



淺談 資通安全 最弱環節

◆ 臺北中正高中資訊組長 — 李詩婷

資通安全的整體安全強度，取決於系統中最弱環節，而政府機關及企業組織中，「人」往往是最容易造成資安事件的原因。



最弱環節 最易被入侵

在「不可能的任務」電影中，阿湯哥飾演的伊森韓特（Ethan Hunt）往往會因任務需求，不得不祕密入侵高度防備的企業組織或政府機關，而作為一個正派特務，絕不會拿猛烈火力來硬碰硬，因此，小組人員就會開始進行行前戰略會議，包含研究分析建築物架構、門禁及警衛編制、內部員工組織分布等所有可能的入侵管道，以從中找出一絲一毫的入侵機會。這種原理不難明白，即是分析對方最容易侵入之弱點，以提高成功的機會。

在「不可能的任務」電影中，阿湯哥飾演的伊森韓特（Ethan Hunt），出任務前會分析目標地點之建築結構、門禁及警衛編制，以從中找出最容易侵入之弱點。這種原理不難明白，即是分析對方弱點，以提高成功侵入的機會。對比資安防護，亦取決於系統中的最弱環節，而「人」就是最易侵入的關鍵點。（Photo Credit: Paramount Pictures）

全的整體安全強度，取決於系統中最弱環節（Weakest Link）」，而「人」就是被公認為是這裡所指的最弱環節，從日益猖獗的網絡釣魚詐騙似乎也印證了此一論點，不管是臉書、LINE，或是簡訊，總是有推陳出新的新詐騙內容。

「人」是資安的最弱環節

近年重大資安事件層出不窮，政府機關及企業組織無不聞駭色變，紛紛提高了資安防護的經費與人力以對抗駭客入侵。但在資通安全領域有一句名言，「資通安

假冒銀行發送簡訊 客戶損失數百萬元

以近期的新聞事件為例，110年1月底，駭客偽冒國泰世華網銀發送釣魚簡訊，

提醒您若收到假冒本行名義或來路不明之簡訊訊息，切勿相信或點選連結，以維護您的權益

國泰世華提醒您：

本行不會主動請您登入網路銀行綁定用戶資料。

使用網頁版網路銀行，請務必再三檢查應為以下正確網址(<https://www.cathaybk.com.tw/>)，若您收到來路不明之簡訊訊息，假冒本行名義請您輸入代號密碼或個人資料，那是假的！切勿相信！如您近日已於可疑網址輸入網路銀行的用戶代號及網銀密碼，建議您儘速進行更改。如有任何疑問，請聯繫165反詐騙諮詢專線或進線本行客服專線：02-2383-1000 或 0800-818-001。

為保障App使用安全，本行將調整以下功能：

1. 交易認證碼申請（自民國110年3月19日起重新開放交易認證碼申請，申請成功後滿24小時始得於線上交易使用交易認證碼驗證）。
2. 非約定轉帳限額調整（自民國110年4月6日起本行非約定轉帳之預設交易限額調整為每筆新臺幣5萬元整，每日新臺幣10萬元整，每月新臺幣20萬元整，若您前已透過櫃檯或網銀App完成設定非約定轉帳之交易限額者，將維持您原設定之交易限額，若需要調整請親臨本行任一分行櫃檯辦理）。

造成您的不便，敬請見諒

國泰世華銀行已在官網及 APP 上宣導相關資訊，強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。（圖片來源：國泰世華官方網站 <https://www.cathaybk.com.tw/cathaybk/personal/news/announcement/2021/012801announceinfo>；<https://www.cathaybk.com.tw/cathaybk/campaign/ebanking/2021fraud>）



內容為：「您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用」，訊息下方同時附上銀行網址要求民眾登入網路銀行。許多人驚見此訊息，心急立即點進此連結網站，而不幸被竊取其用戶代號及密碼，已有多位國泰世華網銀用戶上當；帳戶內資金被盜轉出去，短短3天內就有21人被害，損失金額高達3百萬元。對此，國泰世華銀行已在官網及APP上宣導相關資訊並暫時關閉APP部分功能，並強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。

網路釣魚常見手法

通常駭客若要成功進行網路釣魚，首先必須精心偽裝連結網址，常用手法如將字母「i」改以數字「1」取代，或是字母「w」改以連續兩個「ww」取代等方式，而此次國泰世華詐騙案所使用的偽裝手法就是將真實網址「www.cathaybk.com」改為「www.cathay-bk.com」，由於網址名稱太過接近，難怪用戶難以察覺，點了連結後當然就會被導向偽裝的惡意網站。

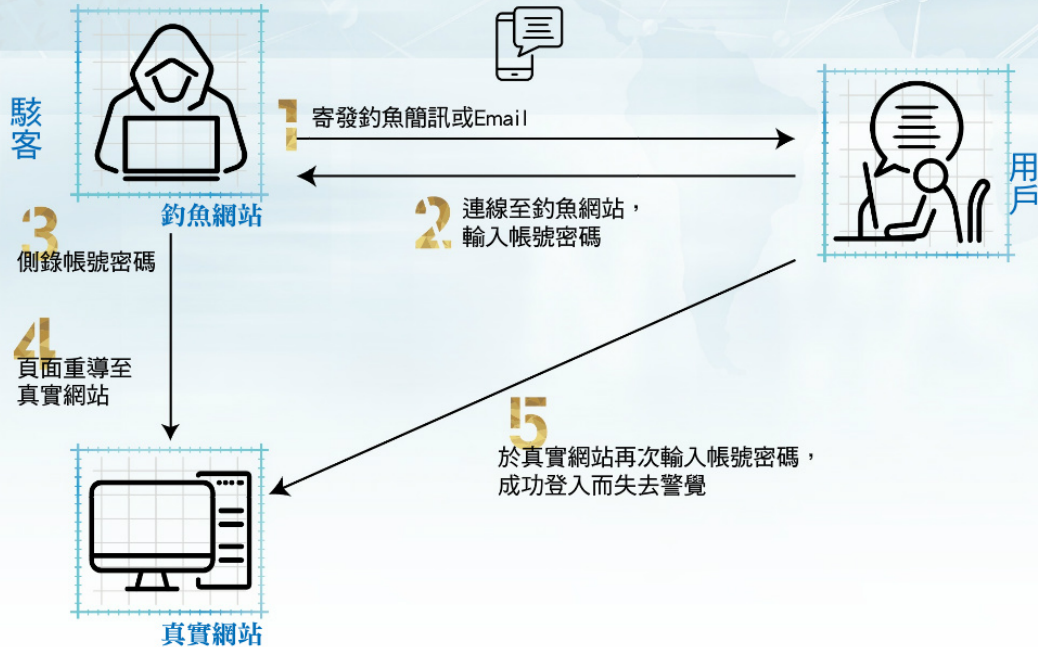


圖 1 釣魚網站非法獲取資料流程

駭客誘騙用戶點擊網址連結只是第一步，第二步則是要騙取用戶之帳號密碼，所以這時就必須利用事先架設的釣魚網站，且其網頁頁面必須跟真實網頁十分近似，包含標題、圖片及登入介面等皆需高度雷同，才能讓用戶放心點選。由於釣魚網站製作無法與真實網站完全相符，因此此時若用戶留心的話，會發現釣魚網站上的部分按鈕或連結功能可能無法點選或使用，或是輸入帳號密碼後卻沒有任何反應。更有甚者，為了不讓用戶察覺到此為釣魚網站，過往案例顯示，駭客可能在用戶輸入帳號密碼後，立即將頁面導向至真實網站的登入頁面，讓用戶誤以為是自己輸入錯誤所導致，而當用戶再次輸入帳號密碼

並成功登入真實網站後，就不會察覺到第一次所輸入的帳號密碼，其實早已被駭客盜錄下來。

防範網路釣魚之自救方式

若民眾收到任何要求登入網路銀行的通知，建議可先與銀行確認，切勿直接在簡訊上點擊連結。另為避免不小心點擊到來歷不明的網址，建議民眾可以養成記住常用銀行網址的習慣，或將銀行網址加入瀏覽器書籤，另外也可利用搜尋引擎找到正確網站，以減少被釣魚網站詐騙的風險。

一旦懷疑自己可能已經中招，除儘速確認帳戶狀態外，另外應該趕快變更密碼，

表 1 2021 農曆年前偽冒臺灣金融機關釣魚簡訊及網站情形

日期	內容	追查釣魚網站數目	受害情況
2021/1/6	釣魚郵件、釣魚網站 疑似偽冒中華郵政寄送郵件，竊取個資。	1 個	不確定
2021/1/27	釣魚簡訊、釣魚網站 【國泰世華】您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用。	6 個	據警方 2 月 6 日統計，已接獲 89 件通報，25 件被害人帳戶已遭盜用，損失金額高達 518 萬元。
2021/2/5	釣魚簡訊、釣魚網站 【台新銀行】您好，由於網路銀行版本更新，請於 2 月 6 日前登入進行驗證，否則將停用您的使用權限，超時請至臨櫃辦理。	17 個	據警方 2 月 6 日統計，已接獲 10 件通報，7 件被害人帳戶已遭盜用，損失金額高達 55 萬元。
2021/2/9	釣魚網站 疑似偽冒富邦人壽官方網站，竊取個資。	1 個	不確定
2021/2/9	釣魚簡訊、釣魚網站 【中國信託】你的網路銀行更新失敗，請立即輸入你的驗證碼以更新資料，超時請重新輸入。	11 個	據警方 2 月 9 日統計，已接獲 1 件通報，尚未有受害者報案。

資料來源：iThome，<https://www.ithome.com.tw/news/142711>。

以搶在駭客前保護好帳戶資金。另外，若自己曾在多個不同網路服務中使用同一組帳號密碼，例如網路銀行、個人信箱、社群媒體及購物網站等，也必須一併更換，以避免駭客利用所竊取到之帳密資料進行多方嘗試。

資安防護無假期 提高警覺最要緊

網路釣魚或網路詐騙，除了針對個人進行資金詐騙外，駭客在入侵機關及企業組織時，也常選擇從機關及企業組織資安防護的最弱環節下手——即人心，利用釣魚信件或簡訊等方式為攻擊發起點，對員工進行詐騙，如此可避免直接與防火牆等資安防護設備硬碰硬，提高攻擊效率。儘管

這不是
打錯我的名字挑戰
而是釣魚網站

catheydf.com catheydf.com
catheydf.com cathaydk.com
cathaydw.com catheydf.com
ctahaybk.com ctahaybk.com

提醒您春節期間
詐騙猖獗形式百百種

#多看一眼
詐騙不走眼

提高警覺守護資訊安全
www.cathaybk.com.tw

為防止釣魚訊息持續橫行，各大銀行彼此串聯，共同於今年農曆春節前在各自的臉書上張貼有趣的防詐騙文案，提醒民眾詐騙集團全年無休，要隨時防範。（資料來源：國泰世華臉書粉絲專頁，<https://zh-tw.facebook.com/cathayunitedbank/photos/a.160335250820488/1811446399042690>）

目前市面上存在惡意網址檢測及惡意郵件過濾等資安產品防護功能，但駭客釣魚手法也在進化，因此，有效培養員工的警覺心、強化資安意識及定期教育訓練，才是守護資安之最佳對策。