資訊安全宣導_11405

小心來自「no-reply@google.com」的 email，它現在可能是駭客網路釣魚

114 年 05 月 07 日

中國信託證券股份有限公司

本文件係屬中國信託證券股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

文件制／修訂記錄

版次	日期	說明	作者	修訂中	定稿
1.0	114.05.07	初稿	何彥甫		V

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

【目　　錄】

壹、 簡述 4
貳、 看似 Google 的安全警示，其實是駭客自導自演!.. 5
參、 釣魚登入頁面建於 Google 平台，更具可信度！ 6
肆、 不是只有 Google!同樣手法也出現在 PayPal!..... 7
伍、 個人電腦使用其他注意事項 8
一、 參考附錄：.....8
二、 社交工程演練相關懲處建議： 11
陸、 參考資料..... 13

【圖 目 錄】

圖 1　Google 信箱示意圖 4
圖 2　偽冒信件示意圖 5
圖 3　假 Google 登入網站 6
圖 4　收信者被簡化成 me.....6

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

壹、簡述

釣魚手法不斷翻新，研究人員揭露，駭客正透過一種精心設計的手法，利用 Google 自家通知系統與網域服務，發送看似來自 no-reply@google.com 的詐騙郵件，目的在騙取使用者的帳號密碼。

這波攻擊被稱為「DKIM 重送釣魚攻擊（DKIM replay phishing attack）」，特別具有混淆性，因為郵件通過 Google 的驗證機制 DKIM，讓收件者誤以為寄件者是 Google，但實際上是駭客。

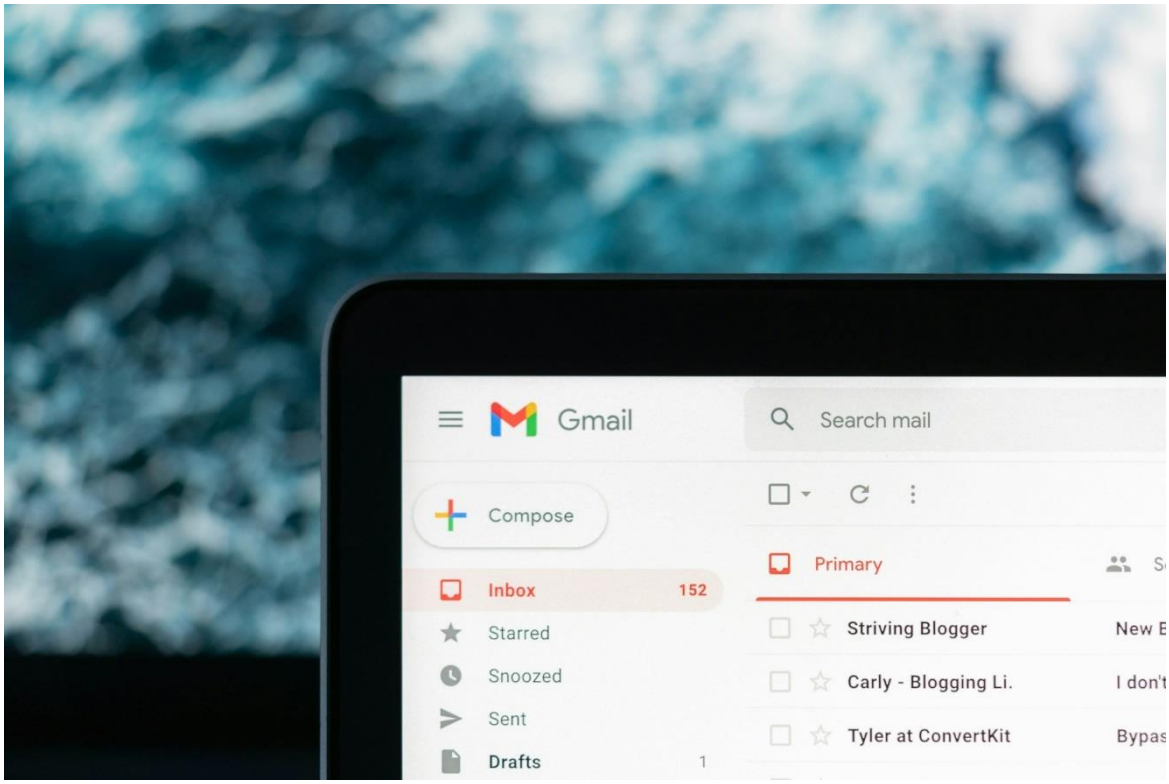

圖1　Google 信箱示意圖

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

貳、看似 Google 的安全警示，其實是駭客自導自演!

據報導，研究人員收到一封看似來自 Google 的郵件，聲稱他的帳戶內容遭到執法單位要求調查。信件使用 Google 官方地址 no-reply@google.com 發送，並夾在其他 Google 安全警示通知之中，真假難辨。

研究人員進一步調查發現，該郵件的實際寄件人並非 Google，而是駭客成立了一個應用程式存取 Google 電子郵件地址的權限，這時 Google 會自動向該郵件發送的安全警報，而駭客再加以轉寄。具體做法是，駭客透過在應用程式的名稱欄位填入整段釣魚訊息，並加入大量空白字元，將 Google 真正的安全警報內容擠壓到畫面最下方。

當這個應用獲得存取權限後，Google 便會寄出一封自動通知信給該信箱，而該信的標題與內容如前述，幾乎完全由駭客控制。接著，駭客將這封看似由 Google 發送、並已通過驗證的郵件轉寄給受害者，成功繞過傳統垃圾郵件過濾機制。研究人員表示，「由於 Google 產生了該電子郵件，因此它是使用有效的金鑰簽署並通過所有檢查的。」

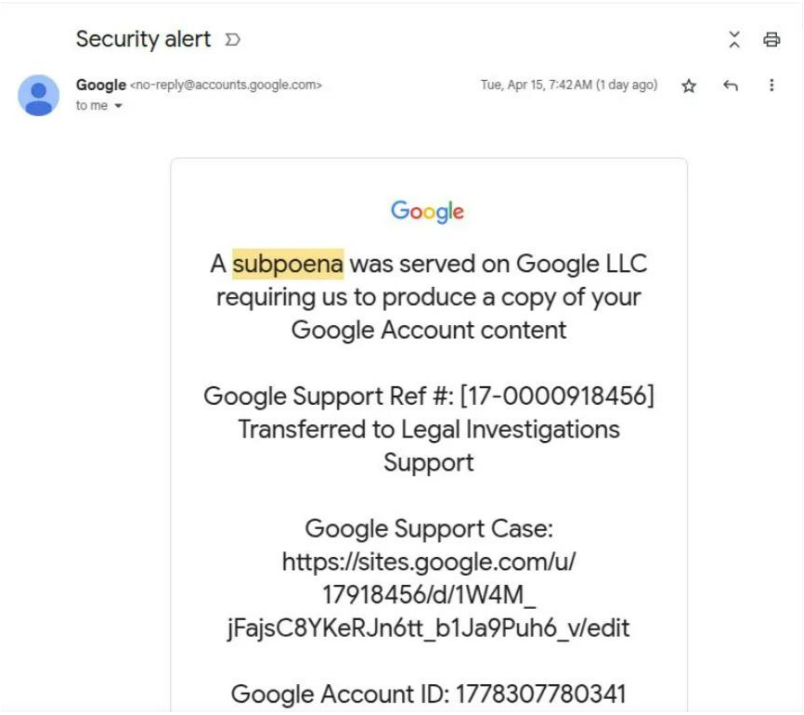

圖 2　偽冒信件示意圖

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

參、釣魚登入頁面建於 Google 平台，更具可信度！

該平台為 Google 提供的免費網頁建置平台，而非一般可疑網址。研究人員指出，這個「假入口」幾乎完整複製 Google 登入頁面，唯一破綻就是它的網域並非 accounts.google.com。這幾乎對非技術使用者來說無法辨識，但並不能否認網域仍是一個重要辨識點。

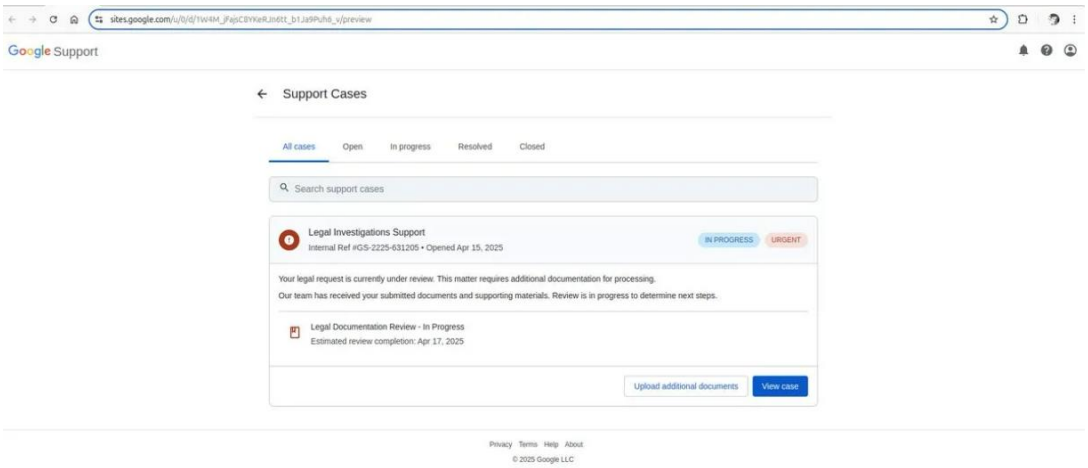

圖 3　假 Google 登入網站

此外，駭客設計一個 email 帳號叫做 me@某個網域，而 Gmail 在顯示郵件時，會把收件人簡化為「me」，這會讓收件者誤以為這封信就是寄給「自己」的，增加誤判機率。

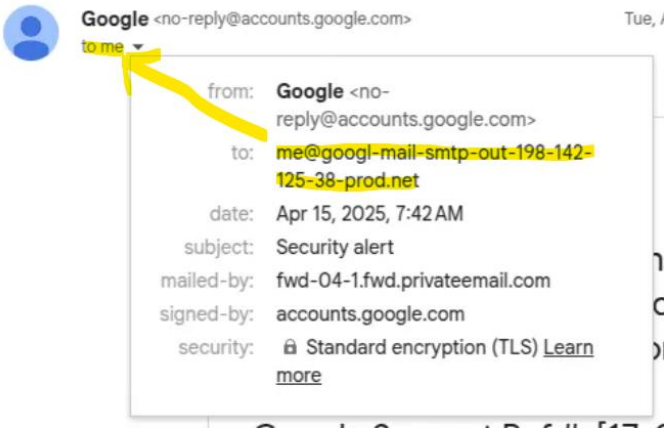

圖 4　收信者被簡化成 me

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

肆、 不是只有 Google!同樣手法也出現在 PayPal!

這套攻擊手法不僅限於 Google。根據資安網站追蹤，今年有釣魚集團針對 PayPal 用戶發動類似攻擊。駭客在新增 PayPal 帳號時，將釣魚訊息寫入帳號名稱欄位，再利用 PayPal 的「禮物地址」選項綁定該帳號，觸發由 PayPal 發出的確認信。

這封確認信經簽章驗證，與 PayPal 官方信件無異，駭客再將該信轉寄至公開郵件清單或目標名單，以誘騙受害者登入仿冒網站，輸入帳號密碼。

研究人員已向 Google 提出錯誤報告，Google 回應已著手處理權限機制的防護問題，但不能保證這類型的攻擊手法不會出現在其他平台上，使用者在收到信件時仍要保持警惕。

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

伍、 個人電腦使用其他注意事項

一、 參考附錄：

1. 個人密碼屬機密資料，由個人所有並需加以保護，密碼長度必須為 8 碼以上並且英文及數字混合，不可明碼儲存、記錄於書面、張貼於電腦螢幕、鍵盤、隔版、桌面...等可視區域；不得共用且不可公開，個人電腦之登入密碼必須定期變更。(CTSWI0027 個人電腦與周邊設備管理規範)、(CTSWI0025 行動資訊設備管理辦法)

2. 為防止他人窺視、不當使用或竄改資料，應設定電腦於五分內啟動內建之螢幕保護程式並設定密碼保護；離開使用中之電腦時，應先啟動內建之螢幕保護程式鎖定螢幕，並視情況結束連線登出(LOGOFF)。(CTSPY0005 資訊安全政策)

3. 考量各營業單位隨時輸單之需求，有關 Key-In 及營業員之個人電腦將不執行螢幕保護程式之設定，但仍需於離開座位時手動執行鎖定電腦功能(請同時按[Ctrl]鍵 ＋[Alt]鍵 ＋[Delete]鍵後，點選[鎖定電腦]之功能)，以確保資訊資源之安全。(CTSPY0005 資訊安全政策)

4. 電腦軟體之安裝與使用悉依本公司軟體採購(使用)標準，詳細軟體安裝清單請參閱(CTSFR0071 個人電腦標準安裝軟體清單)。新軟體之使用須經資訊單位評估無虞並納入採購(使用)標準後方可採購(使用)。(CTSWI0027 個人電腦與周邊設備管理規範)

5. 使用類似網路磁碟功能分享資料時，請符合下列事項。(CTSWI0027)個人電腦與周邊設備管理規範)

6. 非業務執行需求，避免設定資源分享。

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

7. 不應將整顆硬碟（C槽或D槽）設定為資源分享，以避免電腦系統及資料檔案遭到不可預期之複製及破壞。

8. 設置資源分享之資料夾，均應設置密碼及設定存取權限，並於使用後立即關閉分享。

9. 於本公司使用行動資訊設備(僅限各部門申請之筆記型電腦等設備，非公司採購之設備嚴禁攜帶至公司使用)，使用人均需填寫 OA 系統之[(CTSFR0070)資訊設備 IP 位址暨行動資訊設備申請單]，經需求單位主管簽核後，向資訊部權責單位提出需求申請。(CTSWI0025 行動資訊設備管理辦法)

10. 使用行動通訊設備必須設定硬碟密碼鎖，無此功能之行動資訊設備則不需設定。(CTSWI0025 行動資訊設備管理辦法)

11. 行動資訊設備若為該單位公用電腦，使用人員必須於歸還前清除個人資料以確保該行動資訊設備之資訊安全。(CTSWI0025 行動資訊設備管理辦法)

12. 未經資訊單位核准，具備連接本公司網路或存取本公司資訊資源能力之資訊設備，在本公司辦公處所使用時，不得再同時連接無線網路(WiFi)、行動網路與撥接網路(Dial-Up)串連公司以外網路。(CTSWI0027 個人電腦與周邊設備管理規範)

13. 敏感資料（如客戶資料）不應儲存於個人電腦。如因執行業需要暫存，於作業完成後應立即移除，如必須留存時，建議使用壓縮軟體來加密封存該敏感資料。((CTSWI0027)個人電腦與周邊設備管理規範）

14. 使用行動通訊設備必須設定硬碟密碼鎖，無此功能之行動資訊設備則不需設定。(CTSWI0025 行動資訊設備管理辦法)

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

15. 行動資訊設備若為該單位公用電腦，使用人員必須於歸還前清除個人資料以確保該行動資訊設備之資訊安全。(CTSWI0025 行動資訊設備管理辦法)

16. 未經資訊單位核准，具備連接本公司網路或存取本公司資訊資源能力之資訊設備，在本公司辦公處所使用時，不得再同時連接無線網路(WiFi)、行動網路與撥接網路(Dial-Up)串連公司以外網路。(CTSWI0027 個人電腦與周邊設備管理規範)

17. 敏感資料（如客戶資料）不應儲存於個人電腦。如因執行業務需要暫存，於作業完成後應立即移除，如必須留存時，建議使用壓縮軟體來加密封存該敏感資料。((CTSWI0027)個人電腦與周邊設備管理規範）

18. 資料檔案列印時應確認輸出的印表機裝置是否正確，確認無誤後再行列印，取回列印文件或報表時如有發現其他列印資料時，應協助確認該列印資料為何人列印並通知取回，如確認後仍無人認領應協助銷毀該列印資料。

19. 使用電子郵件傳送機敏資料時，需對機密性及敏感性資料加密後再傳送。

20. 避免使用公司電子郵件住址註冊各種網站之會員，以防止收取垃圾郵件及詐騙信件。

21. 嚴禁透過網咖、學校...等公共場所之網路環境使用遠程簽到，以避免遠程簽到登入帳號與密碼遭留存而致他人利用。(CTSWI0039)遠程簽到管理規範

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

表1　各地區電腦聯絡人員

單　位	電腦連絡人員	電子信箱	駐點分機
總　公　司	白凱仁	ricco.pai@ctbcsec.com	2385
	鄭致明	roy.cheng@ctbcsec.com	2383
三重分公司	陳威羽	harvey.chen@ctbcsec.com	199
忠孝分公司	陳威羽	harvey.chen@ctbcsec.com	199
永康分公司	李永宏	luhpro@ctbcsec.com	199
文心分公司	李奇峰	clay.le@ctbcsec.com	199
新竹分公司	鄧和榮	helong.den@ctbcsec.com	199
松江分公司	陳威羽	harvey.chen@ctbcsec.com	199
嘉義分公司	李奇峰	clay.le@ctbcsec.com	199
中壢分公司	鄧和榮	helong.den@ctbcsec.com	199
高雄分公司	鄭宗武	jan@ctbcsec.com	199
資　訊　部	張志鴻	cch@ctbcsec.com	2380
資訊安全小組	吳　洲	chou.wu@ctbcsec.com	2390

二、 社交工程演練相關懲處建議：

期間	觸發條件	對應措施及建議懲處方式
一年 (12 個月/次) 區間： Q4 ~ Q3	未開啟任一封郵件者，視為相對安全人員	無須對應
	僅開啟郵件，而未開啟郵件內連結或附件者，視為低風險人員	無須對應
	累計開啟任一封郵件內連結或附件者，視為中風險人員	1. email 通知該員及部門主管、資訊安全長、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

	累計開啟任兩封郵件內連結或附件者，視為高風險人員	1. email 通知該員及部門主管、資訊安全長、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數 3. 記警告乙次 4. 重新執行資安教育訓練
	累計開啟任三封郵件以上，且皆有開啟郵件內連結或附件者，視為極高風險人員	1. email 通知該員及部門主管、資訊部主管、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數 3. 記警告(含)以上乙次 4. 直屬主管陪同重新執行資安教育訓練

特此提醒同仁收到不尋常的 email 信件，務必提高警覺並依以下建議因應：

1. 同仁可檢視 email 主旨欄，若被標示【外部郵件】，則該 email 係來自外部，而非內部寄件者，請謹慎確認後再開啟。
2. 同仁可檢視 email 主旨欄，若標示【中信銀行郵件】，則該 email 寄件者係來自中信銀行，依此類推。
3. 同仁可檢視 email 主旨是否與工作業務相關，如若與公務無關應直接刪除，勿任意開啟。

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人

陸、參考資料

https://buzzorange.com/techorange/2025/04/22/phishing-emails-from-no-reply-google-com/

本文件係屬中國信託證券股份股份有限公司所有，非經同意不得將全部或部分內容揭露於第三人