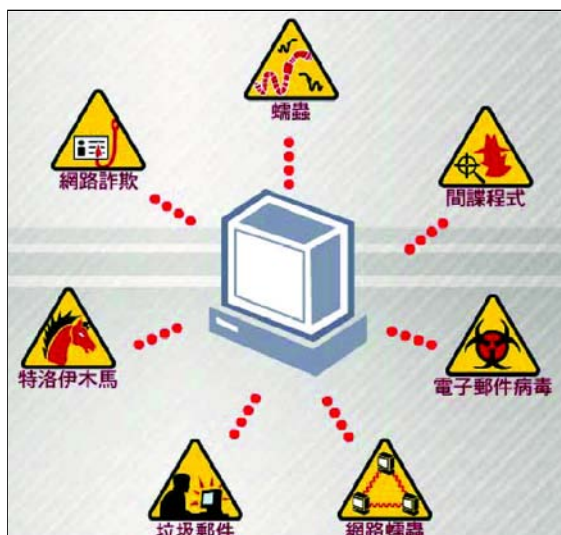
電子郵件病毒通常以附件的形式與郵件一併發送，看起來無害的附件可能帶有惡意病毒。

### 蠕蟲

電腦蠕蟲散播的方式類似現實世界的昆蟲，不斷的自我複製，然後像蠕蟲般在電腦網路中移動，並藉此方法感染其他電腦。

### 特洛伊木馬程式

特洛伊木馬程式就如神話所述，特洛伊木馬程式看起來像是有用軟體的電腦程式，但是卻會危害電腦的安全性（如格式化磁碟、刪除檔案、竊取密碼等）。



資料來源：趨勢科技



## 垃圾郵件

垃圾郵件為用於廣告或未經請求而發送的郵件，對於病毒及蠕蟲等惡意程式的散播者，是很方便的散播方式，因為垃圾郵件通常包含了攻擊性內容和圖片。

## 間諜程式

所謂間諜程式即是使用軟體來監視用戶習慣及個人信息，在沒有用戶的許可或完全不知情的狀況下，將資訊發送給第三者。

## 網路詐欺

詐欺者會在網路上設置看似為真的假網站，發送假裝為金融機構的電子郵件，以願意上勾的方式，取得用戶個人資料。

### 安全的網路金融交易

控制風險 預防風險  
健全的安控機制 良好的使用習慣

### 認識風險

「安全的網路金融交易」建立在認識、控制、預防風險的基礎上

## 控制風險 - 本行提供的保障

在了解網路上對金融交易的威脅後，我們來看本行除內部資訊安全的防護外，提供給網路銀行及網路ATM的用戶什麼樣的保障。

### 網路銀行

#### 1. 128bits SSL全程加密

(<https://ibank.hncb.com.tw>)

在資料傳輸過程中，使用128bits SSL encryption封包傳送資料，就算有人截到資料也無法解開或讀取資料。

#### 2. SSL轉帳密碼：

SSL轉帳密碼僅限於轉入約定帳戶，無法轉入非約定帳戶，對於想要簡單享受網銀便利，SSL轉帳密碼是不二的選擇。

#### 3. OTP：

OTP (One Time Password) 即採用密碼保鏢產生使用一次即丟密碼，由於密碼是由離線產生，所以沒有受到上述各種網路威脅的風險。

#### 4. FXML + OTP：

自96.5.21起使用本行FXML憑證交易的網路銀行用戶必須配合OTP的使用，因此除享受FXML採PKI (CA認證) 的交易保證外，更有OTP無

網路威脅風險的好處。

#### 5. 企業戶編核放分層授權

企業戶可以設定編輯、核定、放行分層授權，可以符合企業內控需求，防杜人為疏失。

#### 6. 每年提醒變更密碼

為預防過久未變更密碼可能會造成洩漏的風險，本行貼心地每年以電子郵件及簽入個人化提示的方式，提醒用戶要變更密碼。

### 網路ATM

#### 1. 128bits SSL全程加密

(<https://www.smartatm.com.tw/>)與網路銀行在資料傳輸過程中有相同的保障，使用128bits SSL encryption封包傳送資料，就算有人截到資料也無法解開或讀取資料。

#### 2. 晶片金融卡

晶片金融卡本身即是一項安全的機制，因為持有卡片的用戶，才能夠使用網路ATM使用該卡片帳戶的餘額，而且晶片卡密碼使用卡片驗證，不會在網路上傳輸，沒有被攔截的風險。

#### 3. 用戶端回應機制（動態驗證碼、支援二代讀卡機）

本行網路ATM採用動態驗證碼且支援二代讀卡機，可以防止惡意程式的威脅。

## 預防風險 - 如何自我保護

使用網路金融交易的保護，除了銀行提供的防護，更重要的是用戶自我使用的習慣，就如同實體的金融交易於網路交易也是一樣，憑證、密碼、晶片金融卡，就如同印鑑及存摺要保管妥當，要如何自我保護，歸納了十點如下：

#### 1. 設定密碼時提高警覺

不要使用身分證字號、生日、電話號碼或具規則性排列等容易被猜中的英文字串或數字作為密碼，並且要妥善保管，切勿使用在其他網路服務的帳戶名稱及密碼，例如電子郵件或網路簡訊，以免被有心人士猜中。

#### 2. 切勿向任何人透漏或寫下您的密碼

客戶本人應該是唯一知道的網路銀行/晶片金融卡密碼的人。確實保密自己的密碼，避免書寫於實體卡片上，切勿向任何人透露。無論在任何情況下，本行不會詢問客戶的密碼，若遇到該情況，請撥打24小時客服專線。

#### 3. 養成定期更改密碼的習慣

保障客戶使用本行網路銀行的安全，簽入密碼及SSL、FXML轉帳密碼，最少一年內須變更，且到期前一個月，在您簽入網路銀行時，提醒作密碼變更，並限制密碼不可與



您身份證字號相同。

#### 4. 注意個人電腦的保密及防護

必需清楚地知道每一個與自己共用電腦的人，同時嚴格限制任何未經授權人士使用個人的電腦，並且必須安裝個人防火牆及防毒軟體。

#### 刑事局提網頁釣魚案件檢測移除程式供民眾下載(更新2007.04.12)

[http://www.cib.gov.tw/news/news02\\_2.aspx?no=343](http://www.cib.gov.tw/news/news02_2.aspx?no=343)

#### 5. 避免提供個人資料及金融資料

一般的電子郵件與網頁並沒有受到安全加密的技術保護，當無法確認傳輸的資料可受到網路安全機制的保護，千萬不要向任何人透露您的密碼。

#### 6. 避免在公共電腦及網咖上進行任何網路金融交易

當在公共場所使用電腦時，要記得確實簽退「網路銀行」或「網路ATM」並關閉瀏覽器，以避免藉由瀏覽器回上一頁的功能，而洩漏資料予第三人。

並請不要勾選「記住」「身分證字號/統一編號」和「代號」的功能，以避免洩漏資料予第三人。

#### 7. 確實核對網址

當利用網路銀行或網路ATM交易時，在登錄網銀時應留意核對所登錄的

網址，以避免不慎進入假網站。

本行之網路銀行網址為

<https://ibank.hncb.com.tw>

本行之網路ATM網址為

<https://www.smartatm.com.tw>

可使用瀏覽器「加到我的最愛」功能，增加以後使用的方便性。

#### 8. 妥善保管交易明細表

只要透過網路銀行或網路ATM進行任何的網路交易動作，如：轉帳、付費等交易，應保存最後執行動作的資料或予以記錄，如發現異常交易或帳務差錯，立即與本行聯繫，出示網路紀錄，避免造成損失。

#### 9. 遠離來源不明的電子郵件

也許會收到像似好友或是公司的電子郵件，但是事實上有些偽造的電子郵件很有可能會讓您在不知情的情況下，下載病毒程式或是木馬程式，或是將您引導到一個偽造的銀行網站。因此切勿閱讀與開啟不明電子郵件的附件檔案。

#### 10. 務必簽退及取出卡片、憑證

為了預防您離開電腦過久，以至遭他人竊用，若您欲離開本行網路銀行或網路ATM，敬請務必執行簽退，並關閉瀏覽器及取出卡片或憑證，以保障您的權益及帳戶安全。網路銀行或網路ATM會在您逾十分鐘未做任何交易時，自動執行簽退服務。



表 2 「網路威脅」VS. 「安全機制」

網路威脅	用 戶	網路銀行	網路ATM
電子郵件病毒 蠕蟲 特洛伊木馬程式 垃圾郵件 間諜程式 網路詐欺 人為疏失	1. 設定密碼時提高警覺 2. 切勿向任何人透漏或寫下您的密碼 3. 養成定期更改密碼的習慣 4. 注意個人電腦的保密及防護 5. 避免提供個人資料及金融資料 6. 避免在公共電腦及網咖上進行任何網路金融交易 7. 確實核對網址 8. 妥善保管交易明細表 9. 遠離來源不明的電子郵件 10. 務必簽退及取出卡片、憑證	128bits SSL全程 加密 SSL轉帳密碼 OTP FXML + OTP 企業戶編核放分層 授權 每年提醒變更密碼	128bits SSL全程 加密 晶片金融卡 用戶端回應機制

結語

表 3 2015年全球重大趨勢與影響( 資料來源：經濟部)





由經濟部於2005年底所提出的「2015年全球重大趨勢與影響」(表3)的「網路化世界」,在全新的商業模式運作下,金融服務為商業活動極重要的一環。在尼爾森於去年十月至十一月一項全球性調查中顯示,全球已有三成二的網路使用者,一周至少使用二到三次網路銀行服務,但台灣的使用率仍然偏低只有26%,名列全球排名倒數第七,由此可知在台灣網路金融服務仍有很高的成長空間;所以

「金融服務 - 網路化」是金融業必然的趨勢。

在我們立足台灣放眼世界的同時,網路金融服務固然相當地方便好用,但電腦備有再好的自動化安全措施,個人沒有良好的使用習慣,就如同將印鑑、存摺等重要物品公開任人取用,但是本文講了那麼多,真要是記不太起來呢。其實很簡單,只要有「網路金融交易安全小祕訣」(表4),就能「保庇您的電腦嘜卡到陰」。

表4 網路金融交易安全小祕訣

網路銀行『四勿四要』	網路ATM『四不一沒有』
<p>四勿</p> <p>『勿』使用容易猜測的密碼</p> <p>『勿』透露或寫下網銀密碼。</p> <p>『勿』提供個人及金融資料予他人。</p> <p>『勿』在公共電腦上進行交易。</p> <p>四要</p> <p>『要』定期更改密碼</p> <p>『要』注意收到的郵件是否可疑</p> <p>『要』妥善保存交易明細表</p> <p>『要』記得簽出及抽出iKey</p>	<p>四不一沒有</p> <p>『不』在公共場所使用</p> <p>『不』安裝不明軟體</p> <p>『不』開啟來路不明郵件</p> <p>『不』將卡片密碼借與他人</p> <p>『沒有』使用時,勿將卡片留置讀卡機</p>

