

長庚學校財團法人長庚科技大學

114年度資通安全教育訓練

☑資通安全系列課程

★課程名稱：

人工智慧發展下的社交工程攻擊應有之防範作為

★授課時數：3 小時



講師：鍾文魁

現職：邦尼管理顧問有限公司 資深顧問

學歷：東吳大學法律學系科技法律組 碩士
華梵大學資訊管理學系資通安全組 碩士

經歷：



大綱

一 人工智慧對社交工程攻擊的影響與發展趨勢

二 識別與防範社交工程攻擊的方法與技巧

三 社交工程攻擊的應對策略與防範

四 討論

大綱子題

一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程
攻擊概述

不見血戰爭／去年遭攻擊近4千億次 台企淪駭客眼中肥羊

2024-06-24 00:57 聯合報／記者馬瑞璿／專題報導



全球資料外洩成本創新高 製表／蔡佩蓉、林雨荷 圖／聯合報提供

一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述

全球駭客和惡意程式都對準台灣！國防、金融、製造業都成目標



商業周刊

更新時間：2024年8月22日 週四 上午11:29

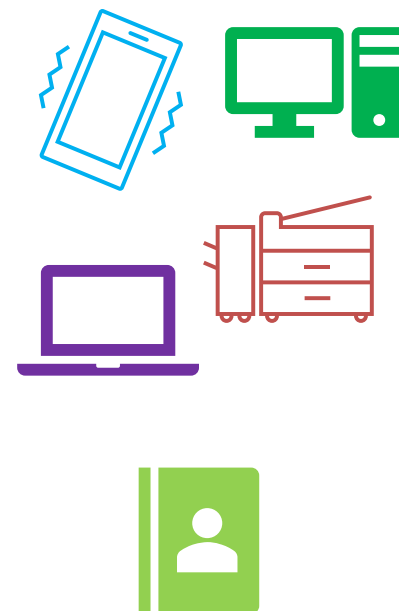
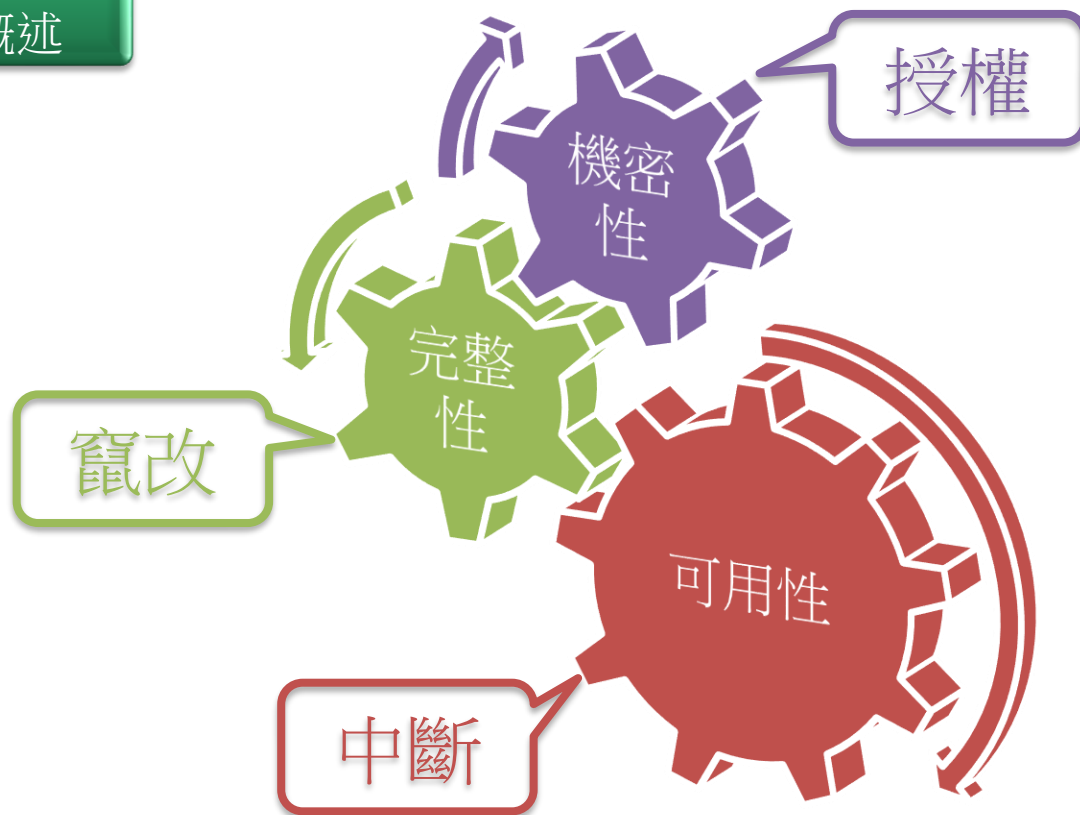


資安已被寫進賴政府的5大信賴產業中。(攝影·楊文財)

一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程
攻擊概述



一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述

什麼是社交工程攻擊？

社交工程攻擊是利用心理學和人類行為漏洞進行的一種攻擊手段。

攻擊者透過操縱受害者的信任或情感，誘使其暴露敏感資訊、執行危險操作或提供非法存取權限。



一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述



2024-10-31 14:02

『公布113年第三季高風險業者・提醒網路賣家慎防新型態詐騙』

2025-03-21 17:15

114/03/08-03/14 民眾通報高風險業者

114/3/15-114/3/21民眾通報假投資(博弈)詐騙網站【網友不會幫你賺錢、請勿聽信網友投資】

發佈日期：2025-03-25 10:06

更新日期：2025-03-25 10:06

詐騙
算不算
社交工程



一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述



一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程
攻擊概述

114/3/15-114/3/21民眾通報假投資(博弈)詐騙網站 【網友不會幫你賺錢、請勿聽信網友投資】

發佈日期：2025-03-25 10:06

更新日期：2025-03-25 10:06

網站名稱	網址	件數
WAIMAOMIKE	it.waimao.it.com	20
ZEUS	mythvipzx.com	14
POYA	www.poyabuysshop.com	10
PHA	wk.phas.it.com	9
宏和	app.fdyreu.com	8
恆泰	www.ritunb.com	8
OANDA	o-andamarts.com	7
Payhawk	www.payhawkforextradan.com	6
GUED	www.guedw.com	6
ACRRSOUSSEL	www.carousell13.shop	6
TikTok	tk.tnsa.top	6
愚果	www.vcnsdkg.com	4

一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述

員工被騙內部權限！Twitter 名人盜帳號事件為
「社交工程」攻擊

俗話說得好，資安最大的漏洞就是「人」。社交工程攻擊用的不是高深的電腦技術，而是用詐騙的方式要到關鍵人物的驗證資訊，進而取得登入權限。



一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述

常見的社交工程攻擊手法

引導點擊
釣魚網站

網頁廣告

釣魚郵件

發送偽裝郵件
誘騙點擊

冒充他人
發送訊息

通訊軟體

電話

偽裝他人騙
取銀行帳秘
或轉帳

一

人工智慧對社交工程攻擊的影響與發展趨勢

社交工程 攻擊概述

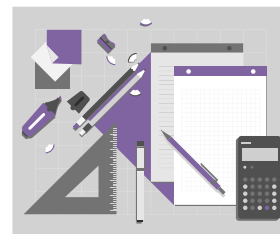


一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

人工智慧



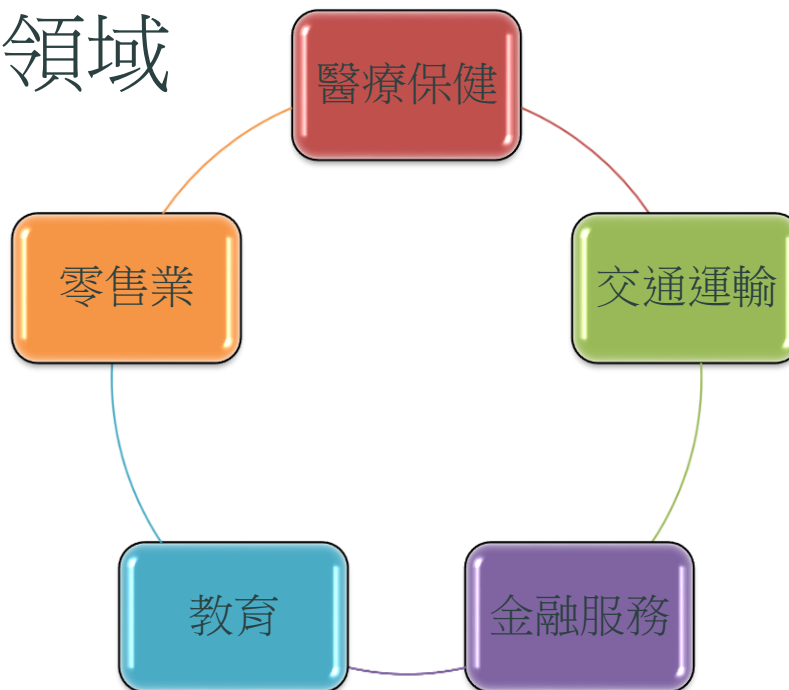
使機器模擬及執行人類智慧的科學與技術領域
使機器能夠學習、推理、理解、認知和解決問題

一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

人工智慧應用領域

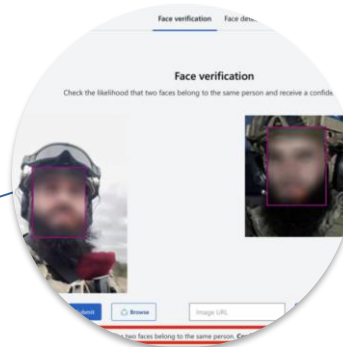


一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

人工智慧應用領域



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

Angel Has Fallen: A swarm of armed drones attack the President
電影場景



實況是：以色列國防軍（IDF）在2021年5月中旬攻擊加薩走廊時，使用了世界上第一個人工智慧（AI）引導的作戰無人機蜂群。這群小型無人機被用來定位、識別和攻擊巴勒斯坦激進組織「哈瑪斯」（Hamas），這是無人機蜂群首度投入到實戰當中。

資料來源：https://www.youtube.com/results?search_query=Angel+Has+Fallen
<https://news.ltn.com.tw/news/world/breakingnews/3591775>

一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

絕密飛行

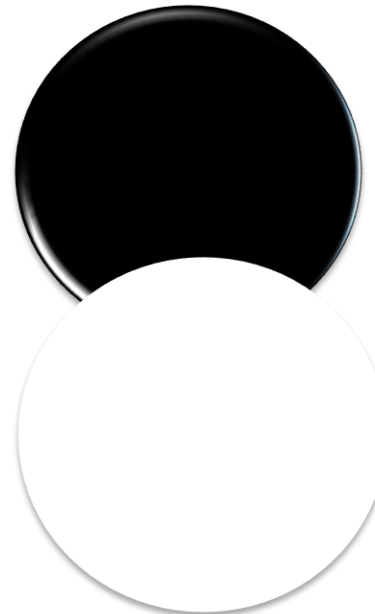


一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

DeepFake



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

「深度偽造(Deepfake)」是「深度學習(Deep learning)」和「偽造(Fake)」的組合詞。



一

人工智慧對社交工程攻擊的影響與發展趨勢

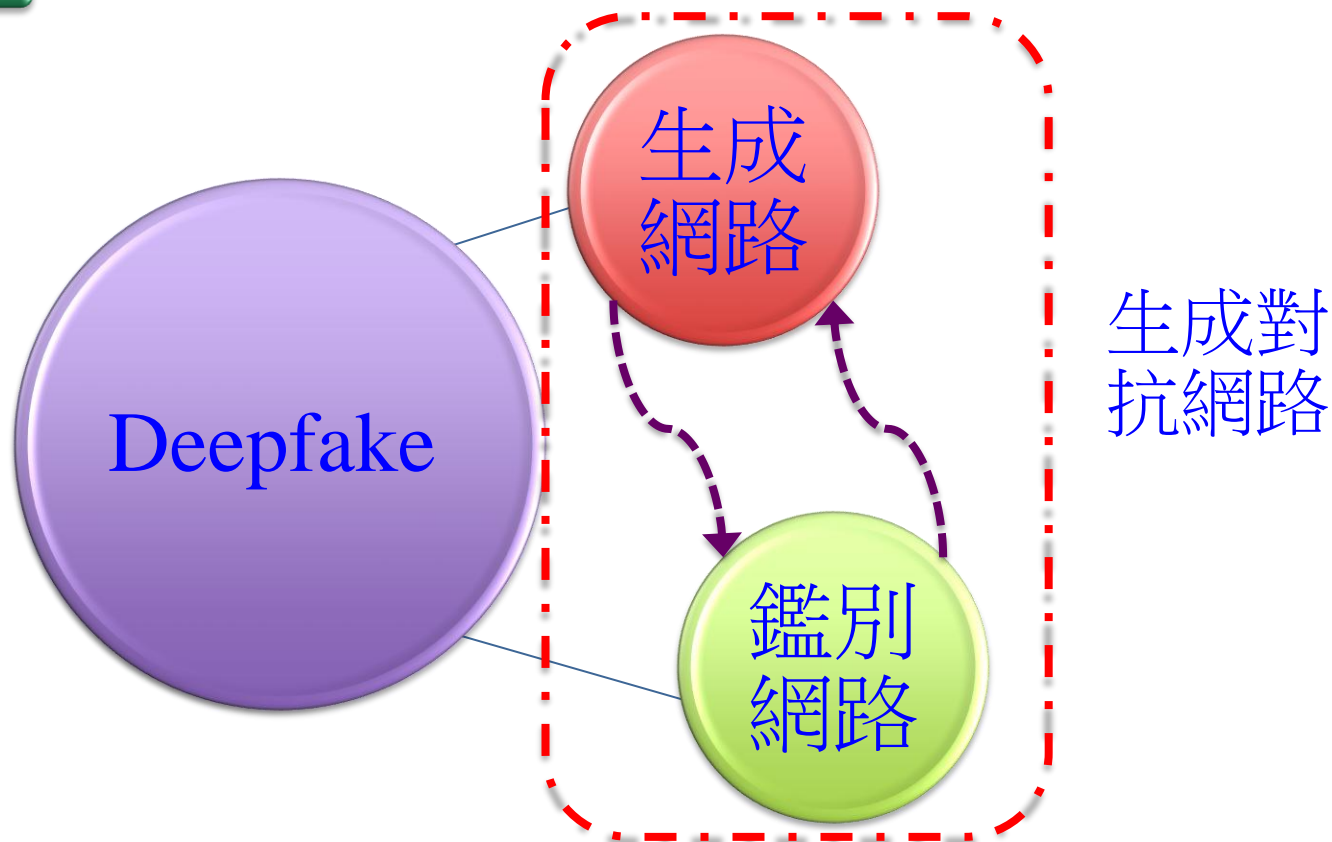
人工智慧如何改變社交工程攻擊



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

- **深度學習與語音合成技術的應用**

現今的攻擊者可以使用AI和機器學習技術進行語音和視頻合成，創造與真實人類相似的語音或影像，這使得他們可以偽裝成受害者認識的人或公司高層，更容易欺騙目標。

例如，利用深度偽造（deepfake）技術，攻擊者能夠製作極具欺騙性的視訊或語音，甚至可以模仿受害者的說話方式。



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

- **AI驅動的自動化攻擊**

AI技術能夠自動化產成客制化的釣魚郵件、網站、訊息或社交媒體內容，讓這些攻擊看起來更具真實性和針對性。

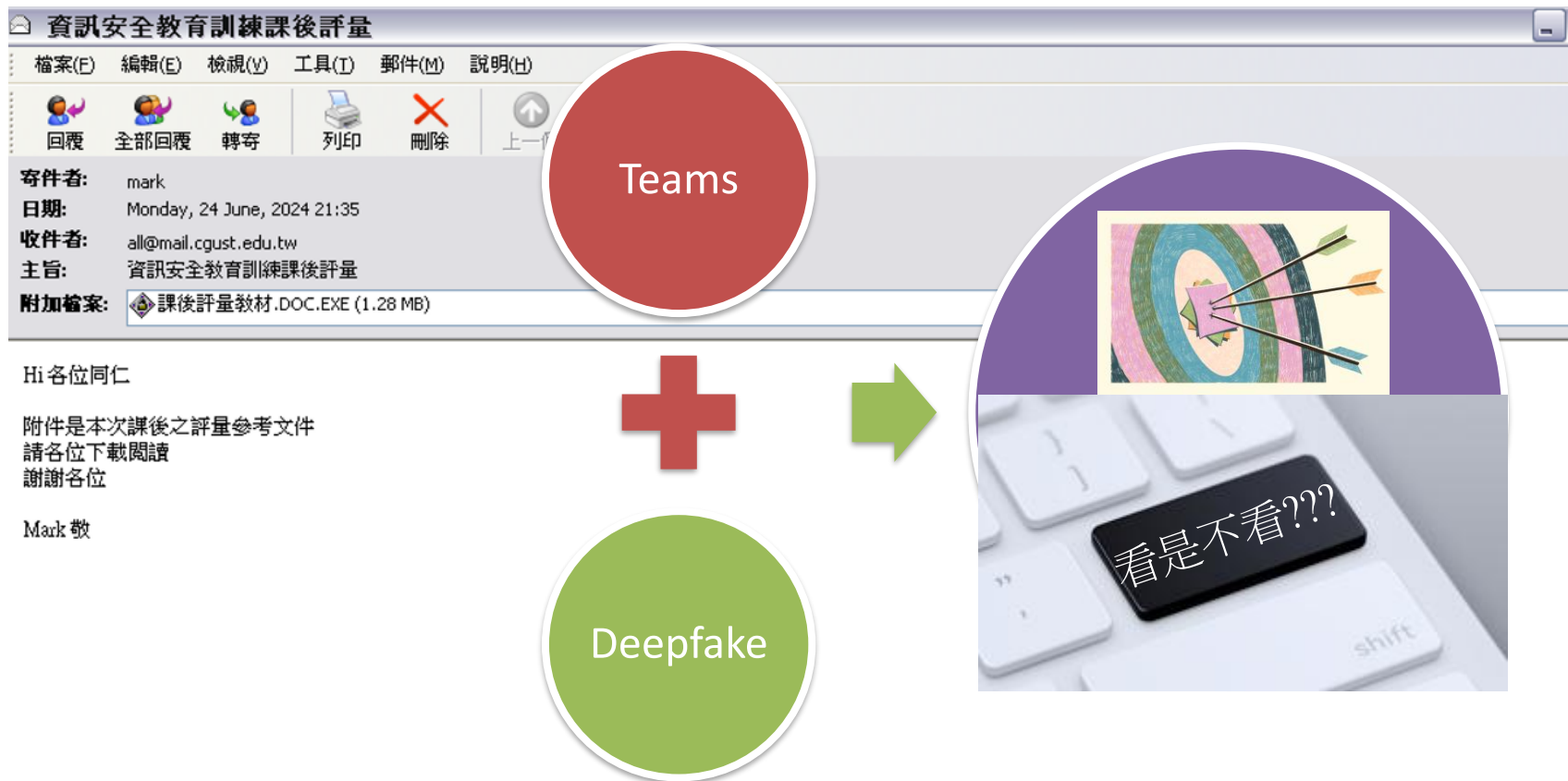
AI系統還能夠分析大量數據，精確識別高價值的攻擊目標，並根據目標的個人特徵、行為模式定制攻擊策略。



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

CrowdStrike 資安報告中的AI攻擊趨勢

- **CrowdStrike對AI驅動的攻擊趨勢分析**
根據CrowdStrike的資安報告，AI和機器學習的進步將會顯著增加攻擊的規模和精確度。
- 駭客不再依賴手動策劃攻擊，而是利用AI快速產成大量針對性強的攻擊內容，並通過自動化的過程來實施這些攻擊。



一

人工智慧對社交工程攻擊的影響與發展趨勢

人工智慧如何改變社交工程攻擊

CrowdStrike 資安報告中的AI攻擊趨勢

- **預測未來的AI攻擊模式**

預計在未來幾年，攻擊者將依賴AI進行更加智能化和個性化的社交工程攻擊。

- 例如利用AI分析受害者的社交網路、通訊內容甚至語音與視頻記錄，以生成極具針對性的攻擊內容，使受害者難以分辨真假。



大綱子題

二

識別與防範社交工程攻擊的方法與技巧



識別與防範社交工程攻擊的方法與技巧

識別社交工程 攻擊的跡象

警示信號與可疑活動

學習如何從電子郵件、網站、電話等通訊中識別出社交工程攻擊的典型特徵。



可疑的發件人
或網站地址

語氣過於急迫
或威脅

要求提供私人
或機密資訊





識別與防範社交工程攻擊的方法與技巧

識別社交工程
攻擊的跡象

可疑的發件人
或網站地址



發件人地址與官方機構不符，
網站地址可能包含拼寫錯誤或
不常見的域名。



識別與防範社交工程攻擊的方法與技巧

識別社交工程
攻擊的跡象

語氣過於急迫
或威脅



詐騙者可能會使用焦慮或威脅的語氣迫使目標快速做出決定。



識別與防範社交工程攻擊的方法與技巧

識別社交工程
攻擊的跡象

要求提供私人
或機密資訊

要求提供帳號密碼、身分證字
號、銀行資訊等。



識別社交工程
攻擊的跡象**AI生成內容的辨識技巧**

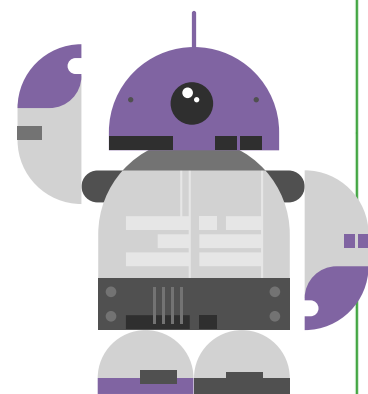
AI生成的內容可能存在語言結構的異常或不自然的格式。

學會識別AI生成文本的異常，例如語氣過於一致，缺乏個人化或過於精確的資訊（例如突然了解非常詳細的個人資訊）。



AI偽造語音和影像的挑戰

「深度偽造它利用深度學習技術訓練大規模的數據，包括人臉圖像、語音，以及視頻等。這些數據用於模仿和學習不同人的特徵、動作和聲音。然後，再利用人工智慧（AI）技術創造虛假內容，包括假的圖像、聲音和影片，從而實現AI換臉或者語音複製等功能。」





識別與防範社交工程攻擊的方法與技巧

人工智慧與社交
工程攻擊的辨識
挑戰

【詐騙】AI深偽技術投資詐騙貼文！蔡英文、張忠謀影片遭變聲置換嘴型冒用 2023/11/16

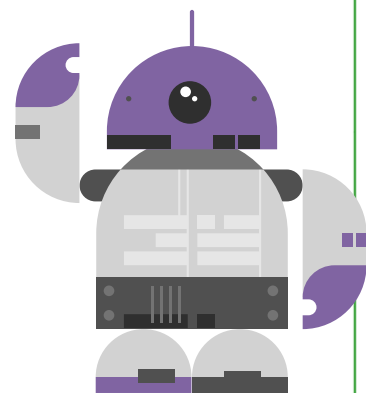


MyGoPen查證參考：

<https://www.mygopen.com/2023/11/deepfake.html>

辨識技巧：

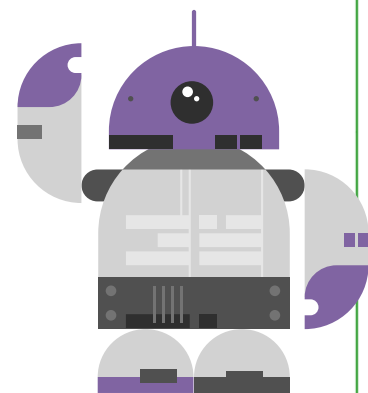
留意語音中的細微異常（例如語調、節奏的微妙差異），以及識別視頻中的不自然之處（例如面部表情是否過於僵硬、眼神移動，觀察頭部以下的身體或背景事物是否一直固定不動）。



偽裝成可信來源的攻擊

利用AI的自動化分析功能，攻擊者能夠創造高度個性化的攻擊資訊，模仿目標的同事或朋友，增加攻擊的可信度。

在收到來自朋友或同事的可疑訊息時，應進行額外的驗證，如直接通過電話確認。





識別與防範社交工程攻擊的方法與技巧

社交工程攻擊 防範措施

實施強密碼策略，並推動雙重身份驗證（2FA）。此外，應該定期審查員工的存取權限，確保僅授權的員工能夠存取敏感資訊。

身份驗證與
授權管理



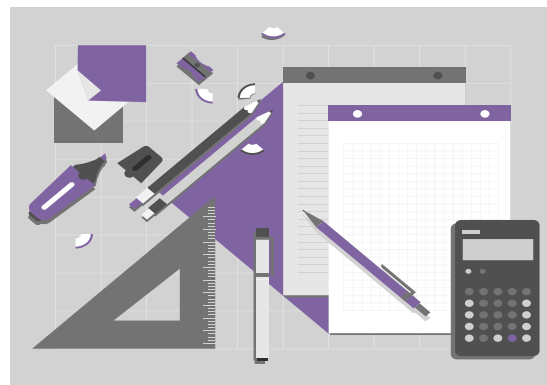


識別與防範社交工程攻擊的方法與技巧

社交工程攻擊 防範措施

定期進行安全意識訓練，教育員工識別和應對社交工程攻擊的基本技能。這應該包括對釣魚郵件、假冒電話的識別，並通過模擬攻擊來提高員工的警覺性。

加強員工資安
意識訓練





識別與防範社交工程攻擊的方法與技巧

社交工程攻擊 防範措施

如果遭遇社交工程攻擊，應該能夠迅速識別並報告問題。

建立緊急應對
流程





識別與防範社交工程攻擊的方法與技巧

社交工程攻擊
防範措施

社交工程攻擊退散

不隨意開啟來路不明之電子郵件
不隨意點擊來路不明之連結或附件
安裝防毒軟體並更新病毒碼
定期執行病毒掃描
隨時注意電腦或網路使用狀態



大綱子題

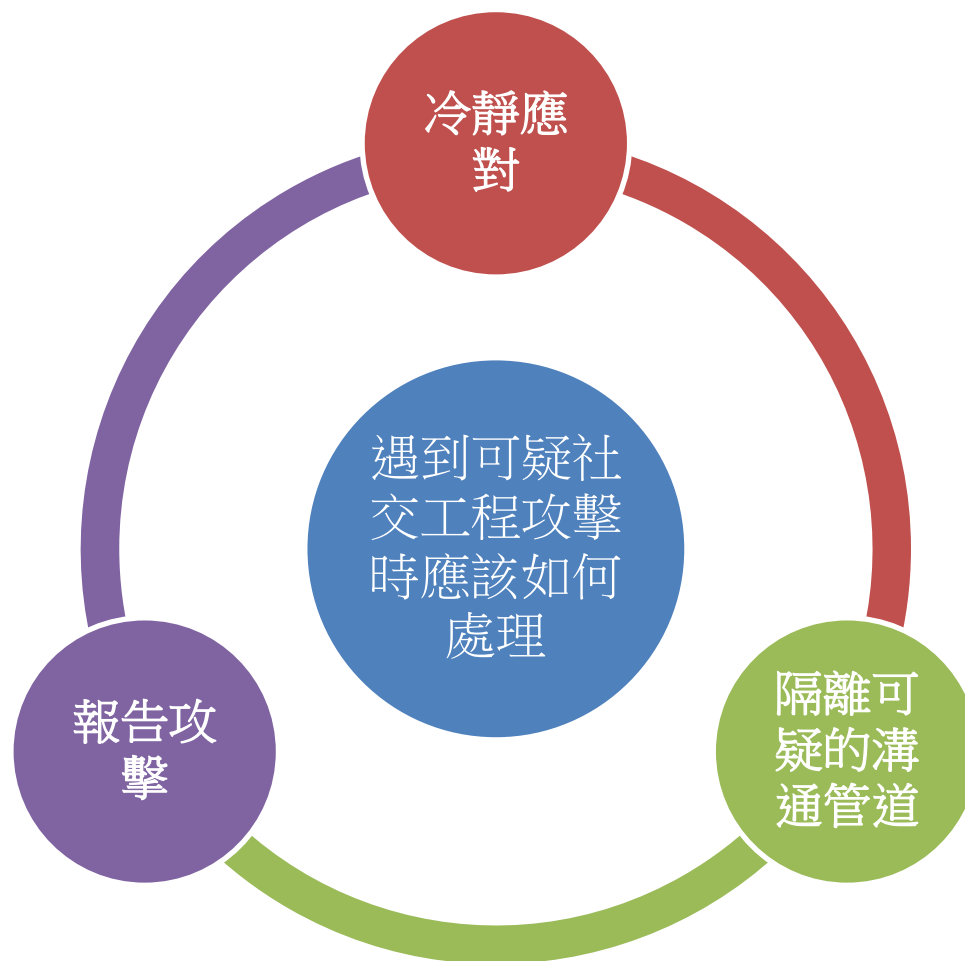
三

社交工程攻擊的應對策略與防範

三

社交工程攻擊的應對策略與防範

應對社交
工程攻擊

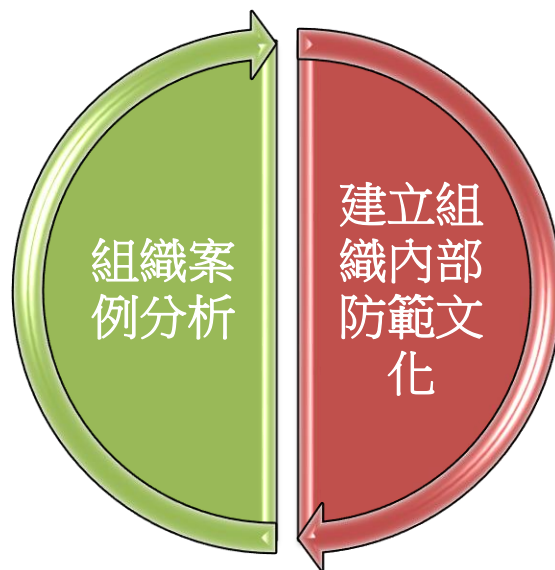


三

社交工程攻擊的應對策略與防範

應對社交
工程攻擊

防範社交工程攻擊組織面策略



三

社交工程攻擊的應對策略與防範

應對社交
工程攻擊

未來挑戰與持續改進

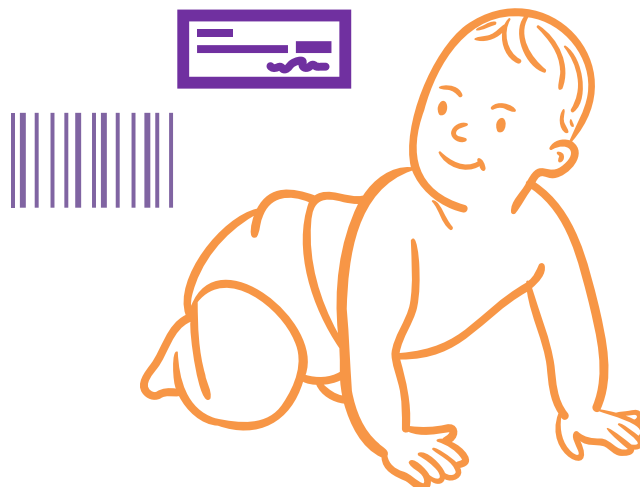
持續監控
與防範

技術創新
與對策

三

社交工程攻擊的應對策略與防範

應對社交
工程攻擊



網路好奇寶寶

四 討論