目錄

一、 登入 FBO 系統 - 1 -

二、 新增一般使用者 - 2 -

三、 作業系統 IE 設定 - 5 -

四、 其他功能說明 - 7 -

1、 基本資料設定 - 7 -

2、 重設密碼： - 7 -

五、 使用者登入 - 8 -

六、 OTP 使用說明 - 9 -

七、 客戶使用安全須知 - 10 -

說明：

密碼函上之密碼為系統管理者身份(admin)，系統管理者的帳號是無法使用查詢或交易。

所以必須先使用系統管理者去新增一般使用者，再使用一般使用者帳號登入富邦商務網，才可使用交易或查詢等功能。

一、登入 FBO 系統

FBO 網址：https://fbo.fubon.com

Step1. 企業統一編號：輸入企業編號(統一編號)或個人身分證號

使用者代碼：初始化為五碼數字(請參照密碼函)

使用者密碼：初始化為六碼英、數字(請參照密碼函)

台北富邦銀行 富邦商務網 密碼函

Taipei Fubon Commercial Bank「Fubon Business Online (FBO)」Password Notification

富邦商務網啟用密碼單 FBO Administra

統一編號 Customer Code：
VN9620 29

序 號：00001

戶 名 Customer Name：
TESXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

列印日期 Print Date：20140808

富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

Step2. 首次登入，系統強制變更使用者代號及設定新密碼。

系統管理者新代碼：最短六個字，可以單純英文或單純數字。

密碼單舊密碼：六碼英、數字(請參照密碼函)

系統管理者新密碼兩次：**需為英文+數字混合**。(英文區分大小寫)

系統管理者姓名、電子郵件：輸入管理者個人資料。

二、新增一般使用者

說明：

開始新增一般使用者，再使用一般使用者帳號登入富邦商務網，才可使用交易或查詢等功能。

路徑：系統權限/權限管理/使用者資料維護

Step1. 先按[查詢]

若為”新加坡地區”客戶，請在畫面顯示電子憑證或 OTP 驗證機制時，輸入 OTP 密碼或於插入放行憑證後輸入 PKI 密碼

Step2. 進入使用者維護畫面後，會出現管理者，直接按[新增]

富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

Step3. 輸入使用者基本資料，完成後按[下一步]。

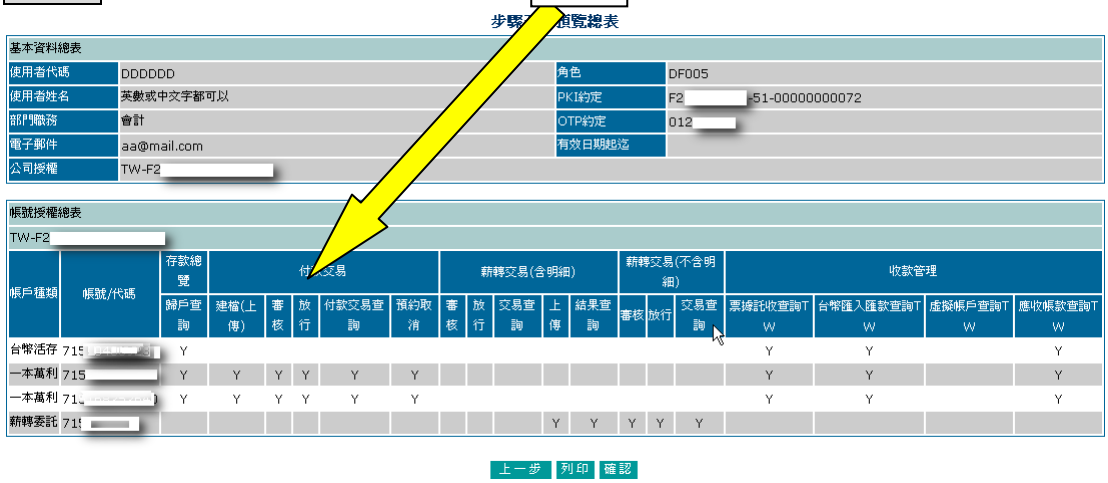
Step4. 設定使用者可查詢的帳號(預設都打勾)，完成後按[下一步]。

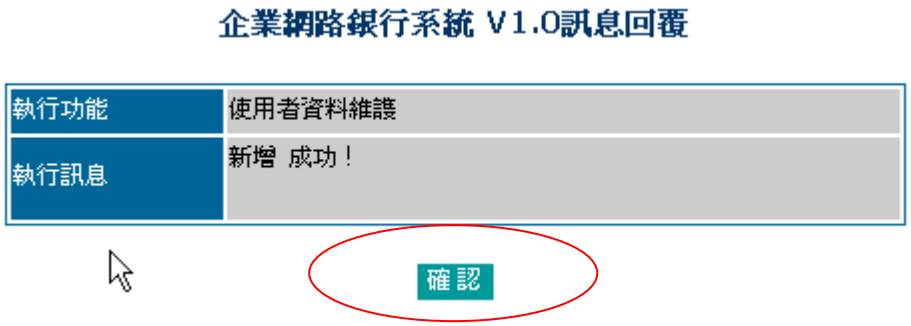
Step5. 設定使用者可查詢的類別(預設都打勾)，完成後按[下一步]。

富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

Step6. 設定使用者可使用的權限(預設都打勾)，完成後按[下一步]。

Step7. 再次確認無誤後，按[確認]。





設定完成後，系統會自動發送使用者初次登入的密碼到使用者的 email。
再用這個使用者登入富邦商務網，才可以開始查詢作業。

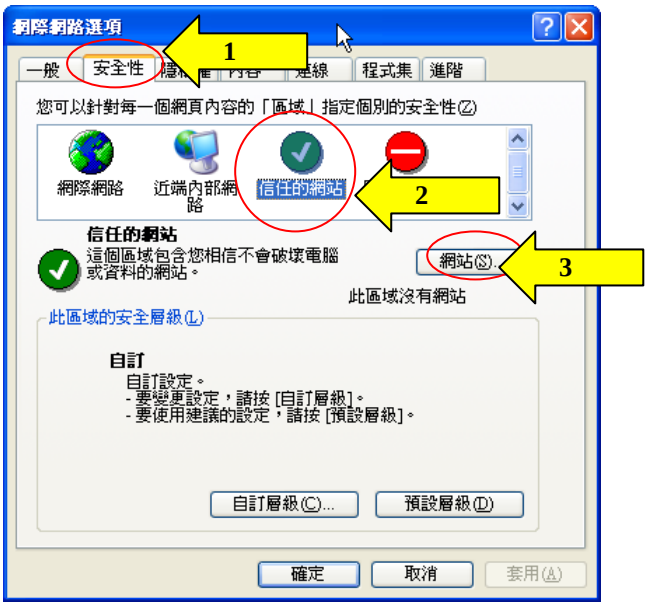
富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

三、作業系統 IE 設定

先開啟瀏覽器(IE)，再到 IE 的上面執行下列步驟

A. [IE]→[工具]→[網際網路選項]

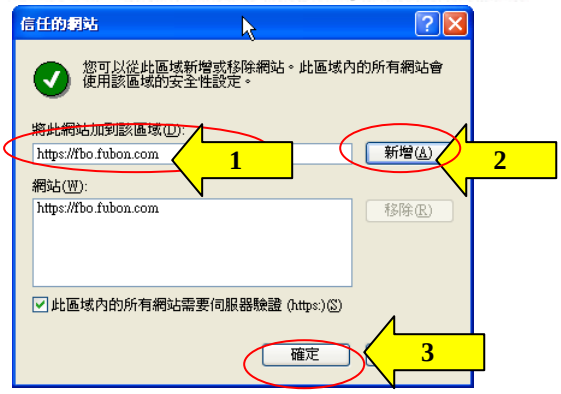
B. [安全性]→[信任的網站]→點[網站(s)]



將富邦商務網加入信任的網站，輸入 https://fbo.fubon.com

再按[新增]→[確定]。

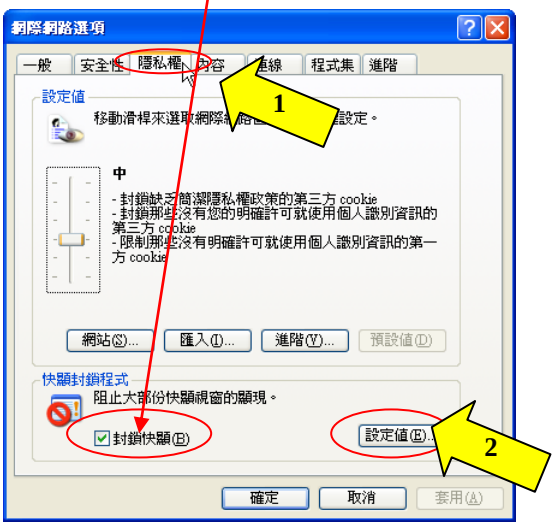
富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860



C. 開放彈跳視窗

點選[隱私權]→[設定值(E)]

註：若無勾選[封鎖快顯]，則[設定值]按鈕會反白無法點選。



輸入富邦商務網網址：fbo.fubon.com，輸入完後按[新增]→[關閉]。

富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

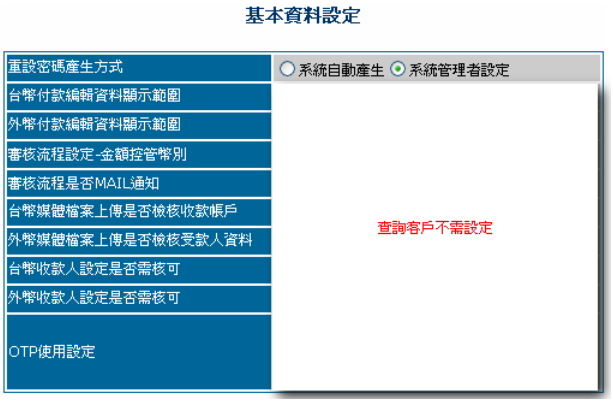
四、其他功能說明

1、 基本資料設定

路徑：系統權限/系統管理/基本資料設定

可設定該公司在執行哪些交易時，需要使用硬體安控來判斷身份別，或需另一人審核才生效。

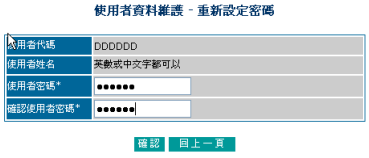
- ✓ 重設密碼產生方式：可設定重新設定使用者密碼時，是管理者手動輸入或者是系統自動發送 email 通知該使用者。
- ✓ 台外幣付款編輯資料顯示範圍：(查詢客戶不需設定)。
- ✓ 台外幣媒體檔是否檢核：(查詢客戶不需設定)。
- ✓ 台外幣收款人是否需核可：(查詢客戶不需設定)。
- ✓ OTP 使用者設定：(查詢客戶不需設定)。



2、 重設密碼：

路徑：系統權限/權限管理/使用者資料維護/重設密碼

管理者可以重新設定使用者密碼，設定方式有兩種，一種為管理者手動輸入；一種則為系統自動發送 email 密碼函給使用者。(視基本資料設定欄而定)



富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

五、使用者登入

企業統一編號：輸入企業編號(統一編號)或個人身分證號

使用者代碼：請參照密碼通知

使用者密碼：請參照密碼通知

PKI 密碼、OTP 密碼：請依持有的設備輸入密碼

若為”新加坡地區”客戶，請增加輸入 OTP 密碼或於插入放行憑證後輸入 PKI 密碼

六、OTP 使用說明

1. 首次啟用動態密碼機：
   - 啟動電源(按下功能鍵[OK])
   - 螢幕自動顯示{ NEW PIN }，請於此時輸入使用者自行設定之「使用者密碼」，密碼長度固定為 4 碼。輸入完成後請按下[OK]
   - 待螢幕出現{ CONF.PIN }訊息後，請再次輸入相同的 4 碼「使用者密碼」。輸入完成後請按下[OK]，即可完成「使用者密碼」設定

2. 日常交易，產生動態密碼：
   - 啟動電源(按下功能鍵[OK])
   - 待螢幕出現{ SELECT }訊息後，按下數字鍵[1]
   - 待螢幕出現{ PIN }後，輸入動態密碼機之 4 碼「使用者密碼」後按下功能鍵[OK]，經系統確認密碼無誤後，螢幕顯示 8 位數的數字動態密碼
   - 將產生的 8 碼數字動態密碼填入交易單中即完成
   - 若於輸入 4 碼「使用者密碼」按下功能鍵[OK]後螢幕出現{ FAIL }訊息時，為密碼錯誤訊息，請再次輸入 4 碼「使用者密碼」。(連續五次錯誤，動態密碼機將會鎖碼)

3. 使用者變更動態密碼機密碼：
   - 啟動電源(按下功能鍵[OK])
   - 待螢幕出現{ SELECT }訊息後，長按數字鍵[4]
   - 待螢幕出現{ PIN }後，輸入原設定之動態密碼機 4 碼「使用者密碼」後按下功能鍵[OK]
   - 待螢幕出現訊息{ NEW PIN }，請於此時輸入使用者欲變更後之「使用者密碼」，密碼長度固定為 4 碼。輸入完成後請按下[OK]
   - 待螢幕出現{ CONF. PIN }訊息後，請再次輸入變更後之 4 碼”使用者密碼”。輸入完成後請按下[OK]，即完成密碼變更作業

富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

七、客戶使用安全須知

台北富邦企業網路銀行-FBO 富邦商務網(以下簡稱"富邦商務網")之安全機制完全遵循最新、最高安全水準之國際標準及業界技術規範，您當可安心使用本行所提供的網路銀行各項服務。本行提供之企業網路銀行是相當安全的，依據分析目前所發生的網路交易安全問題，大多數是出自人為操作上的疏忽，只要平常稍加注意，就不會發生任何的損失！！

為此，本行特別提供下列安全須知供您參考，並提醒您應時時注意：

網路安全威脅

威脅一：電腦病毒 (Computer virus)

所謂電腦病毒是一種會自我複製的可執行程式，常透過網路、磁片、電子郵件等傳輸媒介「傳染」給其他電腦。電腦病毒通常被設計成定時或遇到特殊狀況時發病。當病毒發病時，它很可能會破壞硬碟中重要資料，有些病毒則會重新格式化 (Format)您的硬碟。就算病毒尚未發病，它也可能會佔據一些系統的記憶空間使電腦執行效能會變得比較慢。

威脅二：網路釣魚 (Phishing)

利用電子郵件通知、假網址的方式誘導網路使用者進入詐騙者所製作的「假網頁」。受害者在不知情的狀況下輸入密碼、信用卡號等機密資訊，歹徒取得資料後以各種管道盜用受害者資料及財產。

威脅三：木馬程式、後門程式

木馬程式攻擊手法主要是騙取被害人執行特定的程式來植入木馬程式，再透過該程式伺機執行其惡意行為(如格式化磁碟、刪除檔案、竊取密碼等)。所謂的後門程式，讓駭客可以規避正常的系統稽核程序直接進入到系統，此時的木馬(也稱後門程式)不以竊取機密資料為目的，而以開個後門方便駭客進入系統進行破壞或盜用。

威脅四：電腦蠕蟲

電腦蠕蟲也不會像木馬程式一樣感染其他檔案，但『本尊』會複制出很多『分身』，然後擴散至電腦網路中的各個電腦。最常用的方法是透過區域網路（LAN）、網際網路（Internet）或是電子郵件來散佈自己。
最明顯的感染的症狀就是電腦執行速度會降低甚至強迫關機。

威脅五：系統弱點

電腦的作業系統如 WINDOWS、SOLARIS 等在設計時未考量周全，致使駭客利用作業系統缺陷進行病毒、木馬或蠕蟲的攻擊。以一般用戶所使用的 WINDOWS 作業系統，微軟公司均不定時發布所發現的系統弱點及修補程式供使用者自行下載更新。

交易安全須知

須知一：開戶與申請網路銀行時應注意保密

- 有鑑於不法份子可能利用各種機會騙取您的交易密碼，建議您於開戶時應單獨與行員辦理開戶業務，密碼變更時也避免他人窺視，以免造成有心人士取得開戶資料與交易密碼，影響您的權益。

須知二：請您妥善保管各種密碼

(例如:登入密碼、PKI 卡密碼、OTP 隨機動態密碼設備之開機密碼等)

- 不要使用易被破解之數字做為密碼(例如:公司統編、授權碼、個人身份證號碼、生日、電話或重複的數字)。
- 當您申請相關業務時，請於第一時間內變更銀行發給您的密碼函內之密碼且牢記，並請勿將使用者代號、密碼記錄於電腦或行動裝置內。
- 請您經常不定期變更您的各種密碼。(尤其懷疑密碼有外洩情形時更應馬上變更)
- 切勿將個人的任何密碼告知他人(包括本銀行職員)，銀行一定不會以電話、電子郵件等方式，要求提供任何敏感的個人資料（包含密碼），並請提高警覺，勿將使用者代號、密碼交付給第三人或其他非授權網站。
- 請勿將任何密碼書寫於明顯且易讓他人取得之處，或透過未加密機制傳送密碼。
- 輸入密碼時注意不要被周遭他人窺視。
- 各種不同交易的密碼應有所區分，以免被人一次猜中所有密碼。
- 當您使用的密碼已連續錯誤了 3 次，本行將暫停該密碼對應的網路銀行、PKI 卡或 OTP 隨機動態密碼設備的功能，若欲恢復相關功能或您懷疑有不法人士以嘗試錯誤方式猜測密碼時，請立即洽服務專線由本行專責人員協助處理。.

須知三：請您確認所登入的網址為合法註冊的富邦商務網網址

- 在您執行簽入之前，請先確認您所登入之網址是否為合法註冊的富邦商務網網址，本行富邦商務網之網址為：https://fbo.fubon.com/。
- 若非本行合法註冊的富邦商務網網站，請勿輸入任何 ID.、授權碼及密碼，以避免遭偽冒之網站騙取您的登入資料。
- 請勿透過電子郵件、網路超連結或附件進行網路銀行登入或提供、輸入任何 ID、授權碼及密碼，以避免遭偽冒之網站騙取您的登入資料。
- 若需下載安裝或更新安控程式，請勿透過非本行合法註冊的富邦商務網網站進行相關作業（例如電子郵件、網路超連結）。

須知四：請您使用 PKI 卡交易後，勿將 PKI 卡留在讀卡機上

- 為避免您的 PKI 卡被他人盜用，請您執行完插卡授權交易後，將 PKI 卡隨手抽出妥善保管，勿將 PKI 卡留在讀卡機上。

須知五：當 PKI 卡遺失時請您立刻向本行申請憑證暫禁（暫時掛失）

- 您的 PKI 卡儲存有您的電子憑證，若遺失時，請立刻向本行申請憑證暫禁（暫時掛失），以避免遭他人盜用影響您的權益。
- 申請手續請洽服務專線，將有專人協助處理。

須知六：若您的 OTP 隨機動態密碼設備遺失時，請您立刻向本行申請掛失

- 除了 PKI 卡之外，您可能使用本行的 OTP 隨機動態密碼設備來授權交易，請妥善保管該設備，如有遺失請立刻洽服務專線向本行申請掛失，以避免遭他人盜用影響您的權益。

須知七：請您交易完畢或臨時離座時一定要簽出網路銀行並關閉瀏覽器

- 因瀏覽器具有回到上一頁的功能，當您因故臨時離座或執行完所有交易或查詢動作之後，記得一定要簽出網路銀行系統，並關閉瀏覽器，以避免旁人利用瀏覽器之相關功能取得您交易或查詢的重要資料，若因電腦故障不正常簽出，請等待十分鐘後再試一次。
- 建議電腦設定自動登出（上鎖）功能，並設定不易被破解之密碼為電腦登入密碼。

須知八：請您小心警覺他人是否正冒用您的 ID.進行網路銀行交易

- 當您欲簽入網路銀行，系統卻出現「重複簽入，請重新再試」的訊息時，請稍後再試一次，若反覆出現同樣訊息，則可能有他人正冒用您的身份使用網路銀行，此時請儘速與本行連絡。
- 請檢查登入網頁及過程是否有異樣（例出現可疑的彈出視窗、被要求提供額外的個人資料）及是否有人於窺視密碼並在使用後馬上登出。

須知九：請您盡量不要使用公共場所提供的電腦進行網路銀行交易

- 請盡量不要使用公共場所提供的電腦進行網路銀行交易，以避免暫存在電腦內之簽入 ID.、密碼及所有交易記錄等資料，被有心人士所截取。
- 請盡量不要使用公共場所提供的公共無線網路登入網路銀行交易，以避免簽入 ID.、密碼及所有交易記錄等資料被有心人士所截取。
- 建議關閉無需使用的無線網路功能(如 Wi-Fi、藍芽、NFC)，如需使用 Wi-Fi，應選用加密的網路，並移除不必要的 Wi-Fi 連線設定。

須知十：請您定期更新您電腦上的防毒軟件版本並掃除病毒

- 目前有心人士可透過病毒或詭似之惡意程式碼(如特洛依病毒)取得您存於電腦內的相關資料，請在您的電腦上安裝防毒軟件，並定期更新病毒碼版本，同時掃除病毒。

須知十一：慎防您的密碼被不法者盜竊

- 請您盡量不要進入有可疑的網站，因非法者可利用此途徑秘密地安裝程式，以盜取客戶按鍵時的密碼。
- 請您小心處理不明來歷的電郵。
- 建議您使用加密技術保護高度敏感或機密資訊。

須知十二：定時核對帳戶資料

- 為避免您的帳戶被盜用，請經常核對您的帳戶結餘及對帳單上的資料。
- 及時查閱銀行發出的通訊訊息，並查核交易紀錄。若發現可疑情況，請立即洽服務專線由本行專責人員協助處理。
- 建議您定期備份帳戶結餘、存款異動明細等帳戶資料數據。

須知十三：教您如何辨識偽網站與詐騙 eMAIL

提醒您，最近有網路詐騙的集團，專門製作「與知名網站幾可亂真的假網站」或假借台北富邦名義發送 eMAIL 收集客戶個人機密資料。建議您在使用網路銀行時，盡量以「直接鍵入網址」的方式進入網站，或將常用的網頁設為「我的最愛」網頁，以避免用搜尋或連結方式誤入假網站。

要如何確認您所登入的網站是台北富邦的網站? 您可以從下列幾點來做判別：

如何辨識偽網站

1. 確認顯示的網址是否正確

本行網站首頁對外網址為 www.fubon.com，富邦商務網則是 fbo.fubon.com 開頭。

建議您盡量從本行首頁進入，並針對您常用的功能設定「我的書籤」或「我的最愛」。盡量不要從網路上搜尋本行網址，就可減少上錯至假網站的風險。

2. 辨識網站安全驗證

您可在網路銀行登入前在頁面右下方發現一黃色小鎖頭圖示

or

，並按左鍵二次，這時會有一跳出之小視窗，您可檢視畫面的憑證資訊是否發給為 fbo.fubon.com(富邦商務網網路銀行見下圖)以及憑證有效時間是否過期？

圖.<富邦商務網網路銀行憑證示意圖>

- **如何辨識詐騙 eMAIL**

要如何確認所收到的 eMAIL 確實為富邦商務網所發送的?

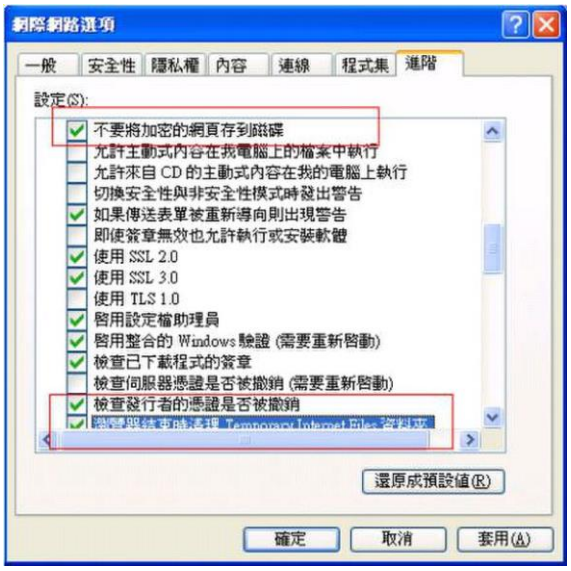
您可以從 Email 寄件者的網址是否為如下所示來做判斷，目前本行正式對外發送 MAIL 的網址：
fboop.bank@fubon.com

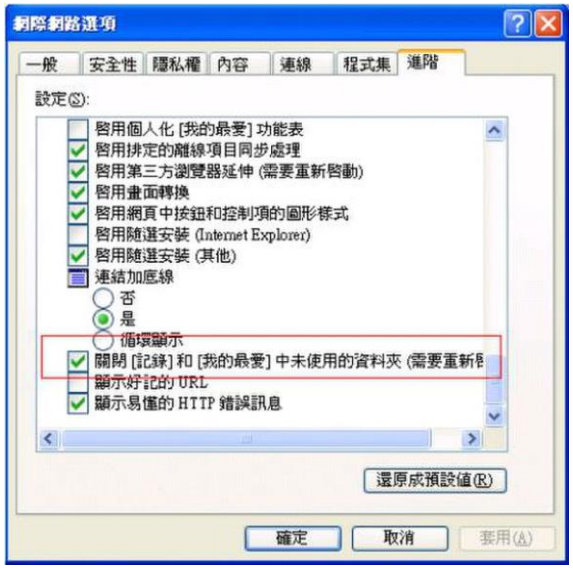
若您對於 eMAIL 之真實性存有疑慮，建議您刪除該垃圾郵件或鏈接郵件。

- **做好 IE 設定，防堵您的安全漏洞**

在網路交易上，除了要避免將個人密碼透漏給他人外，還要注意因瀏覽器設定所引起個人資料或交易資料外洩的風險，在這裡提供三點網路安全設定的小秘訣，其說明如下：

1. 清除網頁暫存資料儲存及記錄（預設值設定為未勾選.....請打勾）

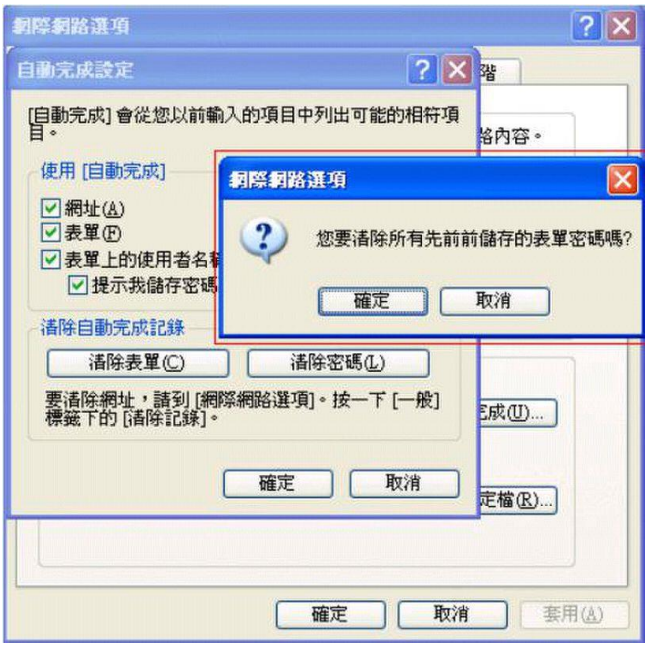




富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

2. 清除密碼記憶

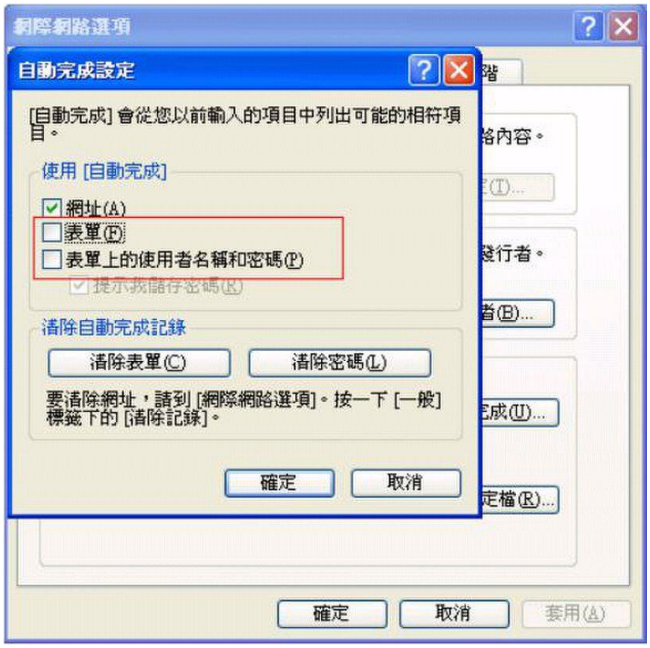
工具→ Internet 選項→內容→自動完成→清除密碼→確定。



3. 取消自動完成功能

工具→ Internet 選項→內容→自動完成→使用［自動完成］

→表單上的使用者名稱和密碼"不要打勾" →確定。



富邦商務網 客服專線 台灣地區請撥：02-6639-7131、香港地區請撥：852-2822-7799
越南地區：84-28-39325888、新加坡地區：65-6470-9860

- **如何防止駭客攻擊**

・建議您於電腦內安裝防火牆和防毒軟體。

・不要收來歷不明的信件。

・不要使用來歷不明的軟體。

・不要上不當的網站，如色情網站。

・eMail 的圖片最好不要下載。

・定期檢查電腦有沒有不明軟體。

・不使用電腦時，了解有無不明資料傳出　　。

・重要資料不要存在硬碟內（建議存在隨身碟或光碟中）。

・建議您不應選擇可將用戶代碼(使用者名稱)和密碼，存儲或保留於瀏覽器的選項（自動完成）。

須知十四：聯絡資訊異動時，請主動通知銀行更新

當您的地址，聯絡電話或其他個人資料有任何更改，請立即通知本銀行更正。本銀行將依照客戶最後登記地址發出通訊，通訊可以專人送遞、郵遞、圖文傳真、專用電報或電子郵件發出。如由專人送遞，在送遞或留放在上述地址後，即視為已送達客戶。如採用圖文傳真、專用電報或電子郵件，則於發出當日即視為已傳達客戶。如採用郵遞，於寄出後即視為已寄達。

須知十五：相關權益法規可至以下機構查詢

欲了解常見的網路銀行詐騙案例或客戶使用網路銀行之相關權益，可連結至以下機構查詢，以確保自身權益。

- 行政院金融監督管理委員會（http://www.banking.gov.tw/）
- 中華民國銀行公會商業聯合會（http://www.ba.org.tw/）
- 香港金融管理局（http://www.gov.hk/tc/residents/）
- 香港銀行公會（http://www.hkab.org.hk）
- 如您需要更詳盡之網銀保安說明，香港金融管理局(Hong Kong Monetary Authority)亦提供網上保安小冊子供您下載，網上保安小冊子之內容由香港銀行公會發佈，並獲消費者委員會、香港金融管理局及香港警務處認可。請連結至香港金融管理局網站 http://www.info.gov.hk/hkma/chi/consumer/internet_banking_index.htm 下載。
- 另<<銀行營運守則>>是由香港銀行公會及存款公司公會聯合發布，並得到香港金融管理局(Hong Kong Monetary Authority)認可，為銀行提供服務予客戶時應遵守之準則，如需下載<<銀行營運守則>>內容得知更詳細資料，請連結至 http://www.info.gov.hk/hkma/chi/consumer/index.htm

感謝您對台北富邦銀行-富邦商務網所提供的服務有進一步的了解，希望這樣的提醒可以協助您更安全地運用網路銀行所帶來的便利，若對網路交易的安全有任何疑慮，歡迎您聯絡服務專線將有專人為您作更詳盡之解說。

若有問題，歡迎致電客服專線，將有專人為您服務。