惡意電子郵件社交工程防護暨資訊安全宣導教育訓練

報告人：網路管理暨行政支援組　劉得璿

敏實科技大學
MINTH UNIVERSITY OF SCIENCE AND TECHNOLOGY

社交工程防護訓練的目的

壹、依據

一、資通安全事件通報及應變辦法第 8 條。

二、臺灣學術網路管理規範相關規定。

貳、目的

社交工程為駭客常用入侵管道，透過電子郵件夾帶惡意程式或連結網址等方式，輔以吸引人之信件主旨及內容，誘使缺乏警戒心的使用者開啟後造成進一步破壞，嚴重損害機關或個人之權益。

為依資通安全法令規定及增進臺灣學術網路安全之目的，爰持續辦理本(110)年度本部、所屬公務機關及臺灣學術網路之社交工程演練服務，並訂定本計畫，透過實施演練作業，提升教育體系人員針對社交工程攻擊之警覺性，並檢驗機關防範社交工程成效，及透過後續持續改善降低社交工程風險。

演練對象

(三)下列之臺灣學術網路連線單位（以下簡稱臺灣學術網路連線單位）

1、其他公私立大專校院。

2、區域網路中心。

3、直轄市、縣(市)教育網路中心。

二、應參與演練人員

(一)人員類型包含機關、學校之正副首長、各級主管及一般行政人員。

(二)人員範圍為機關、學校全體人員（定義為具備公務電子郵件帳號者），不限於正式公務人員身分。

敏於思．實於行

演練方式及時程

一、演練方式

每次演練作業，將針對各演練對象之受測人員寄送 10 封社交工程演練郵件，受測人員挑選方式如下：

(一)本部：各單位所有人員均列入。

(二)本部所屬公務機關、臺灣學術網路連線單位：依演練對象提交之演練人員名單，按人員類型隨機選取 100 人（公務電子郵件帳號），未滿 100 人者則全數列入，主管人員（科組長以上）原則佔受測人員總數 35%以上（特定人員類型如有不足則視情況調整）。

二、演練時程：自本（110）年 4 月至 11 月止，期間辦理 2 次演練。

› 本次受測人數為51人

敏於思．實於行

評量標準

一、演練評量項目（各次演練作業，各演練對象分別計算）

(一)惡意郵件開啟率

1、由本部統一計算，計算方式：開啟演練郵件人數 / 總受測人數

2、郵件透過預覽或點開方式開啟，且信件內文之圖片亦完成下載，始認定為誘騙成功。

(二)惡意郵件點閱率

1、由本部統一計算，計算方式：點選演練郵件內文連結網址或附檔之人數 / 總受測人數

2、受測人員點選郵件內文中之連結網址，將被記錄為遭誘騙成功。同封郵件內文如包含多個連結，受測人員不論點選幾個都將記錄為 1 次。

評量標準

3、受測人員點選郵件內文中之夾檔附件，將被記錄為遭誘騙成功。同封郵件受測人員不論點選幾次附檔，都將記錄為 1 次。

4、因將來路不明的危險信件轉寄給他人會造成更大傷害，故這類行為所導致之郵件開啟、連結點選及附檔點選，將列入轉寄者之受測紀錄。

演練目標

(一)惡意郵件開啟率：各次演練作業，各演練對象應低於10%(含)。

(二)惡意郵件點閱率：各次演練作業，各演練對象應低於6%(含)。

›開啟率不可超過5人

›點閱率不可超過3人

敏於思．實於行

演練目標

三、各次演練作業結束後，對於演練成績不良者，本部將函請演練對象擬定改善措施，相關條件及說明如下：

(一)惡意郵件開啟率或惡意郵件點閱率，未能符合本演練計畫之目標。

(二)未辦理本演練計畫相關配合事項要求且情節重大者，如逾期未提報演練人員名單。

四、本部將檢視前後兩次演練作業之績效改善情形，如演練對象連續2次演練作業成績皆屬不良者，須擬定改善計畫並回復本部備查。

敏於思．實於行

何謂社交工程

- 通過與他人的合法地交流，來使其心理受到影響，做出某些動作或者是透露一些機密資訊的方式，是一種欺詐他人以收集資訊、行騙和入侵電腦系統的行為。

社交工程攻擊的目的

- 強制廣告(不斷開啟惡意廣告)
- 控制主機 (植入木馬後門程式，如挖礦程式)
- 詐騙金錢
  - 各大銀行網站或拍賣網站
  - 勒索軟體
- 竊取帳號密碼與個人資料
  - 販賣個資
  - 偷窺隱私
  - 竊取財物

社交工程攻擊的常見手法

› 早期社交工程是使用電話或其他非網路方式來詢問個人資料，目前社交工程大都是利用電子郵件、網頁、社群網站來進行攻擊

社交工程攻擊的常見手法

› 透過電子郵件進行社交工程攻擊之常見手法

- 假冒寄件者
- 使用與業務相關或令人感興趣的郵件內容
- 含有惡意程式的附件或連結
- 利用應用程式之弱點

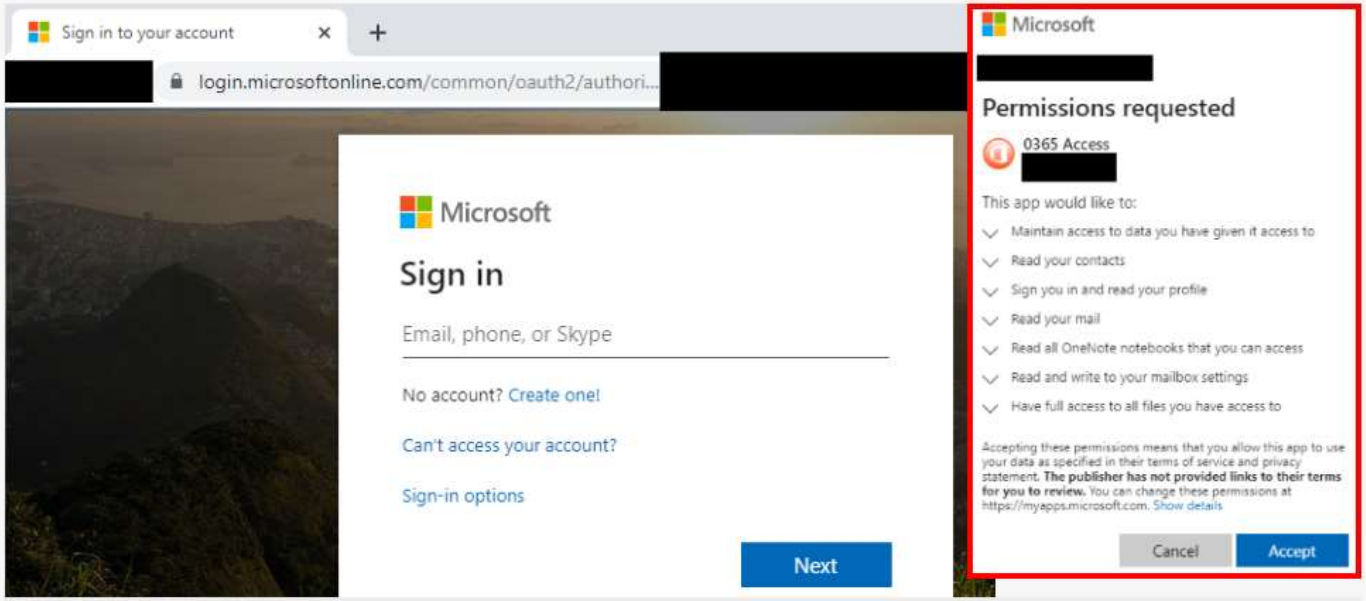
手法案例—假冒服務

首見駭客以惡意Office 365 App存取用戶帳號

駭客假造合法連結誘使受害者主動登入Office 365，並允許惡意Office 365外掛App存取其資料的手法，不需取得帳密即可登入用戶帳號，即使變更密碼或採用雙因素驗證，也無法倖免於難

文/ 林妍溱 | 2020-01-14 發表

按讚加入iThome粉絲團



受害者收到的信件內有一個Excel檔案分享連結邀請用戶前往，主機名為login.microsoftonline.com且由微軟控管。點下去後用戶如果之前沒有登入Office 365，即會出現合法的微軟登入頁面（圖左）。用戶登入後會跳出一個Office 365外掛App要求存取權的對話（圖右）框，用戶一旦按下對話框中的「接受」，該App就可以無礙存取用戶所有信件內容、OneDrive檔案等，完全無需帳號密碼。（圖片來源／PhishLabs）

敏於思．實於行

手法案例─網路釣魚

美國國土安全部網路安全及基礎架構安全署（CISA）與美國調查局（FBI）上周聯袂警告，武漢肺炎（COVID-19）疫情所造成的居家工作風潮，讓企業VPN服務日趨流行，但從今年7月起，駭客集團開始透過語音網釣（Vishing）活動，取得員工登入企業VPN的憑證。

與傳統的網釣活動一樣，駭客先架設了模仿企業網址的登入網站，可能偽裝成支援服務的入口或是員工入口，之後再利用社交網站或各種工具蒐集受害者的背景資料，從姓名、地址、電話號碼、職位或在公司的年資等，接著便透過VoIP打電話給受害者，假裝是企業的技術支援部門，宣稱要重設VPN服務，因此需要他們的憑證，要求受害者提供憑證，包括雙因素認證資訊在內 。

有些被騙的受害者直接提供了雙因素認證資訊給駭客，有時駭客也會藉由SIM卡交換攻擊取得受害者的雙因素認證資訊。駭客入侵企業網路的目的可能是為了蒐集更多的資料，以進一步執行其它的詐騙。

手法案例─實體潛入

資安業者Trustwave近日警告，人們經常聽到社交工程攻擊，手法從網釣攻擊、誘導使用者開啟惡意的連結或附加檔案，但也得留心實體的「邪惡USB」（BadUSB）攻擊，這樣的例子雖然不多，卻是實際存在的。

Trustwave最近發現的一個例子是，一個客戶收到了一個偽裝成來自Best Buy的包裹，內含提供給忠實客戶50美元的禮券，並附上一個USB隨身碟，表示當中含有可用禮券購買的商品。

然而該USB隨身碟卻是一個邪惡USB，它其實是個USB鍵盤，一旦安裝後就會自動注入惡意命令，連結遠端的C&C伺服器，回傳裝置資訊，從電腦型號、硬體資訊、作業系統資訊，到執行程序等，繼之下載其它的命令或惡意程式。

簡單地說，一旦USB的控制晶片被重新程式化以執行其它功能，它就可能被駭客用來發動攻擊，最終控制受害者電腦。

手法案例-假冒網站

正確	假冒	網站名稱
www.mitust.edu.tw	www.mitust.eud.tw	敏實科大
www.chinatrnst.com.tw	www.chinatrust.com.tw	中國信託
www.ntx.gov.tw	www.ntx.com.tw	財政部北區國稅局
tw.bid.YAHOO.com	tw.bid.YAHO0.com	雅虎拍賣
www.vvretch.cc	www.wretch.cc	無名小站
www.pchome.com.tw	www.pchorne.com.tw	PCHome
service@1andbank.com.tw	service@landbank.com.tw	土地銀行

社交工程與人工智慧

以目前來說，Deepfake是最為人熟知的AI人工智慧攻擊手法，AI已經被用於猜測密碼、破解CAPTCHA認證、複製人類語音，以及其他眾多開發當中的非法技術。趨勢科技指出，這表示，未來需要新的過濾技術，來防範假訊息攻擊與網路勒索的風險，並防範專門以AI資料為目標的攻擊。

先前趨勢科技也發布報告指出，某些商品的市場正在逐漸興起，包括Deepfake服務（被駭客用於性勒索，或用來通過某些網站要求的照片認證）、AI人工智慧遊戲機器人（用於預測骰子的點數，或用於破解Roblox的驗證碼）、存取服務（Access-as-a-Service，用於存取駭客已入侵的裝置和企業網路）等。趨勢科技表示，Fortune 500大企業的存取即服務價格可高達10,000美元之譜，某些服務還內含讀寫權限。穿戴式裝置帳號也是逐漸興起的市場，趨勢科技表示，網路犯罪集團可利用這些帳號來從事保固詐騙，要求廠商提供裝置更換。

趨勢科技認為，網路犯罪集團一直都是最新技術的率先採用者，人工智慧技術也不例外。目前AI人工智慧可能被歹徒利用的方式如，製造難辨真偽的大規模社交工程攻擊、開發文件內容辨識惡意程式，以提升攻擊效率。此外，歹徒也會利用AI技術，來躲避影像辨識以及語音生物辨識系統。

› 來源：工商時報

敏於思．實於行

社交工程信件的特徵

- 信件標題與內容都看起來是正常的信件
- 標題與內容多與日常生活、熱門時事結合
- 偽造成上級單位或資訊部門發信

去年題目

郵件	郵件種類	郵件主題	寄件者	附件
1	旅遊休閒	親子遊孩子為何擺臭臉？調查：九成小孩想參與規劃行程	張若云<eva.chang@itapei.net.tw>	親子旅遊規劃方式
2	生活消費	口罩解禁哪裡買？	ETD 民生網<etdh00d@edhealth.org.tw>	各大超商彙整
3	金融財經	台股後勢看漲 看好四大類別	自由經濟報<LTNews@yarn.com.tw>	優勢股建議清單
4	新聞時事	2020 三倍券懶人包一次看懂	消費快訊<go3000@uniprotect.org.tw>	振興券懶人包
5	新聞時事	109 年公教人員健檢辦法	全國人事服務<moe_life@yourlife.org.tw>	健檢辦法細節
6	生活消費	MIT 國產口罩怎麼辨識？哪裡有賣？	10 分生活<etdhood@yourlife.org.tw>	新版口罩防偽方式
7	旅遊休閒	桃園青埔 漫遊奇幻海洋	Kevin Chen<activity@udmnews.com.tw>	活動一覽
8	新聞時事	美豬、美牛進口恐藏三大原因	TEPNEWS<funnyflnd@yarn.com.tw>	三大原因
9	公務相關	【2020 愛你愛你】活動報名事宜	我的 E 政府<my_gov@itapei.net.tw>	活動詳細辦法
10	公務相關	林奇峰 - 志願服務申請	Charls_lin<Charls_1in@itsolution.net.tw>	志願服務申請表

敏於思．實於行

防護三部曲-停看聽

- 停—使用任何新系統前，必須先
  - 執行各種作業系統更新、應用軟體設定
    - Windows / Office Update
    - 設定瀏覽器安全性
  - 啟用個人防火牆
    - 控制台→Windows 防火牆→開啟防火牆
  - 安裝防毒軟體，並確實更新病毒碼
    https://ga.mitust.edu.tw/p/412-1003-100.php?Lang=zh-tw
  - 不要安裝來源不明的軟體

敏於思．實於行

防護三部曲-停看聽

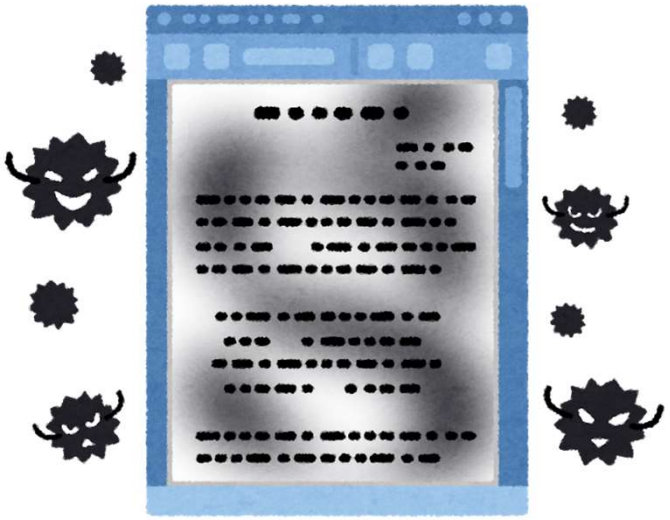
› 停—

- 不瀏覽可疑或非法網站
- 不使用電腦時，採取登出、設定螢幕保護、關機或等防護

敏於思．實於行

防護三部曲-停看聽

- 停—使用任何電子郵件軟體前，必須先
  - 設定收信軟體安全性
    - 關閉郵件預覽功能
    - 關閉自動下載圖片
    - 不要自動回覆讀信回條
    - 以純文字模式開啟郵件
  - 防止垃圾郵件
    - 設定過濾垃圾郵件機制



敏於思．實於行

防護三部曲-停看聽

- 停—使用任何電子郵件軟體前
  - 不開郵件附件和不點擊連結
  - HTML可以執行程式代碼，若程式含惡意代碼則開啟信件時就會觸發

防護三部曲-停看聽

- 看—開啟電子郵件前應先檢視
  - 寄件人
    - 不認識的寄件人，開信要再三確認
  - 郵件主旨
    - 非關公務的郵件儘量不看
  - 附加檔案
    - 這些類型的附加檔案都要小心 exe、com 、 scr、pif、bat、cmd、doc、xls、pps/ppt、reg、lnk、hta、zip、rar、swf、html、mdb
    - 名稱顯示與業務無關或檔名怪異、錯誤，請勿開啟

防護三部曲-停看聽

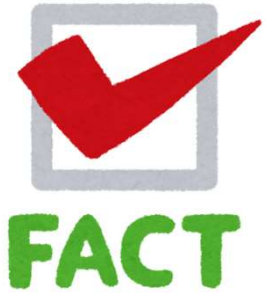
- 看—已經在使用的作業環境
  - 定期更改密碼
  - 不同系統使用不同密碼
  - 定期更新系統及軟體版本
  - 不要在業務系統執行與系統無關的活動

敏於思．實於行

防護三部曲-停看聽

- 聽—若懷疑郵件來源，必須進行確認
  - 透過電話或其他方式向寄件人確認郵件真偽
  - 不要在開啟郵件狀況下，直接按刪除鈕，應回到郵件清單(index)下刪除郵件，以免無意間直接開啟下一封郵件

使用電子郵件時應有的習慣



- 收信
  - 檢查寄件者的真偽
  - 確認信件內容的真實度
  - 不輕易開啟郵件中的超連結以及附件
  - 開啟超連結或檔案前，確認對應軟體（如IE、Office、壓縮軟體）都保持在最新的修補狀態
- 轉信或寄信
  - 未經查證之訊息，不要轉寄
  - 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址傳出
  - 寄送信件給群體收件者時，應將收件者列在密件副件，以免收件人資訊外洩。

6千萬防護資安攻擊

- 千萬不要開啟或回覆來歷不明電子郵件
- 千萬不要下載或執行來歷不明軟體或檔案
- 千萬不要洩露個人帳號密碼
- 千萬不要用非信任電腦處理公務
- 千萬不要隨意透露個人資料
- 千萬不要忘記定期作資料備份

謝謝聆聽
Q&A

插圖來源：いらすとや(https://www.irasutoya.com)

敏於思．實於行