公務機密
資訊安全維護

資安時事案例

保險詐騙驚傳新招 臺銀人壽：千萬別加line！

收簡訊點連結 你被「釣魚」詐了

個人資料保護法

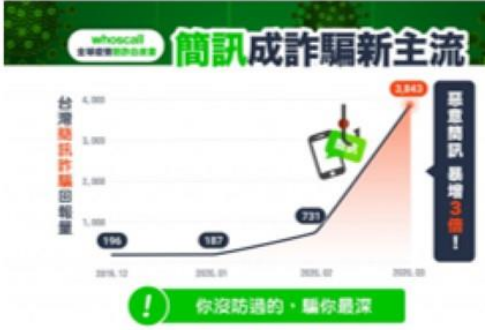
公務機關對個人資料的蒐集、處理、利用

生活中的資安

你夠在意嗎? 考驗人生的社交工程誘惑

數位學習

106年資安動畫金像獎
我要成為資安王!



保險詐騙驚傳新招
臺銀人壽：千萬別加line！

2022-02-18 旺得富理財網 傅德望

國內詐騙事件層出不窮，手法也不斷翻新，近期有保險公司傳出，詐騙集團傳送保單失效停效等簡訊給予保戶，並請保戶加 line確認，後續再進行詐騙。保險公司呼籲，保單停效、失效，或者滿期金、醫療保險金等保險金之領取，保險公司絕對不會傳送簡訊要求加line確認，看到此類訊息，民眾千萬要小心，別上當！

臺銀人壽近期接獲保戶反應收到詐騙簡訊，諸如「600萬醫療險已到達！今天24：00前不領取自動作廢，添加保險業務員確認領取。Line：976298」、又或者是「保單將於111年2月17日停效1年失效，請務必於失效日前申請復效，若有問題請洽營業員賴：a11173」等之類的訊息。

詐騙集團更高招的是，深怕民眾會立刻打電話到臺銀人壽總公司確認，於是先行攻擊臺銀人壽總機，使電話呈現佔線狀態，讓保戶打不進電話，因而誘導他們加入Line詢問。

據悉，目前臺銀人壽已向內政部警政署165 全民防騙網～165專線報案，並呼籲保戶若收到此類詐騙簡訊與詐騙Line帳號，千萬別上當。

通常保險公司在保單停效前或理賠給付需要補件，會以紙本（停效通知函）通知客戶，不會僅以簡訊通知，更不會請客戶加 line，若有疑慮一定要跟自己熟悉的業務員或理專再三確認。
國內又見詐騙新招，臺銀人壽發現自家客戶收到保單到期簡訊，還要求加Line。（臺銀人壽提供）

【臺銀人壽】再次提醒：您的52XX帳戶600萬醫療險已到達！今天24:00前不領取自動作廢，添加保險業務員確認領取.Line：976298

【臺銀人壽】再次提醒：您的52XX帳戶600萬醫療險已到達！今天24:00前不領取自動作廢，添加保險業務員確認領取.Line：976298

收簡訊點連結 你被「釣魚」詐了

記者李奕昕、柯毓庭、王長鼎／連線報導
2022年4月18日
數位時代「人手一機」，歹徒廣發手機釣魚簡訊亂槍打鳥，以假網頁誘使填寫個資後盜刷信用卡、電信小額付費或盜轉網路銀行，甚至植入惡意程式作為遊戲點數詐騙集團人頭。警方去年受理釣魚簡訊案一九五件、財損一千六百萬元均創新高。

從事科技業卅歲柯姓女子近期收到簡訊「欠缺資料，我們無法運送您的包裹」，她有網路購物習慣不疑有他，點擊簡訊中網路連結跳出快遞公司網頁，填入信用卡資料後收到銀行通知刷卡五萬多元，聯繫快遞公司才知是假網頁，驚覺遭盜刷。

不少人曾收到「包裹派送請查收」、「您在本店訂購商品已發」、「參加抽獎」、「免費電影」、「帳單未付」等簡訊，若點擊簡訊中連結，將開啟釣魚網頁要求填資料或被植入惡意程式。有手機被植入惡意程式變「殭屍手機」，轉發釣魚簡訊讓更多人受害，還賠上簡訊費。

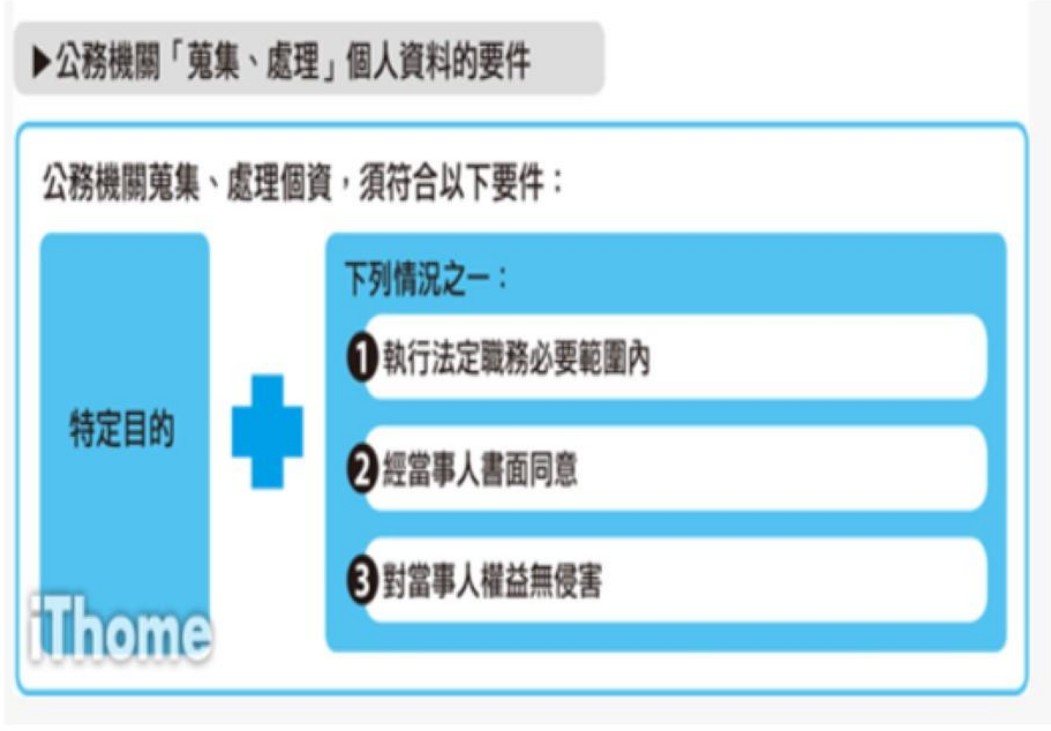
釣魚網頁是造假網頁，誘使填寫信用卡號、到期日、檢核碼後盜刷，例如最近盛行假冒DHL、FedEx等快遞公司發簡訊要求填資料盜刷；有的假網頁則要求填入電信公司傳送小額付費認證簡訊的認證碼，或直接以惡意程式竊取認證碼，再以被害人門號小額付費消費。

去年初出現「變種」手法，歹徒假冒國泰世華、台新等銀行發簡訊「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」，被害人點連結後在造假的網路銀行網頁填帳號及密碼，被盜轉存款到歹徒帳戶。刑事局去年九月破獲莊姓男子為首「假銀行」集團，清查短短四天向六十一人盜轉一千萬元。

另外，詐團需要人頭遊戲帳號存放騙來的遊戲點數，先以不知情民眾的門號上網申請遊戲帳號，遊戲公司傳送認證碼簡訊給用戶時，植入手機的惡意程式同步回傳詐團，歹徒在遊戲網頁填入認證碼完成帳號申請，後續將騙得點數存進帳號；民眾變詐團人頭，經警方以嫌疑人身分通知才驚覺遭利用。

釣魚簡訊驟增，刑事局去年初起協調各大電信公司聯防，接獲報案後提供簡訊發送門號及內容關鍵字、連結給電信公司，停用涉案門號，並阻斷其餘門號發送相同簡訊，相關案件才有減少趨勢。

公務機關對個人資料的蒐集、處理、利用



資料來源:清流雙月刊 37

◆社團法人臺灣 E 化資安分析管理協會、逢甲大學創能學院－林子煒

社交工程形形色色，若不夠留意，駭到你會怕。

社交工程—駭客最有效且省錢之攻擊方式

自從人們可以利用網際網路互通有無，每個人至少都擁有多個網路服務帳號，包括個人或其所屬單位的電子郵件帳號；正因如此，利用資訊科技便利之社交工程犯罪行為層出不窮，且趨勢逐年上升。

社交工程即為人與人之間的攻擊。過去關於此類攻擊定義為「攻擊者藉由社交手法取得系統或網路的資訊」，然而現今攻擊者的目標，已逐漸轉到個人擁有之資訊。此攻擊管道，最常見的為電子郵件、簡訊、即時通訊軟體（如 Messenger、Skype、Line、Instagram、Whats App）等

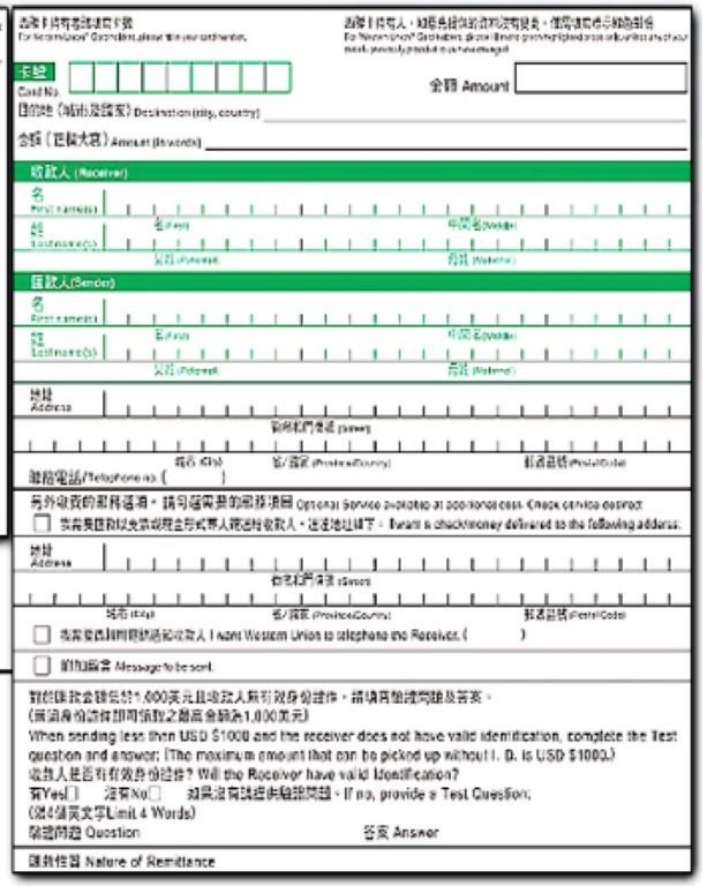
等。為何此種攻擊趨勢會逐年上升？因為對駭客而言，這是最有效、最省成本的攻擊方法。

親身經歷之詐騙案例

以自身經驗為例，某天上午收到親戚X寄來的英文信，信中述說他「正在英國旅遊，但被當地歹徒持槍威脅交出身上所有財產，包括金錢、信用卡、行動電話等。這封信是透過當地的免費網路寄出，現在急需金錢援助，請用西聯匯款（Western Union）匯2,350英鎊（約新臺幣9萬元）給我」。

信中附上姓名與地址，我抱著好奇心利用Google地圖查詢，結果發現那家英國旅館竟然地處在杳無人煙的社區。另個親戚Y也在詢問是否有收到這封信，所以我們研判親戚X的信箱帳戶應該已被盜用，而盜用者寫了這封信，並寄給信箱內所有的聯絡人。

詐騙者指定西聯匯款[1]的原因，係因其匯、收款的雙方都不用開設銀行帳戶，只要填寫雙方英文姓名與出示身分證明即可匯款。作法是在匯款人填妥表格後，系統會產生一組10位數密碼，匯款人只要將



筆者收到透過親戚X信箱寄來的詐騙電子郵件（左），聲稱遭到搶劫急需金援，要求以不用開設銀行帳戶的西聯匯款（右）轉匯。（圖片來源：作者提供）

密碼給收款人，收款人就能憑藉英文姓名及密碼進行提款。時至今日，全球已有相當多利用西聯匯款而被詐騙的案例，警方與銀行都無法追蹤及攔截詐騙款。

社交工程郵件之包含要素

以電子郵件來詐騙至少已有十年歷史，然至今仍有民眾上當，因為民眾輕忽或無知，易讓駭客達到欺騙目的。社交工程電子郵件不乏利用聳動的郵件主旨、偽造受害者熟悉的寄件者、以假亂真的郵件內容等等，試圖吸引使用者上鉤。社交工程電子郵件中會有幾個要素，包含超連結、附件、圖片、郵件內容內嵌程式碼。

- **超連結**：有可能會讓受害者連至攻擊者所架設之惡意網站，藉此收集受害者相關資訊。
- **附件**：多含惡意程式，開啟並執行後會潛藏在受害電腦裡，直接將電腦內資料對外傳輸、偷偷側錄用戶使用電腦的任何行為、接續下載惡意程式至受害電腦再執行各項行為等。
- **圖片及郵件內容內嵌程式碼**：能回報給攻擊者表示「登陸成功」，更甚者直接讓受害者電腦自動從中繼站下載小程式(諸如鍵盤側錄工具、螢幕側錄工具等)，記錄受害者使用電腦行為，再進行下一步攻擊。

以上要素不一定會同時出現，亦可能交互搭配使用，曾有僅憑單一內容即欺騙成功的案例，造成受害者損失。例如，假冒會議邀請信函，成功欺騙到受害者出門參加會議，加害者利用這段時間闖空門等。

勒索軟體通常包裹著社交工程郵件外衣

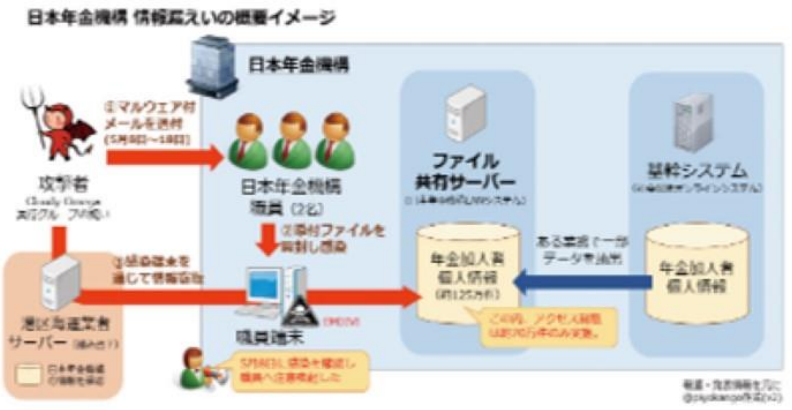
近幾年造成全球重大災情的勒索軟體，大部分行為模式即透過社交工程電子郵件，讓受害者點擊後自動下載並執行一個看似無害的小程式，連線至外部中繼站下載勒索軟體主程式，此主程式會開始掃描電腦所存文件[2]後加密，跳出警告訊息，指示受害者利用比特幣付款至指定帳戶以換取解密提示。

日本年金機構之個資外洩事件

若讀者認為，就算有人「運氣這麼不好」開啟了社交工程電子郵件，造成傷害也不過是個人財產及聲譽。其實損失的嚴重性，絕非想像中的那般簡單。

掌管日本全國國民年金的組織「日本年金機構」（相當於勞動部勞工保險局國

大部分勒索軟體的行為模式，即是透過社交工程電子郵件誘惑使用者點擊，而成為受害者。



日本年金機構個資外洩事件示意圖，遭駭主因係員工不慎打開含病毒之社交工程電子郵件所致。（Photo Credit: piyokango, https://piyolog.hatenadiary.jp/entry/20150601/1433166675）

民年金組），於 2015 年 6 月召開記者會，坦誠因員工電腦受駭客攻擊，導致民眾個人資料外洩[3]；整起事件的起因，即為員工不慎打開含病毒之社交工程電子郵件所致。

剛開始是該機構九州分部員工收到社交工程電子郵件，點選超連結後，即被自動下載惡意程式，並開始不正常的電腦連線。

雖然日本國家網路安全中心（National Information Security Center, NISC）[4] 於第一時間發出通報，但因為日本年金機構檢測不出原因，因此僅更新個人電腦的防毒軟體，直到東京本部也有員工收到同樣的社交工程電子郵件並開啟，偵測到儲存年金的資料庫有異常連線行為後，才驚覺事態嚴重。日本年金機構事後雖通知警方，且 NISC 亦緊急派員處理，然已造成所屬 5 個單位內有多達 19 臺的個人電腦遭受感染，最後清查出竟然有高達 125 萬筆的個資外洩，嚴重影響到仰賴年金度日之日本民眾的生活。

社交工程之攻擊方式

由日本年金機構案例可知，只要個人一時疏忽，即使只是小小電子郵件，就有很大機會對企業、群體，甚至國家安全造成危害。

另外，即時通訊軟體也成為社交工程攻擊管道之一。在 COVID-19 疫情高峰時，國內採取口罩預購制，意外出現「口罩釣魚簡訊」，佯稱口罩到貨，引誘使用者點擊簡訊

內連結，當時亦有不少臺灣民眾受駭[5]。以下再列舉其他社交工程之攻擊種類。

一、**濫發電子訊息**：諸如惡意電子郵件、釣魚簡訊、即時通訊等文字訊息。此類攻擊通常一次廣發給多名使用者，因此亦稱為「垃圾郵件」。

二、**釣魚**：此類攻擊通常會讓使用者「信以為真」，透過話術讓人誤信，進而騙取錢財。近期常見「假交友」、「假投資」即屬此類。

三、**願者上鉤**：經典手法為攻擊者在公司門口隨意丟棄一個隨身碟，該公司不知情員工撿到後，誤以為是公司內有人不小心遺失，為了順利歸還，故而將該隨身碟插進自己的電腦內，殊不知惡意程式就此開始執行。

四、**搭順風車**：尾隨員工進入外人不該進去的區域，進而竊取到公司內部機密資訊。

五、**水坑攻擊**：利用網頁藏惡意程式碼的方式，讓使用者的電腦中毒。只要入侵或偽造目標受害者常瀏覽的網站，植入惡意程式，當受害者瀏覽該網站，即會下載惡意程式。

社交工程攻擊之防範措施

社交工程攻擊防不勝防，面對攻擊，可行的防範措施包含：

一、**使用垃圾郵件過濾器**：現行的郵件伺服器（包括 Gmail）皆有此機制。

二、**定期更新**：隨時更新防毒軟體、防火牆與電腦及手機的作業系統，以防任何安全性漏洞被利用。

三、**仔細確認**：確認訊息與自己是否相關，並查證訊息來源，有必要時打電話向來源確認。

釣魚簡訊經常引誘使用者點擊簡訊內連結，進而竊取民眾個資、詐騙錢財。（圖片來源：內政部 FB 粉絲專頁，https://www.facebook.com/moi.gov.tw/photos/a.1053616048000131/3275894322438948）

人是最大的零日漏洞，只要使用者資安意識稍有不足，即為攻擊者打開一扇自由進出的大門。

四、**提高警覺**：個人應提防不明電子郵件，並且勿任意點選附檔及超連結。

人是最大的 Zero-Day

社會生活中形形色色的誘惑，即是社交工程對於網路用戶的最佳詮釋，諸如「清不完的木馬，無知與恐懼也；補不完的系統，人腦也」、「人是最大的 Zero-Day[6]」等，雖然只是玩笑話，也道出了防範社交工程的最關鍵要素是「人」。資訊技術發展這麼多年，為何電子郵件社交工程依然是攻擊者的攻擊手段首選，乃因為電子郵件是阻力最小的攻擊路徑，只要使用者資安意識稍有不足，開啟惡意電子郵件，即為攻擊者打開一扇自由進出的大門，也開闢了一條讓使用者或其所屬組織邁向毀滅的道路。因此，在日常生活中一定會接觸到電子訊息的我們，勢必要多加瞭解是類攻擊，且必須養成習慣、提防不明電子訊息。相信你只要夠「在意」，必當能防範形形色色且誘惑人性之社交工程攻擊。

社團法人台灣 E 化資安分析管理協會（ESAM）