

常用社群軟體帳號安全防護及遭盜用應變處理

一、帳號為什麼會被盜用

(一) 誤入釣魚網站並輸入帳號資料

詐騙者可能假冒朋友、平台客服、宅配業者或活動單位，以「幫忙投票」、「帳號即將停權」、「重新認證」、「帳號違規」等理由，引導使用者點擊外部連結。網站外觀看起來可能與官方網站相似，但目的其實是誘導使用者輸入帳號、密碼或驗證碼。

LINE 官方曾說明「幫朋友投票」的實際案例，使用者點擊假的投票頁面後，被引導至偽裝的 LINE 登入頁面；Meta 也提醒，假客服可能以帳號發生問題為由，要求使用者緊急登入釣魚網站，甚至要求提供雙重驗證碼。常見情境如下：

適用平台	常見情況
LINE	幫忙投票、假宅配通知、假帳號認證、假好友要求登入
Facebook	假客服、假違規通知、假粉專停權或帳號停權通知
Instagram	假帳號驗證、假客服、假活動或外部登入頁面
Threads	假客服、外部釣魚連結或冒用 Meta 相關服務名義的訊息
各平台	「這是你嗎？」、「幫我投票」、「立即驗證」等訊息搭配不明連結

(二) 把認證碼或登入資料交給別人

認證碼是平台確認操作者身分的重要資訊。

LINE 官方特別提醒，除了本人正在執行帳號移轉等操作外，一般使用 LINE 並不需要把認證碼告訴其他人。若有人要求提供電話號碼、密碼或收到的認證碼，應提高警覺。

Meta 也提醒，假冒客服的詐騙可能要求使用者提供登入密碼，甚至雙重驗證碼，一旦交出這些資訊，攻擊者即可嘗試盜用帳號。

因此，不論對方自稱朋友、客服、公司人員或活動主辦單位，均不應輕易提供帳號密碼及驗證碼。

(三) 掃描來源不明的 QR Code

QR Code 本身不等於詐騙，但使用者可能不知道掃描後執行的是什麼操作。

LINE 官方說明，詐騙者可能假借「加好友」或「驗證身分」等理由要求掃描 QR Code，實際上卻將使用者引導至電腦版或網頁版 LINE 的登入及認證程序。因此，掃描 QR Code 後若出現登入、輸入認證碼或帳號移轉等提示，應先確認是否確實為本人原先要進行的操作。

(四) 使用過於簡單或重複的密碼

數位發展部資通安全署指出，弱密碼及跨平台共用密碼會增加帳號遭入侵的風險；若其中一項服務的帳號密碼外洩，相同帳密可能再被拿去嘗試登入其他服務。資安署因此建議使用至少 15 個字元、具複雜度的密碼，或透過密碼管理工具產生及管理密碼。

LINE 也提醒，如果使用容易推測或與其他服務相同的密碼，可能增加非法登入風險。

(五) 安裝不明程式或授權可疑服務

部分第三方程式、網站或服務可能要求以社群帳號登入。Meta 提醒，當未知網頁或第三方應用程式要求輸入 Facebook、Instagram 等社群帳號登入資料時，應提高警覺。

LINE 也提醒，帳號可能與外部服務產生連動；即使後續變更 LINE 密碼，也不代表所有已登入或連動的服務會自動登出，因此仍需另外檢查。

二、常見情形整理

適用平台	常見情況	主要風險	建議作法
LINE	幫忙投票、活動連結要求重新登入	可能被導向假登入頁，輸入電話、密碼或認證碼後，帳號資料可能遭取得。	不要直接從訊息連結登入；即使由熟人傳來，也先另外確認。
LINE	要求提供簡訊或 LINE 認證碼	認證碼可能被用於登入或移轉帳號。	不是本人正在操作，就不要提供認證碼。
LINE	要求掃描 QR Code「加好友／驗證身分」	可能實際進入電腦版或網頁版登入與認證流程。	確認畫面用途；出現登入或認證提示時先停止操作。
Facebook／Instagram／Threads	帳號違規、即將停權、立即驗證等訊息	可能利用緊迫感誘導至釣魚頁面，騙取帳密或驗證資訊。	自行開啟官方 App 或網站查看，不從可疑訊息直接登入。
各平台	不同服務共用相同密碼	某一服務帳密外洩後，可能被拿去嘗試登入其他服務。	重要帳號使用不同密碼。

各平台	密碼太簡單或容易猜測	弱密碼降低帳號安全性。	使用較長、具複雜度且不重複的密碼。
各平台	沒有啟用雙重／多因素驗證	密碼一旦遭取得，少了一道額外防護。	支援的平台優先啟用雙重或多因素驗證。
各平台	收到非本人操作的登入通知卻未處理	可能代表有人嘗試登入或帳號安全資訊已外洩。	立即變更密碼、檢查登入裝置與安全設定。

三、怎麼避免帳號被盜用

帳號安全防護不能只依靠密碼，而應建立多層次防護。

（一）不同服務使用不同密碼

電子郵件、LINE、Facebook、Instagram 等重要服務，原則上不宜重複使用相同密碼。

尤其電子郵件常被用來重設其他平台的密碼，一旦電子郵件帳號同時遭到入侵，可能連帶影響其他帳號。

資安署建議避免在社群媒體、電子郵件與網路銀行等服務使用相同密碼。

（二）設定足夠強度的密碼

避免以生日、電話號碼、姓名、簡單英文單字或「123456」等容易猜測的內容作為密碼。

資安署建議密碼長度至少 15 個字元，並混合不同類型字元，亦可使用密碼管理工具協助產生及管理密碼。

（三）啟用雙重或多因素驗證

雙重驗證是在密碼之外增加第二道身分驗證。

Meta 官方說明，Facebook 與 Instagram 均提供雙重驗證功能；當使用新電腦、手機或平板存取帳號時，可增加一道帳號防護。

資安署亦建議民眾優先為網路銀行、Google、LINE、社群媒體等重要服務設定兩步驟驗證。

操作方式

各平台可依下列路徑設定（實際選單名稱可能因 App 版本或裝置略有不同）：

- LINE（網頁登入雙重認證）：主頁 → 設定 → 我的帳號 → 開啟「網頁登入雙重認證」。
- Facebook：選單／右上大頭貼 → 「設定與隱私」→ 「設定」→ 「帳號管

理中心」→「密碼和帳號安全」→「雙重驗證」→ 選擇 Facebook 帳號並依畫面設定驗證方式。

- Instagram：個人檔案 → 右上角選單 →「帳號管理中心」→「密碼和帳號安全」→「雙重驗證」→ 選擇 Instagram 帳號並依畫面設定驗證方式。

（四）不要從陌生訊息直接登入

遇到下列文字時應提高警覺：

「帳號將在 24／48 小時內停權」

「你的帳號違反社群規範」

「請立即完成驗證」

「朋友需要你幫忙投票」

「你的包裹無法配送」

「請提供認證碼」

「請掃描 QR Code 驗證身分」

正確方式應是自行開啟官方 App 或官方網站確認帳號狀態，而不是直接從收到的訊息或郵件連結登入。

LINE 與 Meta 官方均將利用緊迫感誘導使用者登入釣魚網站列為需要注意的詐騙手法。

（五）定期檢查登入裝置

資安署建議定期檢視帳號登入時間、地點及裝置，發現不明登入紀錄時，應立即登出相關裝置並更換密碼。

Meta 的帳號安全功能亦提供近期登入裝置檢視及登出功能。

四、粉絲專頁、官方帳號或具管理權限帳號的額外防護

管理者帳號遭盜用時，影響可能不只個人帳號，也可能擴及粉絲專頁、連結帳號或共同管理的數位資產。Meta 官方說明，具有 Facebook 粉絲專頁「完整控制權」的人員可管理設定、增刪其他人的存取權，甚至刪除粉絲專頁，因此此類關鍵帳號應採較高強度的安全管理。

建議作法如下：

- 管理權限依工作需要分配：Facebook 粉絲專頁可區分完整控制、部分控制或工作權限；完整控制者具有較高管理能力，應僅授予確有需要且可信任的人員。
- 避免多人共用同一組管理帳號或密碼；應依人員分配各自所需權限，職務異動、離職或不再負責時，應即時調整或移除其管理權限。

- 管理者優先啟用雙重驗證，並定期檢查登入裝置、帳號安全設定及管理權限名單；發現非本人登入或操作時，立即登出可疑裝置並更換密碼。
 - 綁定的電子郵件也屬重要復原管道，應使用與社群帳號不同的強密碼，並在電子郵件服務支援時啟用雙重驗證；若電子郵件本身遭入侵，可能連帶影響社群帳號復原。
 - LINE 官方帳號另有「管理員」與「操作員」等權限；LINE 官方說明，具有管理員權限者可新增或變更其他管理員，而操作員無法新增管理員。因此，持有 LINE 官方帳號管理員權限的人員帳號應視為關鍵帳號加強保護。
 - 若具管理權限的帳號疑似遭盜，除處理該人員帳號外，如仍有其他可信任且具管理權限的人員可操作，應同步檢查管理權限名單、連結帳號及近期設定變更；發現陌生或可疑存取權時，應依平台提供的權限管理功能移除或調整。
- 補充說明：目前查得 LINE 官方資料可明確佐證的是「LINE 官方帳號」具有管理員／操作員權限；本文此處僅就 LINE 官方帳號之管理權限提出建議，不延伸套用於一般 LINE 群組。

五、發現帳號異常時怎麼辦

收到異常通知，不一定表示帳號已遭盜用，但若確認並非本人操作，應立即處理。

常見異常徵兆包括：

- 收到不是本人操作的登入通知。
- 收到自己沒有申請的認證碼。
- 出現自己不認識的登入裝置。
- 帳號自行傳送訊息。
- 出現自己沒有發布的貼文或限時動態。
- 無故追蹤、加好友或傳送好友邀請。
- 綁定的電子郵件或電話遭修改。
- 密碼突然無法使用。

數位產業署也將「未經授權的登入通知」、「陌生貼文、訊息或好友請求」及「綁定 Email 或手機號碼遭更改」列為 Facebook 帳號可能遭盜用的異常跡象。此時建議依序處理如下：

- 第一步：確認是不是本人操作。

例如剛剛是否有換手機、登入電腦版或自己操作帳號設定。

- 第二步：如果不是本人操作，立即變更密碼。

新的密碼不應與原密碼或其他網站密碼相同。

- 第三步：檢查目前登入中的裝置。

將不認識或已不使用的裝置登出。

- 第四步：開啟雙重驗證並再次檢查帳號安全設定。

避免攻擊者再次利用已取得的密碼登入。

- 第五步：檢查帳號綁定資料。

確認電子郵件、電話號碼及其他帳號復原資料沒有被修改。

- 第六步：檢查第三方應用程式或外部服務。

若曾登入可疑網站或授權陌生服務，應解除連動並登出。

- 第七步：若已發現非本人貼文、訊息或詐騙內容，先保存必要證據，再收回、刪除或檢舉，並通知可能受到影響的親友。

LINE 官方在帳號仍可正常使用、但出現異常登入等情況時，建議變更密碼、關閉允許其他裝置登入、確認登入中的裝置並登出可疑裝置。

六、各平台帳號遭盜後怎麼處理

此時最重要的是先判斷：「我還能不能登入原本的帳號？」不同情況的處理方式不同。

（一）LINE 帳號仍然可以使用

如果 LINE 仍可正常收發訊息，不代表沒有他人登入或操作；若發現非本人活動，仍須立即檢查並排除可疑登入。依 LINE 官方說明，若「登入中的裝置」出現非本人操作的裝置，應先將該裝置登出並變更密碼。

此時應立即：

- 更換 LINE 密碼。
- 關閉允許其他裝置登入。
- 查看登入中的裝置。
- 將可疑裝置登出。
- 檢查是否有非本人傳送的訊息。
- 檢查與 LINE 帳號連動的服務。

特別要注意的是，LINE 官方說明，即使已變更 LINE 密碼，也不一定會自動登出所有已連動服務，因此仍需另外解除可疑應用程式連動並登出相關網站。

（二）LINE 突然顯示「已登出帳號」

這是 LINE 特別需要提醒民眾的情況。

LINE 官方表示，若突然出現「已登出帳號」，應先嘗試執行「再次登入」。同時，官方特別提醒：

不要點選「刪除」。

因為在再次登入畫面中點選刪除，可能導致裝置中的 LINE 相關資料遭刪除。

若無法再次登入，可由帳號本人透過 LINE 官方「與我們聯絡」表單提出申請，由 LINE 確認帳號是否遭第三人盜用。

（三）Facebook 帳號遭盜用

Facebook 官方提供遭入侵帳號的專用復原程序。若帳號遭到入侵，Meta 建議使用以前曾登入過 Facebook 的裝置，進入官方 hacked 帳號復原頁面，依指示進行帳號復原。

數位發展部數位產業署於「斥詐人生－防詐工具箱」設置「Facebook 帳號被盜怎麼辦？」專頁，依帳號目前狀況，將處理方式區分為「確認帳號是否遭盜」、「仍可登入時的處理」、「已無法登入時的帳號復原」，以及「取回帳號後的安全強化」等階段。依該頁內容整理如下：

➤ 如何確認帳號是否被盜？

1. 查看是否有未經授權的登入通知。
2. 查看是否出現陌生的貼文、訊息或好友請求。
3. 查看綁定的 Email 或手機號碼是否被更改。
4. 若發現可疑活動，立即更改密碼或進行帳號復原。

➤ 確定帳號被盜，但還能登入，該怎麼辦？

1. 點擊右上角大頭貼照 → 「設定與隱私」→ 「設定」。
2. 選擇「帳號管理中心」→ 「密碼和帳號安全」。
3. 點擊「更改密碼」並輸入新密碼。

➤ 帳號被盜，而且也無法登入，該怎麼辦？

1. 如果只是忘記密碼：在登入畫面點選「忘記密碼？」→ 輸入 Email、手機號碼或帳號名稱 → 依指示重設密碼。
2. 如果完全無法存取帳號：使用曾登入 Facebook 的裝置，開啟 Facebook 「Report compromised account」帳號遭入侵處理頁面。

3. 選擇「有人未經許可登入我的帳號」等選項。
4. 提供 Email、密碼或其他身分驗證資料。
5. 數位產業署該頁說明：Facebook 會暫時鎖定帳號並進行人工審核。
6. 收到「Final step to get back on Facebook」郵件後，點擊「Reset password」重設密碼。
7. 若上述方法仍無法解決，依 Facebook 官方帳號復原指南尋找適合情況的處理方式。

➤ 取回帳號後，如何提高安全性？

1. 登入 Facebook → 「設定與隱私」→ 「隱私設定檢查」。
2. 選擇「保障帳號安全的方式」。
3. 設定雙重驗證，提高帳號安全性。
4. 另可建立高強度 Facebook 密碼，並檢查其他帳號安全設定。

將數位產業署的說明簡化為：

發現非本人操作



先確認是否仍能登入 Facebook



仍能登入 → 立即更換密碼 → 檢查帳號安全設定



無法登入，但可使用原 Email／手機 → 使用「忘記密碼」重新設定



完全無法登入 → 使用曾經登入過 Facebook 的裝置 → 進入 Facebook 官方遭入侵帳號復原程序 → 完成身分驗證



帳號取回 → 開啟雙重驗證 → 設定高強度且不重複的密碼 → 再次檢查帳號安全設定

(四) Instagram 帳號發生問題

Instagram 帳號復原仍應以 Meta／Instagram 官方登入及帳號復原機制處理。

若連原本綁定的電子郵件或電話號碼都無法使用，Instagram 官方建議先嘗試恢復該電子郵件或電話的存取權限，或更新可使用的帳號聯絡資訊。因此，平時維持正確且仍可使用的電子郵件及手機資料，也是帳號復原的重要準備。

（五）Threads 帳號

Meta 於 2026 年 4 月公布改版 Meta Account，支援 Facebook、Instagram、Messenger、Threads 等 Meta 服務，並將密碼、雙重驗證、電子郵件及 Security Checkup 等部分安全設定集中管理。Meta 並說明，Accounts Center（帳號管理中心）將於未來一年逐步自動更新為 Meta Account，因此不同帳號目前可能看到不同介面。

因此，Threads 若出現帳號安全問題，應依使用者目前實際看到的 Meta Account 或 Accounts Center（帳號管理中心）介面，以及 Meta 官方最新安全與復原程序處理，不宜直接套用早期 Threads 完全依附 Instagram 帳號的舊有說法。

七、帳號救回後還要檢查什麼

帳號重新登入成功，並不代表風險已經完全解除。應進一步確認攻擊者在控制帳號期間是否已經修改資料、傳送訊息或取得其他服務的登入權限。

（一）重新檢查密碼

應重新設定安全性較高的密碼。

如果原本密碼也用在電子郵件、購物網站或其他社群服務，相關服務也應一併更換密碼。

（二）檢查電子郵件及手機號碼

確認帳號綁定的電子郵件及電話仍為本人所有。

如果發現陌生電子郵件、電話號碼或其他復原資料，應立即移除或依平台提供的安全程序處理。

（三）重新檢查所有登入裝置

檢查目前登入中的手機、平板、電腦及瀏覽器。

無法辨識的裝置應登出。

Meta 官方的安全功能可查看近期登入裝置，LINE 亦提供登入裝置管理功能。

（四）檢查第三方服務及授權

確認帳號是否新增陌生的應用程式、網站或外部服務。

LINE 官方特別提醒，即使變更密碼，也不一定能讓所有連動服務自動登出，因此需要個別解除可疑服務。

(五)檢查貼文、私訊及其他操作

查看帳號遭盜期間是否出現：

- 非本人發布的貼文。
- 陌生限時動態。
- 向好友傳送的詐騙訊息。
- 新增陌生好友或追蹤帳號。
- 私訊要求親友匯款或提供認證碼。
- 帳號名稱、大頭貼或個人資料遭修改。

若有非本人發出的詐騙內容，應先迅速保存必要證據（如貼文／訊息畫面、帳號資訊、時間、登入通知等），再收回、刪除或檢舉詐騙內容，並通知親友不要相信相關訊息。

(六)重新確認雙重驗證與帳號安全設定

取回帳號後，應確認雙重驗證仍正常啟用，並重新檢查登入裝置、安全聯絡資訊及其他帳號安全設定。

Meta 官方及數位產業署均將雙重驗證列為帳號取回後的重要安全措施。

(七)涉及詐騙或財產損失時另行處理

如果帳號遭盜期間，已被用來向親友借錢、要求轉帳、購買點數，或本人已提供信用卡、網路銀行等資料，處理範圍就不只是帳號復原。

應儘速：

通知親友帳號曾遭盜用。

保留對話、匯款、登入通知等相關紀錄。

聯絡銀行或相關金融機構。

透過警方或 165 全民防騙網諮詢、查證及報案。

八、重點釐清

✧ 「收到登入通知，就是帳號已經被盜」？

不一定。

例如 LINE 官方指出，若帳號仍可正常使用，可能是第三者正在嘗試登入，也可能有其他操作因素；但只要確認不是本人操作，就應立即更換密碼並檢查登入裝置。

✧ 「帳號被盜後，只要改密碼就安全了」？

不一定。

例如 LINE 帳號若已與第三方服務連動，即使變更密碼，部分服務仍可能維持登入狀態，因此還需要解除應用程式連動及登出相關服務。

✧ 「朋友傳來的連結就可以放心點」？

不能只依傳送者判斷。

朋友的帳號本身也可能已遭盜用。LINE 已有假冒朋友要求投票，再利用釣魚網站竊取下一名使用者帳號資料的實際案例。

若訊息內容與平常互動方式不同，最好利用其他方式向本人確認。

✧ 「只要不把密碼告訴別人就不會被盜」？

帳號防護不只有密碼。

認證碼、釣魚網站、第三方應用程式、陌生登入裝置、弱密碼及重複密碼，都可能影響帳號安全。因此應搭配雙重驗證、定期檢視登入活動及帳號安全設定等措施。

九、結語

LINE、Facebook、Instagram、Threads 等通訊及社群帳號已與民眾日常生活密切結合，帳號遭盜後所影響的不只是單一社群帳號，也可能延伸至個人資料、親友聯繫、其他網路服務及財產安全。帳號安全可以掌握五個階段：

第一，瞭解帳號為什麼會被盜。

對假投票、假客服、假停權通知、釣魚網站及索取認證碼等手法保持警覺。

第二，事前建立安全防護。

使用安全且不重複的密碼、啟用雙重驗證，並定期檢查登入紀錄與帳號安全設定。

第三，看到異常立即處理。

若收到非本人操作的登入通知或認證碼，應立即變更密碼並檢查登入裝置，而不是等到完全無法登入才處理。

第四，帳號被盜後使用官方管道救援。

LINE、Facebook、Instagram 等平台均有自己的帳號復原方式，不應相信網路上自稱可協助「找回帳號」的不明人士或服務。

第五，帳號取回後仍須再次清查。

檢查密碼、登入裝置、電子郵件、電話、第三方授權、貼文及私訊，並通知可能受到影響的親友。

透過「事前預防、及早發現、正確應變、官方復原及事後清查」的完整流程，可降低通訊及社群帳號遭盜用的可能性，也能在事件發生後減少後續損害。

十、官方參考資料

- LINE 支援中心 | 如何防止 LINE 帳號被盜用
<https://help.line.me/line/?contentId=20000293&lang=zh-Hant>
- LINE 支援中心 | LINE 帳號遭到盜用或可能遭到盜用
<https://help.line.me/line/?contentId=20000437&lang=zh-Hant>
- LINE 支援中心 | 防止 LINE 帳號被非法登入及處理方法
<https://help.line.me/line/?contentId=20000438&lang=zh-Hant>
- Meta Safety Center | 保護帳號安全
<https://www.meta.com/zh-tw/safety/topics/safety-basics/tools/security/>
- Meta Safety Center | 詐騙防治
<https://www.meta.com/zh-tw/safety/topics/safety-basics/tools/scams/>
- Facebook Help Center | Recover a Hacked Account
<https://www.facebook.com/help/1216349518398524/>
- Meta | Meta Account
<https://about.fb.com/news/2026/04/meta-account/>
- 數位發展部資通安全署 | 強化帳密安全，落實三大防護原則
<https://web.moda.gov.tw/ACS/press/news/press/18660>
- 數位發展部數位產業署 | Facebook 帳號被盜怎麼辦？
<https://moda.gov.tw/ADI/antifraud/af-toolbox/15736>
- 內政部警政署 | 165 全民防騙網
<https://165.npa.gov.tw/#/>
- LINE 支援中心 | 防止 LINE 帳號被非法登入（盜用）及處理方法
<https://help.line.me/line/?contentId=20000438&lang=zh-Hant>
- LINE 支援中心 | 如何確認自己在哪些裝置上登入 LINE 或 LINE 相關服務：
<https://help.line.me/line/?contentId=20008468&lang=zh-Hant>
- Meta Safety Center | Secure your account :
<https://www.meta.com/safety/topics/safety-basics/tools/security/>
- Facebook Help Center | About Facebook Page access :
<https://www.facebook.com/help/289207354498410/>
- Facebook Help Center | Two-factor authentication :
<https://www.facebook.com/help/909243165853369>
- Instagram Help Center | Two-factor authentication :
<https://help.instagram.com/566810106808145>
- LINE Official Account Help Center | Adding/changing administrators :
https://help.line.me/official_account_tw/web/pc?lang=zh-Hant
- 內政部警政署 165 全民防騙網 | 檢舉 Facebook 詐騙廣告（佐證截圖／記得截圖事證）：
<https://165.npa.gov.tw/assets/doc/Facebook.pdf>
- 數位發展部資通安全署 | 各機關資通安全事件通報及應變處理作業程序（跡證保存）：

<https://law.moda.gov.tw/LawContent.aspx?id=FL095461&media=print>

- 數位發展部資通安全署 | 中小企業基本資安防護指引 三大面向 16 項檢核協助產業防駭

<https://web.moda.gov.tw/ACS/press/news/press/19496>

- Instagram Help Center | Lost access to email address or phone number linked to Instagram account

<https://www.facebook.com/help/instagram/358911864194456>