新北市政府教育局

社交工程攻擊手法大解析

講師：葉益禎

中華民國114年3月18日

課程大綱

序號	大綱
一	社交工程攻擊基本概念
二	社交工程攻擊的手法
三	社交工程攻擊可能造成的影響
四	如何防範社交工程攻擊
五	問題與討論

社交工程攻擊基本概念

社交工程(Social Engineering)是什麼？

- ✓是以收集資訊、欺詐或入侵系統為目的的信任騙局，已發展出各種技術手段，並可能用於犯罪。
- ✓利用人性弱點，應用簡單的溝通和欺騙技倆。
- ✓利用電子郵件誘騙使用者開啟檔案、點開連結，以植入惡意程式、暗中蒐集機敏性資料。
- ✓經常會用社交工程來偽裝自己及動機，通常是冒充成可信任的對象，或以電話偽裝委外廠商維護人員或上級單位人員，乘機騙取帳號及通行碼。

重點提示

- 隨時提高警覺，未經確認不提供資料、不開啟來路不明的電子郵件及附加檔案、不登入未經確認的網站，以避免社交工程的攻擊傷害。

社交工程常見方法

佯裝資訊人員：利用電話佯裝資訊人員，騙取帳號及通行碼。

假冒委外廠商：偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。

偽造釣魚網站：利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。

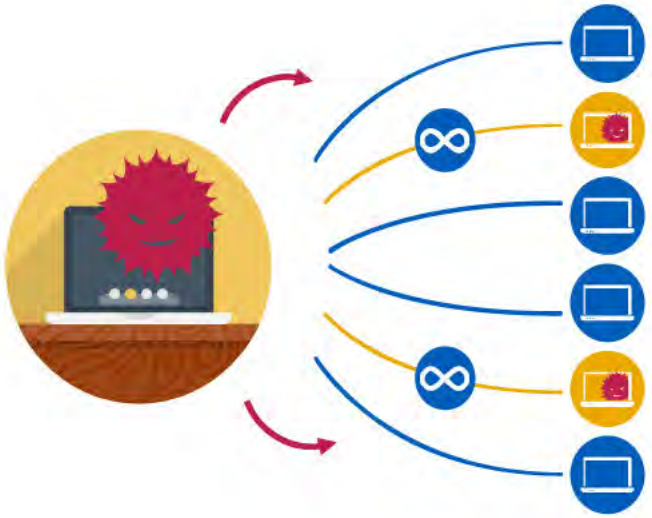
惡意程式附件：利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中蒐集機敏性資料。

冒充軟體更新：誘騙使用者下載，如偽裝的修補程式、P2P下載軟體、工具軟體等，乘機植入惡意程式。

政府機關遭社交工程攻擊手法

偽冒企業寄送社交工程郵件

惡意連結
http://www.outlook.com



惡意程式
-2021.docex.exe
檔案假冒成doc文件執行檔

步驟一

偽冒組織名義寄送社交工程郵件

步驟二

騙取同仁點擊下載惡意程式，造成電腦感染中毒

步驟三

針對連接內部網路之其他設備，擴大進行攻擊

社交工程攻擊的手法

社交工程的攻擊流程

- **Investingation：**
  做攻擊前準備、情報調查。

- **Hook：**
  接觸目標、 編造故事、 控制目標。

- **Exit：**
  清除足跡。

- **Play：**
  執行攻擊、 取出資料。

常見的六種社交工程手法

以下列出幾個注意的主要社交工程陷阱：

網路釣魚（Phishing）

最常見的社交工程類型之一。

下餌（Baiting）

利用人們的貪婪或好奇來引誘受害者。

假托技術（Pretexting）

以為無害而無意間造成資料外洩風險增大。

恐嚇軟體（Scareware）

營造出說服目標給出個人或有價值資料的情境。

魚叉式網路釣魚（Spear phishing）

針對受害者喜好，誘使上當而提供資料。

尾隨（Tailgating）

當某人打開閘門時，他們就跟隨快速地通過。

社交工程手法-1.網路釣魚（Phishing）

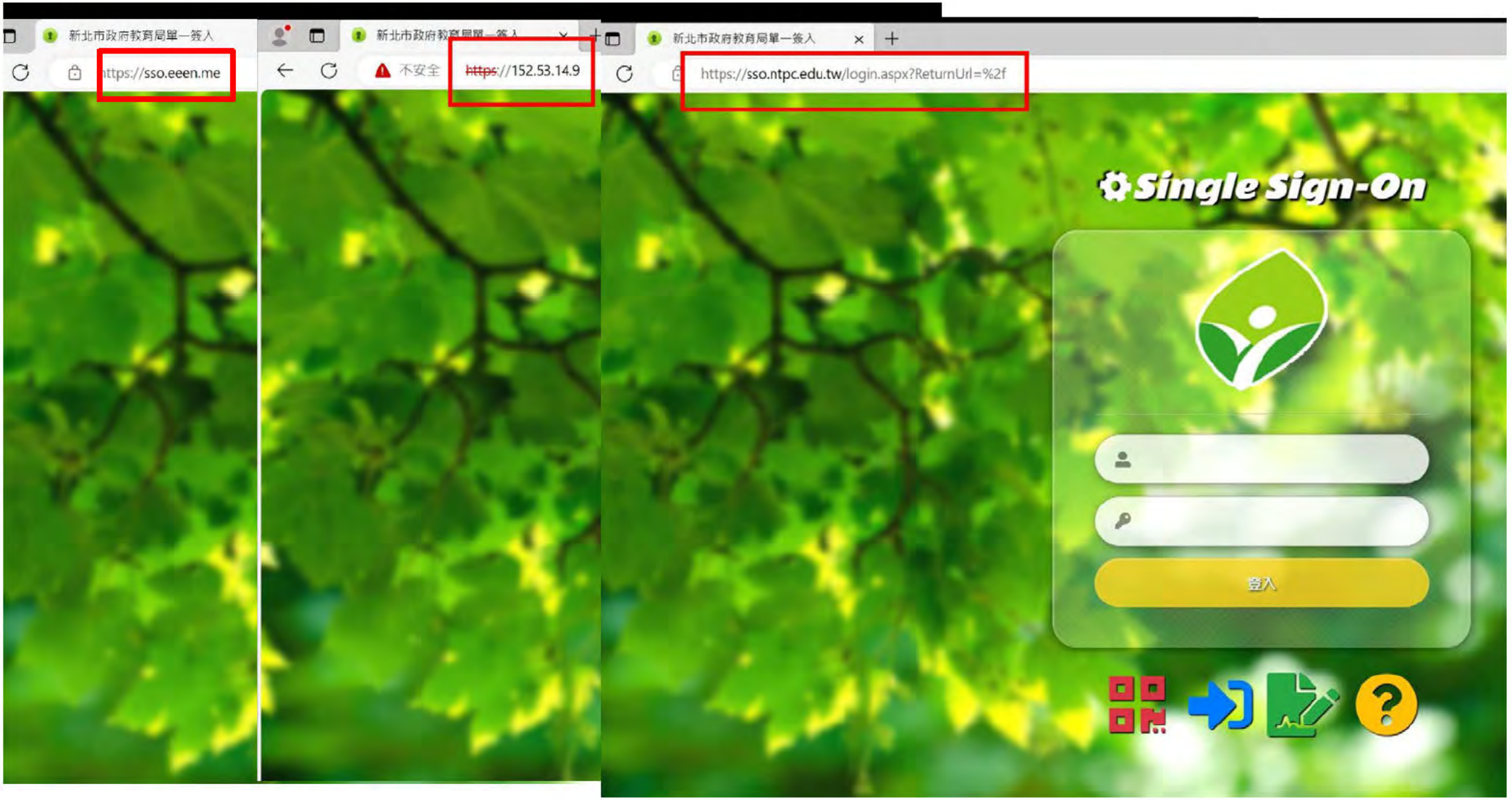
社交工程六大手法

- 網路釣魚（Phishing）
- 恐嚇軟體（Scareware）
- 下餌（Baiting）
- 魚叉式網路釣魚（Spear phishing）
- 假托（Pretexting）
- 尾隨（Tailgating）

網路釣魚通常是指**企圖透過電子郵件、通訊軟體來獲得你個人資訊以竊取你的身份認證。**大多數網路釣魚會企圖讓自己看起來像是一般行為，實際上卻是用於犯罪活動。

它們看起來就像是來自銀行、信用卡公司、信譽良好的公私立機構的正式通知，通常在訊息中會夾帶惡意連結，**引導收件者至看起來與官方極為相似的山寨網站，要求提供帳號密碼等資訊。**

社交工程手法-仔細檢視網頁URL



社交工程手法-2.恐嚇軟體（Scareware）

社交工程六大手法

- 網路釣魚（Phishing）
- 恐嚇軟體（Scareware）
- 下餌（Baiting）
- 魚叉式網路釣魚（Spear phishing）
- 假托（Pretexting）
- 尾隨（Tailgating）

恐嚇軟體的作法是**讓受害者被假警報驚嚇**,讓使用者會誤以為自己的系統感染了惡意軟體。然後他們會安裝建議的軟體修復程式 – 但這可能是惡意軟體，如病毒或間諜軟體。

常見的例子是出現在瀏覽器的彈出橫幅，顯示如“你的電腦可能已經被感染”這樣的文字。**它會提供安裝修復程式，或將你導向一個惡意網站。**

社交工程手法-Netflix釣魚郵件

Netflix 釣魚郵件事件背景與流程

- 背景：Netflix提供線上影音的服務，隨著2020年新冠肺炎肆虐全球，Netflix的股價也在同年成長了高達60%。全球至今約有2億名訂閱者，為娛樂界的龍頭。

➡ 駭客覬覦龐大的用戶資料庫、看準網路用戶行為改變

- 揭發：Netflix在2020年6月收到1400筆用戶投訴經常收到標題寫著「驗證失敗通知（Notice of Verification Failure）」的電子郵件，並要求用戶在24小時內更新其信用卡資料，否則該訂閱就會被取消。

➡ 駭客製造製造虛假急迫的情境，使用戶疏於求證

- 釣魚信件流程：

收到含假網址連結的email → 被引導到極相似的假網站 → 假網站要求用戶提供平常登入的資料、信用卡資訊和帳單地址 → 用戶被帶往真正的Netflix主頁

Netflix & Netfiix ?

社交工程手法-3.下餌（Baiting）

社交工程六大手法

- 網路釣魚（Phishing）
- 恐嚇軟體（Scareware）
- 下餌（Baiting）
- 魚叉式網路釣魚（Spear phishing）
- 假托（Pretexting）
- 尾隨（Tailgating）

下餌（Baiting）是**利用有吸引力的誘餌來引誘受害者**，從實體誘餌如有毒的USB隨身碟，到更加常見的點擊誘騙電子郵件和線上廣告。常見的”**誘餌**“包括**免費電影、獎品或大型比賽和音樂會的門票**。跟大型活動如國際比賽、選舉和賣座表演的行程結合在一起會讓騙局特別容易成功。

典型的策略是詐騙者會要求登入憑證或是有價值的個人資料以換取“大獎”，或將使用者重新導到惡意網站來取得它們的詳細資料或散播惡意軟體。**詐騙分子試著用各種手法來引誘你行動－登入來取得獎品、最後三件襯衫、點入此連結來取得門票等。**

透過郵件標題誘使看郵件內容

序號	種類	信件標題
1	財經類	銀行：央行恐出手降溫房市
2	保健類	喝咖啡會骨鬆？醫：錯！反降骨折風險！骨鬆的真凶是？
3	新奇類	被老婆趕出家門？可憐「雨中罰站」低頭懺悔　動物園笑曝真相
4	旅遊類	【仲夏節優惠方案】觀光署串聯微笑南灣展館
5	科技類	一接詐騙電話就洩 2 個資！專家曝對付「最好招數」
6	科技類	Win 10 支援倒數最後 16 個月　微軟跳「全螢幕視窗」提醒用戶
7	擬真類	「全透明文字」一招讓 iPhone 鎖定畫面變高級！隱私不外漏
8	時事類	明年最低工資「有望漲 4%」　月薪估逾 2.8 萬.時薪 190

社交工程陷阱-4.魚叉式網路手法（Spear phishing）

社交工程六大手法

- 網路釣魚（Phishing）
- 恐嚇軟體（Scareware）
- 下餌（Baiting）
- 魚叉式網路釣魚（Spear phishing）
- 假托（Pretexting）
- 尾隨（Tailgating）

魚叉式網路釣魚通常**鎖定特定個人或某機構的特定員工及其社群媒體帳號 (如 Twitter、Facebook 和 LinkedIn)**，它們會精心製作出很有說服力的電子郵件內容，並且在電子郵件當中挾帶可造成感染的附件檔案和連結。**一旦開啟檔案或連結，就會執行惡意程式或將使用者導向某個網站**。接下來，駭客就能建立其祕密通訊網路，然後朝攻擊的下一階段邁進。

- 魚叉式網路釣魚 (Spear Phishing)是勒索軟體 Ransomware攻擊企業的主要手法
- 醫療保險公司_ Anthem Inc. 大規模資料外洩的主因 : 魚叉式網路釣魚 (Spear Phishing)
- 南韓爆發最大駭客攻擊事件 因魚叉式網路釣魚 (Spear Phishing)而起
- 91%的APT 目標攻擊來自:魚叉式網路釣魚 (Spear Phishing)

進擊的詐騙!! ChatGPT/GAI輔助攻擊

攻擊手法：

1. 個性化詐騙：
 生成式AI可用於模仿組織或個人的風格，使網路釣魚看起來更可信。利用數據分析等方式，客制化詐騙訊息用以針對使用者的興趣及弱點。例如：用暱稱稱呼你的電子郵件、在信件中提及你最近的網購內容。
2. AI聊天機器人：
 聊天機器人可以與使用者進行對話，與使用者建立信任，拿取使用者的個人訊息。
3. 深偽：
 AI創建的逼真影像和聲音可以冒充與使用者親近的人。例如：來自銀行的電話要求緊急行動。

重點提示

- 勿在網路上過度分享個人訊息，驗證任何請求的真實性，並通報可疑活動。
- 識別過度個性化訊息、未經請求的報價和壓力策略

社交工程手法-5.假托（Pretexting）

社交工程六大陷阱

- 網路釣魚（Phishing）
- 恐嚇軟體（Scareware）
- 下餌（Baiting）
- 魚叉式網路釣魚（Spear phishing）
- 假托（Pretexting）
- 尾隨（Tailgating）

假托技術（Pretexting）**大多是透過電話完成，需要的是營造出說服目標給出個人或有價值資料的情境。**詐騙分子會假冒成正當或熟悉的人來安撫目標，像是ISP的客服，不同分公司或辦公室的同事，或是來自公司技術支援的人。犯罪分子有時會事先收集關於目標的資料來讓騙局看起來更加可信。

例如: 非預期地接到來自**“技術支援”**人員的電話，內容是關於需要**立即處理的問題**？或者是**冒充前老闆說服員工給禁區密碼**。也許來電者會要求提供個人資料或帳號資訊來立即處理問題。

社交工程手法— 語音釣魚(Vishing)

何謂語音釣魚(Vishing)？

- 是一種**社交工程詐騙**，攻擊者會**偽裝**成他人來打電話給受害者，目的是為了**騙取個人資料或金錢**。
- 語音釣魚跟社交工程息息相關，通常是利用**受害者心理**來說服他們採取行動。語音釣魚詐騙者會用**威脅**或**獎勵**的方式來讓受害者覺得自己必須服從。受害者經常會收到**威脅性**的**語音郵件/電話**，出現像是**法庭案件**或**凍結帳戶**等內容。

重點提示

- 提高對社交工程技巧的認識，特別是如何識別**語音釣魚攻擊**。
- 不要在接到來電要求提供**個人**或**財務信息**時**直接給出**，特別是當通話裡帶有**強烈的急迫感**。
- 當收到不明**來電**或是**未知來電且開頭有+號**時，可以直接掛斷電話。

社交工程— 變臉詐騙(BEC)

何謂變臉詐騙(Business Email Compromise, BEC)？

- 使用社交工程技巧來詐騙，第一種方式是，**偽照資料**，透過**釣魚郵件**詢問網站服務、報價等信件來**確認窗口**，通常會**鎖定經手交易的相關人員**，例如財務長、採購人員。第二種方式是，入侵**公司窗口的電子信箱**。駭客可能**即時攔截**與**竄改付款文件**的電子郵件，**改成駭客的付款帳號**。或者駭客也可能**入侵員工**的**電子郵件**帳號，以其身分**要求該公司的客戶或合作夥伴匯款**至指定的詐騙用帳戶。
- 全球變臉詐騙駭客最常鎖定的產業目標，前三大都是**常用電子郵件進行國家交易往來溝通的產業**，包括製造、食品以及零售產業，因為這些產業通常都有國外客戶，同時又對資安的警覺性很低。

重點提示

- 提高對社交工程技巧的認識，學會識別**可能的欺詐信號**
- 實施嚴格的**財務控制程序**，如在進行**大額**或**非正常交易**時需要**多人審核**。
- 使用電子郵件安全工具。

社交工程— 交友詐騙（Catfishing）

何謂交友詐騙（Catfishing）？

- 駭客利用**別人的照片、影片或個人資料建立一個虛假的社群帳號**，這些假身份通常用於網路霸凌或尋求關注，進而用來**騙取金錢或受害者的個人資訊**，但都不會與受害者有**實際接觸**，這些被盜取的個資隨後可能被用於另一次社交工程攻擊。
- 另一種方式是詐騙者在**交友平台**建立假的個人檔案，然後開始**約會、見面**，與受害者**建立感情聯繫**，進而詐取**金錢及個人機敏信息**。

重點提示

- 不要隨便給予網路上的陌生人金錢或貴重物品。
- 對於與自己交往不久的網路朋友的突然請求，**保持警惕和懷疑**。
- 網路交友須謹慎，見面時需要確定對方真實身分，避免落入社交工程圈套。

社交工程— 交友詐騙（Catfishing）

駭客深度偽造員工聲音成功入侵 Retool公司

Retool

- 此起事件由駭客向 Retool 多名員工發送釣魚簡訊，聲稱自己是 Retool IT 團隊人員並表示能夠解決員工無法獲得醫療保險的薪資問題。收到釣魚短信後，大多數 Retool 員工沒有進行回應，但有一名員工中計，因而引發了此次網路攻擊事件。
- 害員工點擊了簡訊中的網站連結，該連結到引受害者到虛假的登入網站，登入並進行多因子身分驗證後，網路攻擊者使用人工智慧的深度偽造技術模仿該員真實聲音，並向其他員工通話。雖然受害員工多次對電話表示了懷疑，但不幸的是，最後還是向攻擊者提供了一個額外的多因子身份驗證（MFA）代碼。
- 由於Google Authenticator 應用程式最近引入了雲端同步功能，該功能雖然便於用戶在手機遺失或被盜時可以存取多因素驗證碼，但 Retool 指出如果用戶Google帳戶洩露，那麼其多因子驗證代碼也會被洩露。進入Google帳戶就能立即存取該帳戶中的所有 MFA 權杖，這是網路攻擊者能夠進入內部系統的主要原因。

資料來源： 資安人2022/03/28
影像來源： Morgan Stanley

社交工程手法-6.尾隨（Tailgating）

社交工程六大陷阱

- 網路釣魚（Phishing）
- 恐嚇軟體（Scareware）
- 下餌（Baiting）
- 魚叉式網路釣魚（Spear phishing）
- 假托（Pretexting）
- 尾隨（Tailgating）

尾隨（Tailgating又稱piggybacking）是犯罪分子所使用最簡單和古老的招數之一。就如字面意思的跟著其他人，利用他們的憑證來進入限制區域– 當某人打開閘門時，他們就**快速地通過而不用買票**。

現在，有越來越多公司的辦公室有門禁，尾隨（Tailgating）問題也跟著增加。但門禁對安全來說相當重要。**除了要保護實體安全，限制進入工作場所的某些區域可以防止設備或智慧產權被竊**。不幸的是，員工對這**規定態度鬆散**，經常認為只是種安全守則，並不重要。

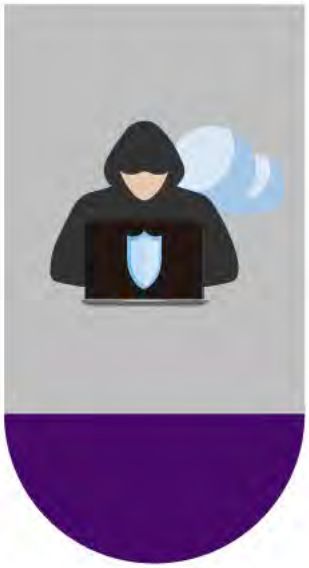
社交工程攻擊可能造成的影響

駭客想要盜取的資料

遭社交工程攻擊可能造成的後果

竊取硬碟中的檔案資料

監聽鍵盤輸入的敏感資料



遠端遙控用戶端電腦

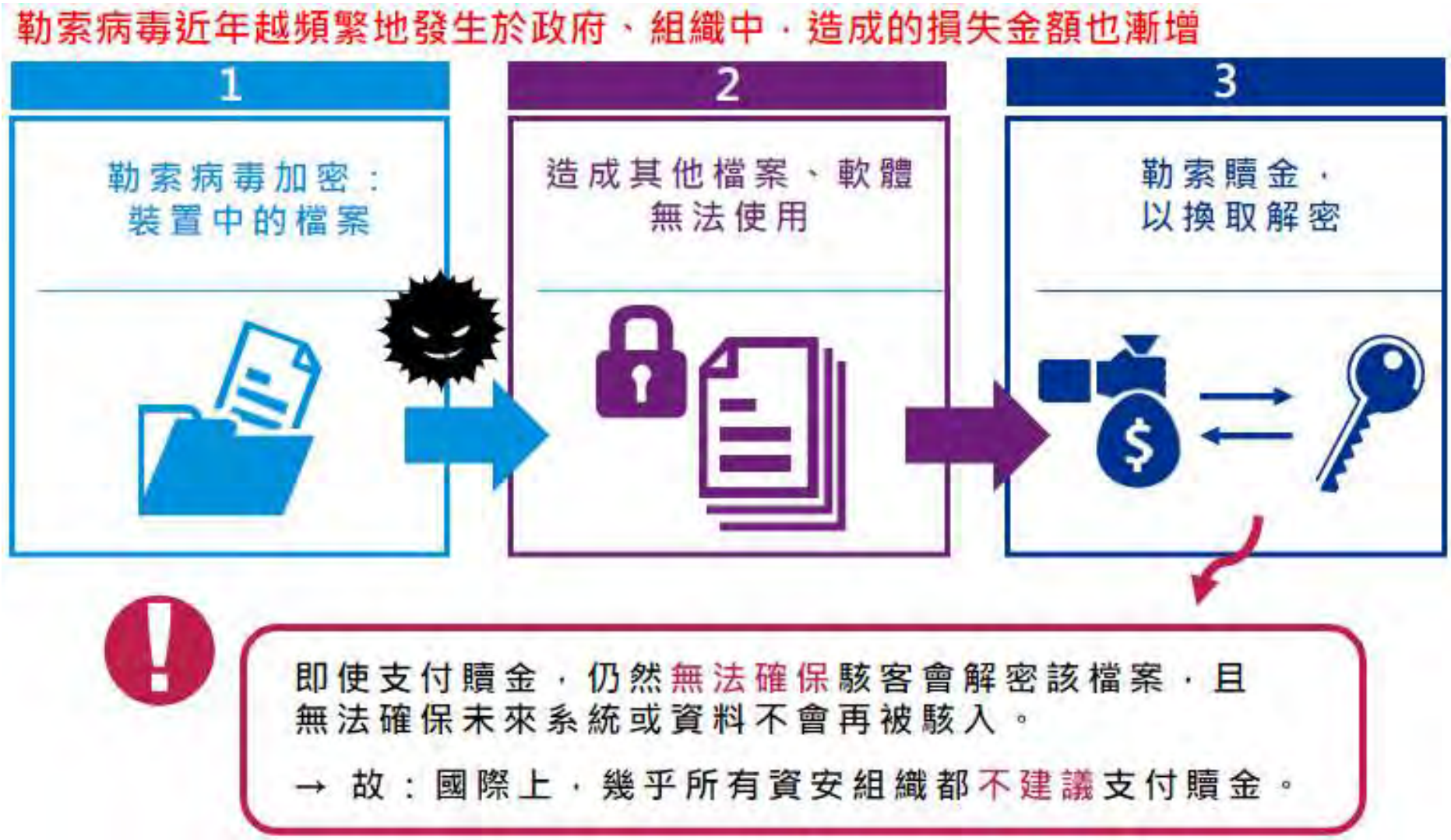
攻擊其他內部的電腦

成為攻擊內部網路的跳板

勒索軟體攻擊風險激增

- 日益增長之數位依賴加劇網路威脅
  - WEF「2021年全球風險報告」指出，2020年惡意軟體與勒索軟體攻擊分別增加 358% 與 435%
  - 勒索軟體即服務(Ransomware-as-a-Service, RaaS)之興起與網路犯罪生態體系之形成，推波助瀾下讓勒索軟體之威脅範圍與經濟損失日漸擴大
- 勒索軟體鎖定大型企業或政府關鍵基礎設施
  - Conti駭客集團對哥斯大黎加政府進行勒索軟體攻擊，導致包括財務部、稅務及海關等機關資通系統停擺
  - Laspus$駭客集團攻擊全球包含T-Mobile、NVIDIA、微軟、三星等大型科技公司，至大量機密內容被公開

什麼是勒索病毒


勒索病毒近年越頻繁地發生於政府、組織中，造成的損失金額也漸增
1
勒索病毒加密：
裝置中的檔案
2
造成其他檔案、軟體
無法使用
3
勒索贖金，
以換取解密
即使支付贖金，仍然無法確保駭客會解密該檔案，且
無法確保未來系統或資料不會再被駭入。
→ 故：國際上，幾乎所有資安組織都不建議支付贖金。

勒索病毒特色及行為

事先潛伏、伺機而動

- 駭客可能在數月前透過同仁**個人電腦**、**網頁**或**DB伺服器**，入侵機關內部網路並開始**刺探與潛伏**，竊取**特權帳號**後侵入網域控制伺服器(AD)。
- 派送具**惡意行為的工作排程**，執行排程時將駭客預埋在內部伺服器中的勒索軟體下載至記憶體中執行。

勒索病毒攻擊手法


一
二
三
四
●入侵同仁電腦、伺服器、潛伏於機關內網
●竊取特權帳號
●侵入網域控制伺服器
●竄改排程，派送具惡意行為的工作排程
●遭加密 顯示勒索訊息/電郵，要求贖金以取回檔案

如何防範勒索病毒攻擊

- 在校內宣導以下事項：
  - ✓ 不明郵件請勿開啟，不要輕易相信主旨為中獎、優惠、折扣、免費等不實資訊。
  - ✓ 如對來信有疑問(尤其是親友)，須先連絡寄件人確認郵件及附件來源。
  - ✓ 不點選可疑的網路連結或下載可疑的檔案；拾獲隨身碟勿好奇打開查看。
  - ✓ 請勿使用公務系統帳號或電子郵件信箱註冊外部網站會員。
  - ✓ 定期確認電腦防毒軟體之病毒碼與作業系統更新，並設定防毒軟體定時執行全硬碟掃描(請勿中斷)。
  - ✓ 定期執行重要資料備份，並須將於備份後備份媒體離線。

社交工程與零時差攻擊之間的關係

兩者之間的關聯性？

- 可**利用社交工程**進行**零時差攻擊**，例如：攻擊者可能會利用**社交工程**技巧**誘使受害者下載有害的軟體**，這種軟體利用未知的漏洞來入侵系統。
- 社交工程和零時差攻擊經常一起使用，使攻擊更加有效。

零時差攻擊是什麼？

是指攻擊者在**軟體**或**系統漏洞被公開或補丁發佈之前就開始進行攻擊**。

這種攻擊通常**很難防範**，因為**沒有人知道這種漏洞的存在直到攻擊發生**。

KPMG觀點

- 提高對社交工程技巧的認識，不要隨便點擊**不明連結**或**下載未知的檔案**。
- 保持軟體和系統的**最新版本**，即使這不能保護你免受零時差攻擊，但它可以**減少其他已知漏洞的風險**。
- 使用網路安全工具，如防火牆、防病毒軟體等。

APT鎖定式攻擊竊取機密資料

- APT攻擊是常見網路攻擊手法，駭客集團常鎖定特定組織或國家，精心策劃結合多種攻擊手法，持續而隱匿地逐步滲透，藉此竊取機敏資料
  - 美國國土安全部網路安全暨基礎安全局(CISA)於2022年5月發布AA22-103A警訊指出，已有APT駭客團體針對特定ICS / SCADA裝置，開發具備高度自動化攻擊能力之模組化工具，駭客成功進入OT網路後，即可透過工具掃描、入侵及操控受影響裝置

JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

APT Cyber Tools Targeting ICS/SCADA Devices

SUMMARY

The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising

Actions to Take Today to Protect ICS/SCADA Devices:

- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
- Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks.
- Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors.

Astaroth 銀行透過網路釣魚攻擊竊取用戶敏感資訊

近期網路上出現一個名為 Astaroth（又稱 Guildma）的銀行惡意軟體，針對巴西進行網路釣魚攻擊活動。

1. 攻擊者透過模仿官方稅務文件誘使受害者下載包含惡意軟體的壓縮檔案。此惡意軟體使用混淆的 JavaScript 程式碼繞過安全防護，並連接到命令和控制伺服器，這種攻擊手法可能導致長期損失，包括資料外洩、信譽受損、監管罰款和業務中斷，目的是竊取用戶敏感資訊。
2. 要警惕可疑的電子郵件和網站，不要點擊未知連結或下載附件，並建議採取措施，例如加強密碼策略、使用多因素身份驗證、保持安全解決方案和軟體更新以及實施最小特權原則。

重點提示

- 建議：
  - 實施多因素認證（MFA）：在關鍵系統和帳戶中啟用多因素認證，增加未經授權存取的難度，即使帳號密碼被竊取，仍可提供額外保護。
  - 定期更新安全措施：保持防毒軟體和其他安全解決方案的最新狀態，定期更新系統和應用程式，修補已知漏洞，降低被惡意程式利用的風險。
  - 最小權限原則（PoLP）：確保員工僅擁有執行其工作所需的最低權限，限制不必要的系統存取，減少內部威脅和潛在損害。

資料來源：wizon 2024.10.16

駭客藉由Google表單騙取個資

駭客於釣魚郵件中濫用Google表單竊取企業個資，使用Google表單之原因除其受到消費者與企業信任外，Google網域亦被大眾信任並躲避防毒軟體檢測。

1. 此釣魚郵件冒充美國小型企業管理局(Small Business Administration, SBA)，並使用Google表單為網絡釣魚頁面。電子郵件中聲稱SBA正進行COVID-19補助申請，只需點選連結填寫表格即可，惟大多數人不知道SBA近期已停止受理申請。
2. 駭客目的在於蒐集受駭者之個資，包括雇主識別碼、社會安全碼、駕照詳細資料及銀行帳戶資訊等，受駭者點選申請按鈕後，表單內容將傳送至製作表單之駭客，駭客隨即盜賣個資，或洗劫銀行帳戶。
3. INKY之研究員補充，去年涉及「偽冒政府」之網路犯罪導致超過1.42億美元之損失。今年到目前為止，已偵測超過14,000封釣魚電子郵件皆使用Google表單進行詐騙。

重點提示

- 不論學校或個人皆須提高警覺，對於要求提供敏感資訊的電子郵件，即使來源看似可信，也應保持懷疑，避免直接點擊其中的連結或提供個人資料。
- 對於一切網路資料皆需驗證真實性，可直接聯繫相關官方機構，確認該資訊的真實性，避免落入釣魚陷阱。
- 建議使用安全工具，安裝並更新防毒軟體和反網路釣魚工具，增強對此類攻擊的防護能力。

資料來源：資安人 2024.10.28

藉由Proofpoint郵件安全服務漏洞送出數百萬封釣魚信件

研究人員發現針對Proofpoint電子郵件防護服務而來的攻擊行動，駭客平均每天藉此發送300萬封釣魚郵件，過程中冒用知名企業品牌來行騙，並能通過大部分的資安系統偵測。

1. 駭客疑似利用Proofpoint郵件防護服務的漏洞EchoSpoofing，從而讓發出的釣魚郵件具有通過驗證的SPF和DKIM簽章，並能回應Proofpoint的電子郵件轉發服務，而能夠突破主要的資安防護系統偵測。而這些駭客大量散布的釣魚郵件，用途是竊取收信人的資產或信用卡資料。
2. 根據Guardio的觀察，相關行動今年1月出現，平均每天寄出300萬封惡意郵件，單日最高可達到1,400萬封。

重點提示

- 須加強檢查郵件防護服務配置，檢查 Proofpoint 等郵件防護服務的配置，確保僅允許授權的 Microsoft 365 租戶的郵件轉送，避免被駭客利用。
- 加強電子郵件安全措施，如部署先進的電子郵件過濾和威脅檢測系統，攔截惡意附件和釣魚郵件，防止攻擊者通過電子郵件途徑入侵。

資料來源：iThome 2024.08.01

勒索軟體Black Basta透過微軟Teams進行社交工程攻擊

針對勒索軟體Black Basta的攻擊行動，有資安業者提出警告，指出這些駭客結合社交工程手法，利用微軟Teams文字交談訊息，引誘使用者依照指示安裝遠端管理工具，從而挾持受害電腦，並作為入侵企業組織的跳板。

1. 發動大規模垃圾郵件攻擊後，上鉤的使用者就會被引至與特定微軟Teams用戶交談，攻擊者通常會透過貌似微軟技術支援人員、管理者、服務臺成員的Entra ID帳號登入微軟Teams，而且在Teams用戶身分顯示沿用這些名稱，使一般人誤以為他們是微軟的這些工作人員，而且，駭客通常會將帳號的顯示名稱設置為含有Help Desk的字串，聊天室的名稱多半是OneOnOne。
2. 若使用者照做，攻擊者就有機會藉由上述的遠端管理工具（RMM）控制受害電腦，並植入AntispamAccount.exe、AntispamUpdate.exe、AntispamConnectUS.exe等有效酬載，最終部署滲透測試工具Cobalt Strike，以便將受害電腦當作存取企業內部網路環境的跳板。

重點提示

- 應驗證技術支援人員身份，在接受任何技術支援之前，應透過官方渠道核實對方的身份，避免直接回應來自未知來源的技術支援請求。
- 建議公司限制遠端管理工具的使用，如在企業環境中，應限制或監控RMM工具的安裝和使用，防止攻擊者利用這些工具進行未經授權的遠端控制。 並實施嚴格的系統監控，及時發現異常的遠端連線或可疑活動，並定期審查系統日誌，確保及時發現潛在的安全威脅。

資料來源：iThom 2024.11.1

中國駭客組織Earth Lusca利用地緣政治議題在台發動社交工程攻擊

根據趨勢科技資安威脅研究員的調查顯示，著名中國駭客組織Earth Lusca利用中國及台灣的地緣政治敏感議題，在2024台灣總統大選期間透過社交工程手法發起駭客活動。

1. 整起活動於2023年12月至2024年1月期間最為活躍，透過初始存取、執行惡意程式與躲避防禦、搜尋檔案、資料編碼、滲透的流程設計來感染更多的目標。
2. Earth Lusca組織最新行動所採用的戰術工具、技術手法與程序(TTPs，Tactics, Techniques and Procedures)，趨勢科技資安威脅研究團隊指出該集團組織是利用一份名為「China’ s gray zone warfare against Taiwan」的壓縮檔案作為誘餌，誘使受害者點擊下載，進而感染目標對象，而壓縮檔中包含從多個台灣地緣政治專家或其組織中的員工所竊取的文件。

重點提示

- 組織對此類攻擊仍不可掉以輕心，學校與個人皆應避免點擊可疑的電子郵件和網路連結，並保持軟體更新及修補安全漏洞，方可降低成為駭客攻擊受害者機率。
- 學校與個人皆須提高對網路釣魚攻擊的警覺， 對於涉及敏感政治議題的未經證實的文件或郵件，應保持高度警惕，避免隨意點擊或下載附件。並加強組織內部的資安防護，應定期檢查系統安全，確保未被未經授權的第三方入侵。

資料來源：iThom 2024.03.05

惡意 PyPI 套件攻擊引發AI 搜尋引擎的社交工程疑慮

由於 Python 的廣泛應用及受歡迎程度，也讓駭客開始在 PyPI 裡製作一些惡意套件包，提供使用者下載安裝，試圖竊取 GCP 帳密，造成資安攻擊事件發生。

1. Checkmarx 研究人員發現 2024 年 6 月上傳到 PyPI 平台上的 “lr-utils-lib” 套件，有資安上的疑慮，會針對 macOS 的作業系統竊取 GCP(Google Cloud Platform) 帳密而造成資料外洩。從一部分 “lr-utils-lib” 套件 setup.py 簡化版程式裡可以看出一些惡意行為的痕跡。
2. 在程式裡有發現一個名為 go 的列表，裡面有 64 個經過雜湊後的 UUID資料。發現程式會比對雜湊後的 IOPlatformUUID 是否在列表裡，看得出來有在針對特定的 UUID 做攻擊。
3. 如果資料外洩成功，攻擊者就能夠未經授權存取使用者的Google Cloud資源，造成資安危害。

重點提示

- 建議老師或學校使用官方和受信任的來源，優先使用有良好評價和大量用戶的套件包。查看套件包的下載量和維護情況，選擇經常更新、維護的套件包。
- 在使用不常見的套件包前，在PyPI上檢查是否來自可靠的開發者或組織。 並檢查套件包的詳細信息，包括發佈者和套件版本歷史，如果資訊量及下載量不多，請謹慎評估使用。

資料來源：iThom 2024.11.04

駭客組織Scattered Spider鎖定IT人員發動社交工程攻擊

研究人員針對駭客組織Scattered Spider最新一波的攻擊行動提出警告，並指出對方鎖定雲端SaaS應用程式而來，從中竊取企業組織的機密資料，並移轉至AWS或GCP平臺上外流。

1. 這些駭客對服務臺撥打電話，聲稱他們收到了新手機，需要重設多因素驗證（MFA）機制。在與服務臺管理員互動的過程中，對方不僅能重設特權帳號的密碼，還能繞過多因素驗證防護。
2. 在成功得到受害組織的初始存取權限後，這些駭客針對微軟應用系統進行內部偵察，並找出遠端連線的存取管道。他們經常挖掘SharePoint網站上提供的VPN、虛擬桌面基礎設施（VDI），以及遠距辦公相關的內部文件進行調查，從而濫用合法工具遠端存取受害組織的內部環境。
3. 駭客不僅濫用了單一簽入（SSO）機制，還能藉由Okta管理平臺觀察這些帳號的狀態，進一步偵察。

重點提示

- 資訊組長須加強身份驗證流程，即使來電者提供個人識別資訊，也應採取多層次驗證，避免僅依賴單一資訊進行身份確認。
- 如使用 SaaS 應用程式應確認其安全配置，定期審查與更新，避免因配置不當導致的安全風險。並部屬行為監控系統，偵測異常的存取行為，如短時間內多次重設 MFA 或特權帳號的異常活動，及時發出警報。

資料來源：iThom 2024.06.17

注意! Deepseek釣魚網站

- DeepSeek是中國的低成本AI模型，目前在全世界迅速獲得全球關注。從2024年12月1日至2025年2月統計已有超過2600個釣魚網站被創立用於詐騙，詐騙方式為：
  1. 詐騙加密貨幣：誘使用戶購買假加密貨幣。
  2. 假IPO股票：聲稱出售DeepSeek的首次公開募股（IPO）前的股票。

重點提示

- 建議：
  - 用戶：提高警惕，避免點擊可疑連結。
  - 學校：改進詐騙檢測和下架，部署實時數位冒充保護能力。

資料來源：yahoo 2025.02.08

簡訊詐騙、廣告安全持續氾濫

資料來源： iThome 2023.10.06

有假借【台灣電力公司】名義發送提醒用戶電費未繳或停電的簡訊及電子郵件，並提供假網址、假檔案連結，誘使詐騙用戶信用卡個資及下載惡意程式等

1. 台電公司在27日發出防詐騙提醒
2. 詐騙信件標題電號以遮罩方式呈現
3. 詐騙附件為ZIP檔為主，開啟檔案可能導致電腦受駭
4. 位發展部在7月初表示，將從簡訊源頭號碼端做管理，將打造政府專屬短碼簡訊平臺，希望讓民眾更好識別簡訊發話方是來自政府機關。

重點提示

- 懷疑未知簡訊:如收到陌生號碼簡訊，應保持警惕不要隨便等選任何連結或回覆提供個人資訊需求。
- 建議在智慧型手機上安裝可信任的安全防護應用程式，並隨時使用最新版本，如此便可降低訪問惡意網站及安裝到惡意應用程式的風險。趨勢科技有免費提供可判別網址安全性的服務。
- 請勿從簡訊所引導的網站安裝應用程式。防範惡意應用程式的基本方法，就是只透過Google Play、App Store、電信業者等所營運的官方應用程式商店、開發商的官方網站取得應用程式。

中國駭客假借台積電的名義進行網路間諜攻擊行動

資料來源： iThome 2023.10.06

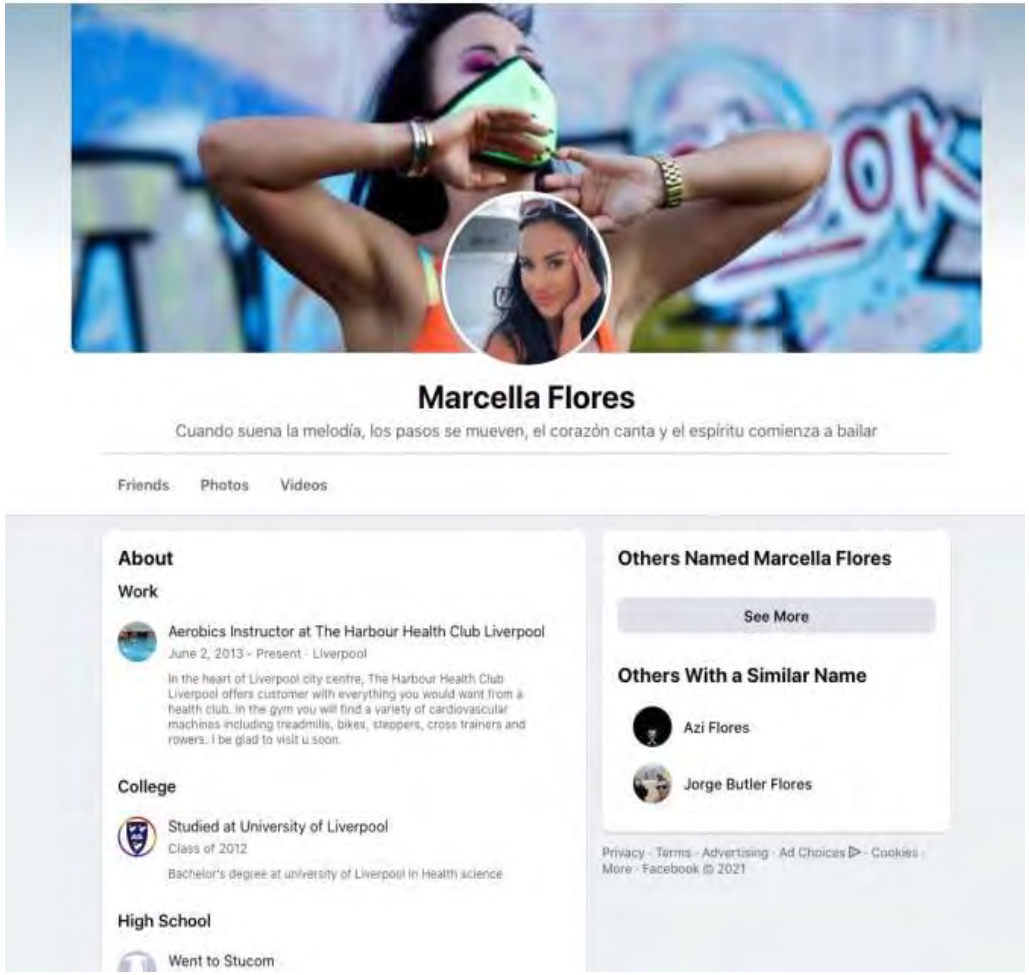
駭客疑似透過釣魚郵件，寄送聲稱是台灣積體電路製造公司（台積電）的簡介PDF檔案，一旦收信人開啟該文件，電腦就會啟動名為HyperBro的惡意程式載入工具

1. 駭客利用過往未被揭露的惡意程式下載工具進行滲透。
2. 工具透過Windows內建的PowerShell及BitsTransfer模組，從已被入侵的中國億賽通Cobra DocGuard加解密伺服器取得惡意程式
3. 程式安裝啟動之後，會利用另一家資安業者McAfee簽章的可執行檔mcods.exe，運用DLL側載手法執行Cobalt Strike的Shell Code，而該Shell Code連線的C2伺服器IP位址，與HyperBro相同。

重點提示

- 看到陌生郵件就要提高警覺，如果是認識的人所寄來的，仍應盡可能透過電話、即時通訊等方式與對方確認；如果是系統通知信件，也可以在網路上找到官網並發問
- 注意**Email中出現文字異常的狀況**、**看似正常的假冒重要信件**以及**看似正常的假系統通知信**

社交工程釣魚郵件植入後門事件
- 2021年WFH期間駭客美人計詐騙得逞案例



- 資安公司Proofpoint指出駭客組織TA456FB上偽造了一個有氧舞蹈教練的帳號，並與一名在航空業承包商子公司工作的員工建立了聯繫，透過企業和個人即時通訊軟體來保持聯繫，而攻擊者利用持續的電子郵件通訊，向目標發送惡意軟體，最終得逞
- 根據調查團隊指出，TA456透過假社群帳號，向受害者先發了一些與健康相關的郵件、圖像及影片，以騙取受害者的信任和建立融洽的關係。在受害者因此降低心理防備之後，才在布線的幾個月後，向受害者發了一封所謂「飲食調查」郵件，並且得逞

資料來源：國外媒體報導、https://www.techbang.com/posts/88850-zian-detailed-how-the-hacking-group-tricked-defense-contractor

社交工程融合人工智慧的資安案例 - 到底應該如何正確識別老闆？

Forbes

EDITORS' PICK | Oct 14, 2021, 07:01am EDT | 76,205 views

Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Cybercriminals cloned the voice of a company director in the U.A.E. to steal as much as $35 million in a huge and complex heist. GETTY

- 杜拜一位銀行經理接到公司董事打來的電話：公司有一項收購案，要從帳戶裡轉出巨額資金，希望他核准這道流程，還附上了相關律師的電子郵件，以確認金額和轉入帳戶。這交易看起來完全合乎規定，流程也沒有問題，何況還是老闆親自打來的電話，於是就按要求將3500萬美元如數轉出，但他萬萬沒有想到，電話那頭熟悉的老闆的聲音，其實是用語音複製技術所合成的
- 這個案例顯示，使用AI在網路犯罪中所製造出來的影像和聲音，能夠造成多大的破壞性。更可怕的是，如此逼真的轉換，操作過程並不難。例如在Github上大熱門的的AI擬聲專案Real-Time-Voice-Cloning，能夠在5s內複製你的聲音並產生任意內容，還能直接下載或者自行訓練合成器

資料來源：國外媒體、 https://www.techbang.com/posts/91247-ai-voice-cloning

利用員工的社群網站及電子郵件入侵組織

別讓你的個人檔案像一本可以自由翻閱的書

- 個人可能覺得分享生活中的大小事務很有趣，但是對心懷不軌的人，這正是大好機會，利用你**過度分享的資訊**，在你察覺之前，**滲透掌握你的一舉一動**，即使你分享資訊沒有損失，最終仍可能**為此付出代價**。
- **駭客可能寫電子郵件**給的他的上司，提出非常**有趣的提案**，在假試算表**嵌入惡意程式碼**，只要幾秒鐘就能完成。事實上大部分攻擊，都使用**社交工程**，建立**可信的藉口**欺騙受害者，一時判斷不當，駭客就能取得他所要的**存取權限**。

重點提示

- 維護**組織**的**資料安全**，也要維護**個人**的**資料安全**
- 建立社群人脈固然重要，但要進行隱私設定，**別讓陌生人看光你的一切資訊**。
- 發文時也要**遵循組織安全規定**，也要小心收到**陌生訊息或內容**

屏大遭冒名詐騙案例：社交工程之巧手

案例簡介

- 詐騙手法層出不窮，有位木工師傅遭到詐騙集團**冒用屏東大學職員的名義**，聲稱校內有緊急工程需施作為由，要求店家承作，並且須與其指定的材料廠商合作，購買垃圾桶，並催促木工師傅在簽約前，先匯款材料訂金30萬元給材料商，待店家匯款後，便失去聯絡。
- 詐騙者利用**社交工程技巧**，包括**信任建立**、**欺騙**與**操縱**等方式成功騙走金錢

重點提示

- 對所有來自**未知來源**的信息**保持警覺**，並進行**必要的驗證**
- 在進行金錢交易時，尤其要對任何要求**立即付款**或**不尋常的付款方式**保持警覺
- 提供如何有效地防止社交工程的建議，例如定期進行反社交工程的訓練和教育

如何防範社交工程攻擊

防範社交工程攻擊基本觀念

- **寄件者身份不可靠，安全判斷需多角度驗證**
  - 即使寄件人來自 **edu** 或 **gov** 網域，也不能完全相信。
  - 檢查郵件內容，注意語句/用字是否不自然、要求是否異常緊急。
- **校務行政系統不會主動聯繫，操作謹慎核實**
  - 校務行政系統不會主動透過電子郵件或簡訊要求點入連結進行操作。
- **全面守護個人資訊安全，遠離詐騙風險陷阱**
  - 不要隨意提供密碼、身分證號碼或其他個人資料給不明來源。
  - 避免點入未經確認的連結或下載附件，以免中毒或資料外洩。

如何辨識社交工程郵件

在點擊進入郵件前，確認此封信主要內容，由於近期不論是社交工程測試、或真實駭客的攻擊方式，逐漸日新月異，因此若與「安全性警告」、「與業務/研究案資訊有關」的主旨更要謹慎留意。

釣魚郵件經常利用「安全性警告」、「帳號將被停權」、「中獎通知」，近幾年甚至演變到「與業務/研究案資訊有關」等相關名目，吸引被害者注意，並引起緊張情緒或貪小便宜的心態，使其一步步走入陷阱當中。因此，在執行任何行動前，都應該先小心確認這封郵件的真實性。以下是一些辨別釣魚郵件的小撇步，一起來看看吧！

如何避免點擊社交工程郵件

點擊前可確認事項

檢查寄件者的電子郵件地址是否正確，尤其是 @ 後面的網域名稱。例如，來自 Google 官方或系統的 Email 地址結尾應該是 google.com，而不會是 gmail.com，因為 Gmail 是開放給一般使用者都能註冊的網域。

如何避免點擊社交工程郵件

若不慎點擊先別慌！還有可補救機會

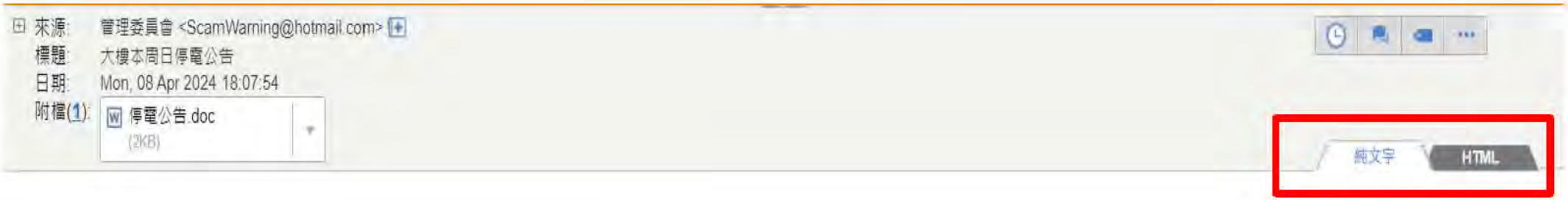
1. 僅點擊信件，且以純文字開啟：

✓ 點擊任何郵件時盡量以純文字開啟，若不慎點擊進入郵件，沒有改成透過HTML模式閱讀郵件、或是點擊、下載信件內的附件跟連結，仍有較大的概率駭客不會收到點擊的回傳值。反之，如透過HTML模式閱讀郵件，若以此模式開啟就會顯示郵件內的圖片，郵件內圖片恐嵌入惡意程式碼，仍會回傳數值給駭客，因此以純文字模式閱讀，會擋掉許多風險。如果懷疑郵件有問題，可在outlook的「垃圾郵件」匣中開啟郵件，也是以純文字模式開啟郵件。

2. 千萬不可點擊下載可疑信件之附件檔案

✓ 若點擊進入疑似社交工程信件，先別急著依據信件指示下載附件或是點擊連結，建議先電話與對方確認信件真偽，並確認為社交工程信件後將信件刪除、或是移至垃圾郵件匣。

如何避免點擊社交工程郵件



您好，
為了進行必要的設備維護或升級，我們將進行臨時性的停電，感謝您的理解與合作。

以下是停電資訊：
時間：週日凌晨開始至週日22點整
地點：本大樓1樓以上之樓層

停電期間，為了確保您的安全，請在停電前提前離開本大樓，同時注意停電期間用電設備是否已關閉，盡可能將用電設備的停用，以免設備受損。我們深感抱歉給您帶來的不便，並感謝您的諒解與支持。

如有任何緊急情況或需要進一步協助，請聯絡我們的緊急客服：0800-123-321。
謝謝您的合作。

純文字開啟模式(會阻擋圖片及惡意連結)

如何避免點擊社交工程郵件

1.HTML開啟模式(不會阻擋圖片及惡意連結)
2.請注意！使用手機開啟Webmail信箱，不會使用純文字開啟信件。因此若收到不明、可疑、標題聳動的主旨，先別急著開啟閱讀，待細部確認後再行動作。

如有任何緊急情況或需要進一步協助，請聯絡我們的緊急客服：0800-123-321。
謝謝您的合作。

詐騙猖獗!!分辨詐騙信件的小撇步

近期詐騙信件猖獗詐騙手段亦日益翻新，收到偽裝成合法機構的詐騙郵件已成為常見現象。為了避免公務資料外洩和資產損失，以下步驟請注意:

真實案例

對應步驟說明

1. 辨識寄件者合理性，是否為常態性公務來往人員，若非請提高警覺。
2. 辨識信件主旨是否符合您的公務範疇，若非則切勿再點開信件。
3. 若已誤點開信件時，辨識信件內容是否合理(語法、敘述邏輯..等，例 先生/媽媽非正常語法、烏克蘭客戶不合邏輯)，若與公務無關不點選連結及不下載附件。
4. 署名者與寄件者不符(寄件者為張O雯，卻是朱O奇署名)，可辨識不合理。
5. 簽名檔雖與寄件者同名，卻夾帶他人姓名或不明公司資訊，可辨識不合理
6. 可疑信件無論夾帶任何檔案，切勿點擊與下載。

●看到可疑的信件，應小心求證，或通報資安室協助判斷真偽，並留意來源是否可信任。

可以利用網路儲存我的密碼嗎?

網路儲存密碼安全嗎？

利用網路儲存密碼提供人們方便，然而當電腦被有心人士取走後，帳號密碼亦隨之被竊取，因此手動輸入密碼為較佳的登入方式，抑或於不同網站上設定不同帳號與密碼可以減少多個網站被同一帳號密碼登入的機率。

重點提示

- 除了密碼是否儲存的問題外，密碼設定的強度也很重要，建立複雜且長的密碼為佳，且需定期更換密碼以降低密碼被猜出而侵入個人帳號的機率。

網路常見弱密碼

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	123456	< 1 Second	8,159,358
2	123456789	< 1 Second	1,817,250
3	12345678	< 1 Second	700,019
4	654321	< 1 Second	245,827
5	1234567890	< 1 Second	210,168
6	woaini	2 Minutes	190,926
7	password	< 1 Second	125,606
8	zxcvbnm	< 1 Second	114,139
9	147258369	8 Seconds	108,762

最易在暗網洩露的20種密碼組合

您設定的密碼安全嗎？安全程度恐怕不如您預期的那般高。手機安全公司Lookout最近公佈了黑暗網站洩露帳戶信息中最常見的20個密碼列表，這些易被破解的密碼包括簡單的數字和字母排列(例如“123456”和“Qwerty”)以及易於輸入的短字句(例如“lloveyou”)等。查看一下這張清單，好確保自己所設定的密碼不在此範圍。

123456	123456789	Qwerty	Password
12345	12345678	111111	1234567
123123	Qwerty123	1q2w3e	1234567890
DEFAULT	0	Abc123	654321
123321	Qwertyuiop	lloveyou	666666

密碼暴力破解法 Brute Force Attack

以破解8位數密碼所需時間為例

- 全數字 → 不到一秒
- 全英文小寫 → 1分13秒
- 數字+英文小寫 → 16分30秒
- 數字+英文大小寫 → 21小時
- 數字+英文大小寫+特殊符號 → 24天
- 破解9位數 數字+英文大小寫+特殊符號 的密碼 → 6年

密碼安全議題

2024弱密碼報告

Top 8 弱密碼	
1	123456
2	password
3	123456789
4	guest
5	qwerty
6	abc123
7	letmein
8	password1

五大危險密碼設定方式

1. 長度不足
2. 複雜性低
3. 同一密碼多次重複使用
4. 以季節做為密碼
5. 用球隊/歌手/電影當密碼

密碼安全議題(續)

密碼安全性原則，困擾到駭客還是自己?

密碼安全性發明者Bill Burr坦承錯誤，與其規定英文、數字、特殊符號等組成複雜度，不如追求密碼長度。複雜的密碼不一定有效，因為人的記憶力有限，過於複雜的密碼不好記，另一方面，為了同時符合複雜性的要求並易於記憶，" P@$Sw0rD" 成為了流行的密碼，但其實容易被破解。

密碼需求

- 複雜性需求(包含大小寫、特殊字符)
- 最低長度限制
- 週期性要求變更密碼

建議的密碼選擇

- 具備長度、隨機性並且易於自己記憶的密碼(可用英文模態打注音輸入法)
- 多重因子認證(MFA)

密碼安全性設定宣導

教職人員電腦密碼應注意事項

密碼設定：

- 避免使用「qwerty」、「1qaz2wsx」及「!@#$%^&*」等鍵盤規律性作為密碼。

密碼安全性設定宣導

教職人員電腦密碼應注意事項

Google建議用戶在設密碼時最少要有8個字元，而且不要使用連續順序的數字或英文字等簡單組合。同時也應盡量使用**兩步認證**（2FA）功能（如有的話），以及定期進行安全設定檢查。

設定安全密碼的技巧

- 注音輸入法只有在台灣學中文的人才會使用，因此不容易被國外的駭客破解
- 設定時須包含以下的韻母才會有特殊符號出現
  - ㄡ、ㄥ、ㄝ、ㄤ ⇨ .、/、,、;
  - 王建民 ⇨ j;6ru04aup6
  - 彭政閔 ⇨q/65/4aup3

安全的電子郵件使用習慣

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 (例如：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**，避免將別人郵件地址傳出
- 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。

如何防範社交工程？(1/2)

社交工程防範方法

避免人性弱點遭利用：

- ✓ 提昇自我資安認知與警覺性
- ✓ 重要資料或密碼輸入時，應注意是否有旁人窺視
- ✓ 討論業務機密應注意場合
- ✓ 透過網路或電話溝通時，應確認對方身份
- ✓ 使用者帳號或密碼不可洩漏給任何人

平時電腦使用習慣：

- ✓ 安裝正版防毒軟體並定期執行更新及掃毒
- ✓ 定期更新作業系統和應用程式漏洞
- ✓ 定期更換密碼，且強度要夠

如何防範社交工程？(2/2)

社交工程防範方法

電子郵件防禦注意事項：

- ✓ 非公務業務相關不明來源與可疑之電子郵件請直接刪除，勿開啟、勿轉寄
- ✓ 不輕易點選、下載或回傳電子郵件內的連結
- ✓ 取消郵件預覽功能
- ✓ 不隨意開啟附件(附加檔案件及資料)
- ✓ 確認寄信人與主旨間的關係
- ✓ 非經查證，不要直接點選郵件中的超連結 ，詳細檢視網址是否正確(可將常用的網址加入我的最愛)
- ✓ 善用密件收件人

如何識別社交工程的詐欺行為？

社交工程的手法：

- 詐騙者巧妙地利用**賣家的好奇心**、**不熟悉「蝦皮」的情況**，並偽裝為客服以**獲取信任**
- 詐騙者建立了**虛假的需求**（必須通過審核才能接受蝦皮付款）和**假的解決方案**（提供假的蝦皮客服連結進行審核）
- 利用了**假台新銀行電話**來獲取**賣家的信任**，進一步**引導賣家提供銀行資訊**，並嘗試**引導賣家進行匯款操作**

重點提示

- 要對所有詢問**個人或銀行資訊**的請求**持懷疑態度**，特別是來自**未知來源的請求**
- 請熟悉你所使用的平台的**安全措施和認證流程**，**不要點擊**來自**未知來源的連結**
- 對於任何要求進行**轉帳或存款的請求**，特別是來自**未知來源的請求**，都要**格外小心**

如何預防新型態通訊軟體詐騙？

新型態的通訊軟體詐騙介紹

- 根據調查，2022年偵測到1.4萬的可疑連結
- 描述**假投資以及其他新型態的詐騙**，包括**LINE輔助認證**和**Google表單詐騙**

社交工程的技巧？

- 使用社交工程技巧進行這些詐騙，如**建立信任**、**利用恐慌感**等
- **AI科技**的發展如何可能使**詐騙更為狡猾**，並增加了資安與網路犯罪的風險

重點提示

- 提醒教職人員對任何在通訊軟體中接收到的**可疑連結保持警惕**
- 建議進行反社交工程的訓練和教育，以提升對**這些詐騙手法的識別能力**
- 強調在進行任何形式的金錢交易或資訊分享之前，**確認對方的身份與可信度**

社群媒體防護— FB安全設定(1/4)

社群媒體防護— FB安全設定(2/4)

社群媒體防護— FB安全設定(3/4)

社群媒體防護— FB安全設定(4/4)

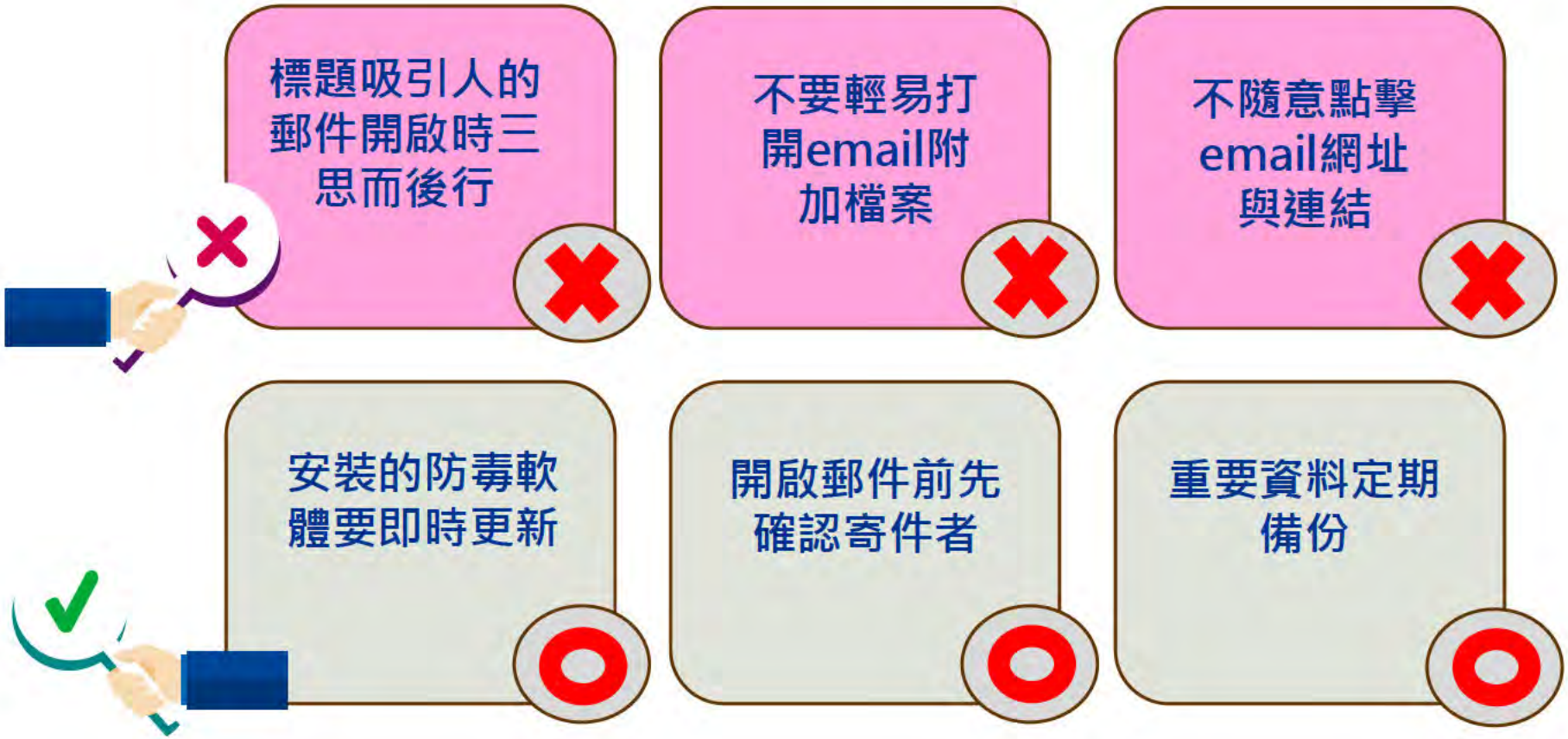
社群媒體防護—Line的安全設定(1/2)

社群媒體防護— Line的安全設定(2/2)

如何防範社交工程?

如何避免社交工程攻擊

防範社交工程— 三不三要


標題吸引人的郵件開啟時三思而後行
不要輕易打開email附加檔案
不隨意點擊email網址與連結
安裝的防毒軟體要即時更新
開啟郵件前先確認寄件者
重要資料定期備份

收到社交工程郵件通報流程

- 向教網中心回報時機：
  - 如收到來自以下網址所寄出之社交工程郵件
    - @ntpc.gov.tw
    - @ntpc.edu.tw
    - @*.ntpc.edu.tw(例如@apps.ntpc.edu.tw、@OOOO.ntpc.edu.tw都屬之)
  - 非上述來源無需回報
- 回報方式：
  - 由收件者直接將社交工程郵件轉寄至security@ntpc.edu.tw並副本給校內資訊組長
  - 資訊組長收到後請立即提醒校內師生：
    - 請勿點選相同的郵件
    - 針對此則情資無須再回報

問題與討論