

認明公司官方網域，慎防假冒高層之電子郵件詐騙！



近期發現有不法分子假冒公司主管或合作單位負責人名稱，使用 Gmail 等免費信箱寄發惡意郵件，企圖引導收件人「建立 LINE 群組」、「提供 QR Code」或「變更匯款帳號」。

如果收到銀行信件，請勿點擊信中連結，務必自行輸入網址或透過官方 App 核對。
收到任何要求「金流變更」、「加群組」、「提供個資」的信件時，執行以下檢查

廣華管理・廣鴻企管・萬智環球 稅務通訊 | 2026 年 03 月號

服務客戶 × 聯繫夥伴 × 積極應變全球變局

【資安重要公告】認明公司官方網域，慎防假冒高層之電子郵件詐騙！

致 各位先進與尊榮客戶：

近期發現有不法分子假冒公司主管或合作單位負責人名稱，使用 Gmail 等免費信箱寄發惡意郵件，企圖引導收件人「建立 LINE 群組」、「提供 QR Code」或「變更匯款帳號」。

本公司在提醒：

1. 絕不私下拉群：本公司及主管絕不會透過電子郵件要求您建立私下 LINE 群組來交辦公務，一般都由顧問主導服務。
2. 唯一官方網域：本公司所有官方商務溝通，一律使用官方電子郵件網域@allway-obu.com(公司的網域)。建立一個鐵律：「認網域，不認名字」。

案例一：假冒高層/合作單位要求「拉群組」

- 詐騙手法：顯示名稱顯示為公司高層（如：蘇 X 瑋），內容要求建立 LINE 群組、提交 QR Code 或安排工作。
 - 破綻：
 - 詐騙電郵：蘇 X 瑋 winchesterluiz373@gmail.com
 - 官方電郵：蘇 X 瑋 <kevinsu@allway-obu.com>（須帶有公司專屬網域）
- 免費信箱（Gmail、Yahoo、Outlook）人人都能註冊，名字想改什麼就改什麼。
本公司絕對不會使用免費信箱交辦公務或要求同仁/客戶私下拉 LINE 群組。

案例二：極度逼真的「銀行/支付通知」偽裝（變體字、相似字）

詐騙集團最常利用極其相似的字母（網域欺騙）來冒充銀行或大型機構：

● 詐騙電郵：service@ct-bcbank.com 或 notify@cathay-bk.com (多一橫或錯一字母)

● 真正銀行：service@ctbcbank.com、service@cathaybk.com.tw，銀行網域必相同

如果收到銀行信件，請勿點擊信中連結，務必自行輸入網址或透過官方 App 核對。

收到任何要求「金流變更」、「加群組」、「提供個資」的信件時，執行以下檢查：

檢查項目	● 詐騙郵件特徵	● 本公司官方標準
寄件人地址	顯示名稱是熟人，但點開看電郵是之前沒有連絡過的 xxxx373@gmail.com	官方專有網域 xxxx@allway-obu.com
通訊要求	要求掃描 QR Code、加入私密 LINE 群組、告知密碼	公務溝通皆有正式官方管道，絕不私下索取權限

客戶與夥伴：若收到疑似冒名本公司的信件，請立即撥打本公司各區電話或聯繫您原本的固定窗口對核，切勿直接回信。

企業必看！5 大超擬真郵件詐騙

1 假冒老闆叫你「私下拉群」

- 把頭貼和名字改成公司老闆（如：蘇 XX），寫信跟新人說：「我現在在開會，你先去建一個 LINE 群組，把 QR Code 寄給我，等一下有工作交辦。」
- 一秒看穿破綻：名字雖然對，但點開看他的滑鼠 E-mail 其實是 xxxx373@gmail.com（免費信箱）。公司老闆怎麼可能不用公司專屬信箱？只要看到信件上有黃色 [External 外部郵件] 標籤，卻自稱是內部主管的，通通都是詐騙！

2 假冒合作夥伴「變更匯款帳號」

- 用一個跟原本廠商極度相似的信箱（例如把 google.com 改成 g00gle.com，英文字母 o 變成數字 0），寫信給財務說：「我們公司換銀行了，這次的貨款請匯到新戶頭。」
- 破綻：信箱網域多了一個槓、少了一個字母，或者根本是亂碼。
- 只要遇到「要換匯款帳號」的，請先對回原本合作窗口的官方電話，絕對不能只看 Email 就把錢匯出去！

3 假冒應徵者或寄發帳單「誘騙點連結/附件」

- 寄信給 HR 說「這是我的履歷.rar」，或者寄給採購說「這是您上個月過期的催繳帳單.exe」。同仁一按，電腦立刻中毒藍屏，接著全公司的檔案都被鎖死，被勒索幾百萬贖金。
- 破綻：莫名其妙的壓縮檔（.zip /.rar）或執行檔（.exe），催促「趕快點開確認」。
- 不認識的信、沒合作過的廠商，千萬別手癢去點裡面的連結和下載附件！

4 假冒公司系統通知「密碼過期要修改」

- 寄信假冒是公司人資系統或 IT 網管，寫著：「您的出缺勤系統密碼已過期，請在 24 小時內點擊下方連結修改，否則會影響發薪！」你點進去一個長得一模一樣的假登入畫面，輸入了帳號密碼，密碼就這樣被偷走了。
- 破綻：那個修改密碼的網址，根本不是你們公司的內部官方網址。
- 公司要改密碼，一律自己打開瀏覽器去登入系統，絕對不要點信件按鈕去輸入密碼！

5 假冒知名銀行寄發「帳戶安全異常通知」

- 這連一般大眾都會騙！寄一封長得跟銀行一模一樣的信，寫著「您的網路銀行有異常登入，請點此立刻驗證解除限制」。點進去輸入網銀帳密後，公司或私人的存款立刻被轉光。
- 破綻：寄件者的電郵地址根本不是銀行的官方網域（真的網域是 ctbcbank.com，假的是 ct-bcbank.com）。
- 收到銀行的緊急通知，請直接打開官方 App 查看，或是撥打信用卡背面的客服電話，千萬不要從信件連結登入網銀。