

客戶服務中心

[授權管理者初次使用申請](#)

[使用聯邦 e 聯網系統設備需要符合哪些要項](#)

[聯邦 e 聯網服務項目](#)

[常見問題 Q&A](#)

[防範網路釣魚](#)

[密碼設定原則](#)

[安全宣告](#)

[文件下載專區](#)

[客戶服務專線](#)

客戶服務專線

說 明

銀行業務諮詢、申訴與掛失服務專線
(02) 2545-1788 進線後請按 19 轉接專人

文字客服 ([前往文字客服](#))

[TOP](#)

使用聯邦 e 聯網系統設備需求符合哪些要項

系統設備需求

1. 作業系統：windows 7 以上或是 APPLE MAC
2. 瀏覽器：IE、Edge、Chrome、Firefox、Safari、Opera
3. 憑證元作環境需求：

| Windows ServiSign | Mac ServiSign |
|-------------------------------|---------------------------------|
| ※ Windows ServiSign PKCS11 介面 | ※ Mac ServiSign PKCS11 介面 |
| ※ Windows：7/8/8.1/10 作業系統 | ※ Mac OS：10.11/10.12/10.13 作業系統 |
| 🚩 IE：11 | 🚩 Safari：9 以上 |
| 🚩 Edge：40 以上 | 🚩 Chrome：68 以上 |
| 🚩 Chrome：68 以上 | 🚩 Firefox：61 以上 |
| 🚩 Firefox：61 以上 | |
| 🚩 Opera：18 以上 | |

[TOP](#)

| 類 別 | 功 能 項 目 |
|--------|--|
| 臺幣帳戶查詢 | <ul style="list-style-type: none"> · 餘額查詢 · 交易明細查詢 · 定期存款帳戶查詢/解約試算 · 託收票據查詢 · 支存提回票據查詢 · 當日匯入匯款查詢 · 虛擬帳號查詢 · 退匯明細查詢 |
| 臺幣貸款查詢 | <ul style="list-style-type: none"> · 貸款明細查詢 |
| 外幣帳戶查詢 | <ul style="list-style-type: none"> · 餘額查詢 · 交易明細查詢 · 定期存款帳戶查詢 |
| 收付款服務 | <ul style="list-style-type: none"> · 單筆轉帳 · 整批轉帳 · 轉帳付款交易查詢/註銷 · 薪資轉帳 (企業戶需另外簽訂「受託代發員工薪津約定書」) · 薪資轉帳付款交易查詢/註銷 · 外幣單筆轉帳 · 外幣匯出匯款 · 外幣結匯 · 外幣付款交易查詢 |
| 企業設定管理 | <ul style="list-style-type: none"> · 付款帳戶管理 · 收款帳戶管理 · 檔案匯入格式設定 |
| 授權中心 | <ul style="list-style-type: none"> · 人員管理 · 角色管理 · 簽核流程管理 · 交易簽核流程設定 |

常見問題 Q&A

| 項次 | 常見問題 |
|----|--|
| Q1 | 利用憑證 UBKEY 執行放行發生「找不到憑證」時，應如何處理？ |
| A1 | 請檢查您的電腦是否有安裝其他的讀卡機，或是其他憑證，如工商憑證、銀行放行憑證等，請先移除或拔除後，請再重新操作，即可排除此一問題。 |
| Q2 | 憑證 UB KEY 密碼輸入錯誤鎖住了怎麼辦？ |
| A2 | <ol style="list-style-type: none">1. 憑證 UB KEY 密碼輸入連續錯誤達 3 次，系統則會鎖住暫停使用。2. 請攜帶帳戶原留印鑑至本行任一分行臨櫃填寫「聯邦 e 聯網 申請/變更/註銷申請書」辦理憑證 UB KEY 密碼解鎖，憑證 UB KEY 無須送回銀行，即可重新使用。 |
| Q3 | 公司授權管理者 (admin) 忘記「使用者代號/密碼」或是密碼輸入錯誤鎖住了怎麼辦？ |
| A3 | <ol style="list-style-type: none">1. 授權管理者 (admin) 密碼輸入連續錯誤達 5 次，系統則會鎖住暫停使用。2. 請攜帶帳戶原留印鑑至本行任一分行臨櫃填寫「聯邦 e 聯網 申請/變更/註銷申請書」辦理授權管理者 (admin) 密碼重設，即可重新使用。 |
| Q4 | 一般使用者代號/密碼忘記了或是密碼輸入錯誤鎖住了怎麼辦？ |
| A4 | <ol style="list-style-type: none">1. 一般使用者密碼輸入連續錯誤達 5 次，系統則會鎖住暫停使用。2. 請通知公司授權管理者 (admin) 登入系統後執行「管理設定」→「授權中心」→「人員管理」點選「變更」，重新設定一組「登入密碼」或「使用者代號」，重設或變更該使用者之代號/密碼，交易完成後，該使用者即可重新登入使用。 |

✚ 何謂網路釣魚？

Phishing 與英文「fishing」（釣魚）發音相同，兩者意義也差不多。若引用直接中文典故：「姜太公釣魚，願者上鉤」是最佳翻譯。根據反網路釣魚工作小組（APWG）定義，網路釣魚詐騙手法，多半是利用**偽造電子郵件與網站**作為「誘餌」，輕則讓使用者不自覺洩漏個人資料，成為垃圾郵件業者的名單；嚴重一點，電腦可能會被植入木馬程式，破壞系統或讓重要資訊遭竊。而最危險的情況是：誘騙使用者的銀行帳號密碼、信用卡號與身分證字號等機密資料，釣魚者再伺機偷竊金錢或有價資訊。

網路釣魚所用的誘餌千奇百怪，包括偽裝成知名銀行或線上服務業者通知使用者資料過期、無效需要更新，或者是基於安全理由進行身分驗證，要求使用者重新確認銀行帳號密碼或信用卡號。只要使用者一時不察經由電子郵件指引的網址連結偽造的帳號登錄頁，就成了數位版姜太公手中「願者上鉤」的肥美大魚。

✚ 網路釣魚常見手法及防範方法：

1、要求確認信用卡號與密碼，駭客趁機偷卡號

釣魚詐騙者偽裝銀行寄發的電子郵件，要求確認個人信用卡號與密碼，經由郵件內偽連結指引連至假的網路銀行，只要一時不察卡號密碼一併遭竊。

防範方法：本行絕對不會以寄發 e-mail 郵件要求客戶揭露帳戶資訊或任何密碼，請提高警覺，千萬不要回覆此類郵件，並立即刪除。若有任何問題或收到任何可疑郵件，請隨時與本行客服部門 02-2545-1788 聯絡。

2、偽造假網路銀行網站，偷取網路銀行帳號與密碼

惡意偽造一模一樣的網站內容，還註冊一個類似的網域名稱混淆視聽，難辨真偽，只要客戶一登入此網站，輸入網路銀行的帳號及密碼，即被竊取帳戶密碼，致使帳戶金額被盜轉。

防範方法：要到銀行交易網站請自行輸入網址，不要利用點選信件內之連結或以網頁連結方式直接連接至銀行交易網站。另外，執行重要交易前，養成檢查網址正確性之習慣。

3、下載修補程式?小心木馬上身

以電子郵件為誘餌，拐騙使用者存取信件中的網頁連結、或開啟附加檔案，建議收件者快速下載微軟漏洞修補程式在不知不覺中被植入木馬程式，藏匿在使用者電腦中伺機竊取銀行帳戶密碼。

防範方法：對不明郵件請立即刪除，建議各位客戶最好能安裝防毒軟體，確實更新病毒定義檔，避免開啟來路不明的電子郵件中的網址和附加檔案，並且妥善制定防火牆規則，慎防受害。

4、我中獎了...？是被騙了！

毋須利用病毒或程式碼，單用電子郵件散發假消息誘拐使用者匯出錢財。在這之前，可能已有「上游」詐騙者經由網路抽獎得知受害者資料。

防範方法：所有易被詐騙的案例中，大多數人是「貪小失大」的原因居多，甚有「貪大失更大」之事例發生，是以防詐第一要務為：「勿存貪念」，貪念是好的魚餌，是造成您被騙的主因。另外設法確實向真正的機構查詢，亦可避免被騙。

建議各位用戶最好能安裝防毒軟體，目前大部分的防毒軟體都有技術可以防範網路釣魚，其次是屏除貪念，再來當網友上網瀏覽網頁以及輸入個人資料時，要特別注意網頁的網址是不是所要連結網頁的網址。或是利用各銀行及金融機構所提供連絡電話確認其提供資料是否屬實，多一份小心、少一份貪念，或許就可以讓你自己免於受到網路釣魚客詐騙手段的危害。

■ 密碼設定規則

1. 密碼需為 6~12 碼
2. 密碼需包含英文及數字
3. 不可連續 4 碼相同或 4 碼排序文數字組合，如：1234 (不可)、abcd (不可)、aaaa (不可)、3333 (不可)
4. 不可和原密碼相同

■ 密碼安全設定及管理技巧

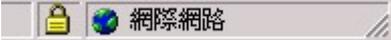
1. 設定網路密碼時，儘量使用英文字母和數字的組合。
2. 避免設定「懶人密碼」，所謂「懶人密碼」係指一般大眾喜歡設定自己熟悉的文數字作為金融交易密碼，常見的「懶人密碼」如下：
 - (1) 身分證字號的排列組合
 - (2) 生日數字的排列組合
 - (3) 家中或公司電話排列組合
 - (4) 幸運數字
 - (5) 英文名字
 - (6) 共用同一組密碼
3. 定期更改您的密碼，不要將您的密碼告知他人。
4. 為避免駭客入侵您的電腦，竊取您的機密資料，請勿點選打開來路不明的電子郵件、賀卡及附件檔等；並請您加裝安全性防衛軟體如防火牆或防毒軟體，隨時注意台灣微軟公司及趨勢科技公司所公佈的更新程式或最新病毒碼，適時更新您的電腦，減少木馬程式（後門程式）、病毒、蠕蟲及其他程式惡意碼 入侵您的電腦，側錄您的資料。

密碼設定原則

網站傳輸資料加密保護

1. 本行網路銀行是使用 SSL128 位元的安全加密機制，任何網路交易的客戶，資料傳輸皆經加密處理。
2. 本行網路銀行服務系統均依照財政部所頒「金融機構辦理電子銀行業務安全控管作業基準」之規定辦理。
3. 本行資料庫受防火牆機制重重保護，以防範駭客無法入侵銀行內部網路系統，並保護取得客戶交易機密資料。
4. 客戶設定的密碼在本行系統均經 "亂碼" 加密保護，任何人無法透過任何查詢方式或系統程式由銀行端知道客戶自行設定的密碼。
5. 當您使用本系統時，若您停止操作超過 10 分鐘，本系統將自動登出，以避免您的交易被旁人偷窺或介入，確保您的權益。
6. 密碼連續輸入錯誤達到 5 次，密碼將被註銷停用。

SSL 網站檢查

1. 若您使用 IE 瀏覽器，請檢視瀏覽器視窗右下方，必須要出現如右一個已鎖上的小鎖圖案。

2. 要確認您現在的 SSL 加密強度，只須將滑鼠指向該小鎖，即會顯示 SSL 安全保護的加密位元。

網路安全提醒

- 秘訣一：登入前請確認聯邦個人網路銀行網址 (<https://mybank.ubot.com.tw/>)、企業網路銀行網址 (<https://myebank.ubot.com.tw/>)與行動銀行手機應用程式「 聯邦 樂活 APP」名稱正確性。
- 秘訣二：請提高警覺防範詐騙集團套取密碼。
- 秘訣三：請於輸入密碼時，提高警覺避免旁人窺視。
- 秘訣四：且勿與其他應用系統及服務密碼共用。
- 秘訣五：請勿點選來路不明網址及程式並建議安裝防毒軟體。
- 秘訣六：請勿書寫密碼於金融卡或其他明顯且他人可取得處。
- 秘訣七：請勿記錄密碼於電腦或行動裝置內。
- 秘訣八：請勿透過未加密機制傳送密碼。

取消記憶功能

1. 開啟 I.E.→工具→INTERNET 選項→內容→自動完成→清除自動完成紀錄 (清除密碼) →確定。(此時電腦會幫您清除以前儲存的表單密碼)
2. 工具→INTERNET 選項→內容→自動完成→使用『自動完成』→清除「表單上使用者名稱和密碼」→確定。

表單下載

| 說 明 |
|---|
| 聯邦 e 聯網 服務約定條款 前後對照表 |
| 聯邦 e 聯網 服務約定條款 (B2B01) |
| 聯邦 e 聯網 服務申請書-新申請 (B2B02) |
| 聯邦 e 聯網 約定事項變更申請書 (B2B03) |
| 聯邦銀行電子訊息傳真修改確認書 (B2B05) |
| 聯邦 e 聯網 關係戶授權書 (B2B06) |
| 聯邦 e 聯網 外幣匯出匯款申請書 (B2B07) |
| 聯邦 e 聯網 安控設備簽收單 (B2B08) |
| 聯邦 e 聯網 服務申請書(OBU 專用) (B2B09) |