資訊安全宣導_11407

釣魚/詐騙信件手法解析

114 年 07 月 02 日

中國信託證券股份有限公司

文件制／修訂記錄

版次	日期	說明	作者	修訂中	定稿
1.0	114.07.02	初稿	何彥甫		V

【目　　錄】

壹、 簡述 4

貳、 釣魚/詐騙信件手法分析 5

參、 實際案例解析釣魚/詐騙信件判斷要點 6

肆、 實際案例解析 ..... 錯誤! 尚未定義書籤。

伍、 個人電腦使用其他注意事項 9

一、 參考附錄：.....9

二、 社交工程演練相關懲處建議： 12

陸、 參考資料 14

【圖 目 錄】

圖 1　釣魚信件示圖.....4

圖 2　常見詐騙手法示意圖.....8

壹、 簡述

釣魚信件是一種常見的網路詐騙手法，攻擊者會偽裝成受信任的單位，例如銀行、公司或政府機關，透過電子郵件、訊息或其他通訊方式誘使你提供個人資訊或點擊惡意連結。

這些郵件通常設計得很逼真，可能會使用正式的標誌、語氣，甚至引用你的姓名，讓你誤以為是真的。他們可能會聲稱你的**帳戶有異常活動**，要求你立即驗證資料，或者提供看似**誘人的優惠**，吸引你點擊連結。但實際點進去後，你會被帶到偽造的網站，輸入帳號密碼，個人資訊就會外流，更糟糕的是你的電腦會神不知鬼不覺的落入詐騙者的手裡，成為詐騙者手中的武器。

但是，只要把握住幾個原則，多加留意，就不會輕易上當導致個人資訊的外流，甚至電腦被駭入。

以下分別整理釣魚/詐騙信件常見的手法及判斷要點，並提出案例，以一目了然的方式搭配判斷步驟。

圖1 釣魚信件示意圖

貳、 釣魚/詐騙信件手法分析

1.「目的」

- 騙取信箱帳號&密碼以寄發更多廣告/詐騙信件。
- 取得個人資訊以進一步進行金錢詐騙，例如中獎通知、投資獲利機會等。
- 利用**惡意程式達到控制電腦的目的**。

2.「內容類型」

(一)『針對性』的詐騙信件

- 偽造成付款通知、帳號/信箱停用、驗證確認等信件，假造信件會附上該服務 logo，以騙取信任，例如中信證券、Google 等 logo
- 詐騙信中提供的網址連結，也會導向 URL 類似或網頁仿真的網頁

(二)『亂槍打鳥型』的詐騙信件

- 利用好康資訊誘使收信者點選連結或開啟附件，例如中獎通知或投資獲利機會
- 各種通知信件，例如快遞、送貨、銀行通知等，通常會騙取開啟信件附件

3.「手法型態」

- 點選詐騙信件中的網址連結連到網頁後輸入帳號密碼
- 點選詐騙信件中的網址連結連到內藏惡意程式的網頁
- 透過附件內容騙取使用者回覆個人資訊，例如繳費通知
- 利用帶有**恐嚇**、**急迫性質**的信件內容，**造成收信者驚慌、失去判斷能力**，並予以勒索匯款

參、 實際案例解析釣魚/詐騙信件判斷要點

TIP1. 誰寄的?

別相信呈現的「寄件者名稱」及「email 地址」

- 釣魚信件常用的技巧就是假造電子郵件的顯示名稱，甚至 email 地址都可以假造

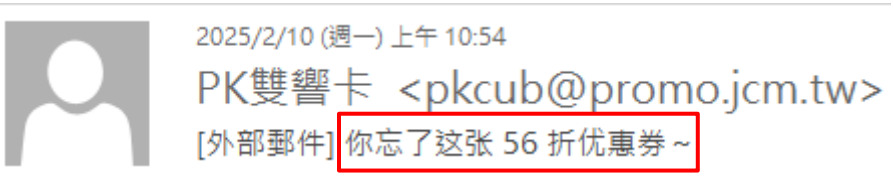
【技巧】將滑鼠移到寄件者名字上會出現相關訊息

TIP2. 信件主旨

留意信件主旨中的緊急或威脅字眼

- 常見的釣魚/詐騙手法就是企圖激發收信者著急或恐慌的反應

【技巧】先深呼吸，穩定自己的情緒，不要讓情緒主宰行為，然後再根據其它要點判斷信件真偽



TIP3. 信件寫法

睜大眼睛看清楚信件寫法是否何規

- 假冒信件常會用混淆視聽手法，故意把網址或 email address 拼錯或**不經意流漏出駭客本身國家的語言**

【技巧】公司內部信件絕對不會使用簡體內容

TIP4. 寫給誰的?

信中的稱呼很重要！

- 信件開頭稱謂如果是很模糊的泛稱，**代表寄件者不清楚你的個人資訊!**例如：親愛/尊敬的用戶、Dear user/Sir/Madam 或是非您姓氏的稱謂等，最好提高警覺！

親愛的陳O?先生/小姐您好

感謝您的支持與愛護，您的保單號碼H228***035之保單資料明細一覽表(MULTIPLE)已隨此電子郵件寄送，請直接開啟附件，輸入您的身分證字號或居留證字號，即可檢視相關內容。

TIP5. 是誰寫的?

注意信件的署名

- 信件末尾若未提供詳細的署名或聯絡方式，很可能就是釣魚信件，**因為詐騙不希望提供您任何管道聯絡官方，也不會留下詐騙者自己的聯絡方式讓警察來抓他!**

TIP6. 網址連結是真的安全嗎?

請注意網址 URL 和來信方的關係，例如中信證券為 ctbcsec.com

- 注意網址 URL，詐騙信件經常會故意混淆或拼錯網址，例如 http://www.ctdcsec.com/、http://www.ct6csec.com/

【技巧】把滑鼠游標移到信件中的連結上，就會顯示連結的真正網址

http://newoa.ctbcsec.com/flow/fm7_mailapprove.aspx?requisitionid=ffd15023-3594-4618-a48b-a4711aff511f
按一下或點選以追蹤連結。

前往檢視網頁(或由證券新 OA 網站登入)

TIP7. 小心信件附件!

切勿點開信件附檔

- 若非認識或正在等待的信件，切勿打開任何信件的附檔
- 附檔類型是可以偽裝的，看起來是圖片，可能實際上內藏惡意程式

TIP8. 注意回信內容

千萬不要在信中提供個人資訊！

- 合法的銀行、校方、企業信件絕對不會要求在電子郵件中提供個人資訊
- 不要在信件中提供帳號和密碼！

圖2 遭釣魚示意圖

肆、 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。

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)

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

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

	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。

伍、參考資料

https://www.cc.ntu.edu.tw/mailtips/index.html