

115 年 9 月份安全宣導

目錄

壹、機關安全維護宣導

〈延長線安全須知〉

貳、消保宣導

〈新北市消保官公布市售兒童智慧手錶查
核結果〉

參、反詐宣導

〈各類防詐宣導管道〉

肆、公務機密維護宣導

〈導入 OpenClaw 應落實五項資安防護〉

伍、廉政宣導

〈受贈財物規範〉

壹、機關安全維護宣導

延長線安全須知

(摘錄自:遠傳電信-心發現文章)

(一) 3招避免延長線引發電線走火

1. 電線不細綁重壓

電線長期細綁或被重物壓住，一方面不容易散熱，同時還會使裡頭銅線折損斷裂，導致溫度過高而起火燃燒。

2. 高功率電器避免使用延長線

冷氣、冰箱、微波爐、電磁爐、烤箱、烘乾機、吹風機等高功率的家電應盡量避免使用延長線；即便非用不可，也要避免一條延長線插上兩個以上的高功率電器。

3. 有無自動斷電保護裝置

選購延長線時，除了一定要有商品安全標章外，最好要具備過載保護功能。一旦使用的電器功率超過負荷時，過載保護機制就會自動切斷電源，保障家庭用電安全。

(二) 6步驟養成良好用電習慣

1. 拔插頭不拉扯

有些人在拔插頭時會習慣直接抓著電線往後扯，這樣容易造成內部銅線和外部絕緣層斷裂，進而造成電線老化。

2. 要用電時再插上插頭

除了冰箱、電熱水瓶等需要 24 小時運轉的電器外，其餘家電可以視使用情況拔掉插頭或關閉延長線電源，不僅可以省電，也能減少因長期產生電流而導致的電線老化。

3. 電器周邊不堆放易燃物

紙張、衣物、床單等盡量不要放在電器和插座周邊，以免電線短路產生火花時不慎釀成火災。

4. 定期清掃插座灰塵

「積汙導電」指的是許多大型家電如電視、冰箱、烤箱等，一插電後多半不會更換位置，插座周邊長年累積大量灰塵、毛髮，這些髒汙遇到水氣就有可能成為導體，造成電線短路走火。

5. 延長線定期汰舊換新

建議每 3 到 5 年就要檢測一次家中的延長線並更新。

6. 購買有安全標章的家電與電器

記得選購通過經濟部準檢驗局檢驗、貼有「商品安全標章」的家電，才能為居家安全多添一層保障。

貳、消保宣導

新北市消保官公布市售兒童智慧手錶查核結果

(摘錄自:新北市政府新聞公告)

新北市政府法制局於今年兒童節前，針對網路平臺熱銷之 5 款兒童智慧手錶辦理購樣檢測。檢驗結果顯示，5 款手錶在「電氣安全」及「化學物質」檢測上皆全數符合標準，但在「商品標示」部分卻 100% 不合格，消保官已移請主管機關要求業者限期改善，以維護消費者權益，不符合產品皆已於販售通路下架。

消保官表示，本次抽驗嚴格檢驗電池安規與化學物質，並委託臺灣檢驗科技股份有限公司進行，針對網購平臺隨機購買的 5 款兒童智慧手錶針對家長最關心的電池自燃疑慮，依據「電氣安全規範」進行嚴格測試。結果顯示，5 款手錶的開路電壓差在 24 小時內均未超過 5%，充放電功能皆正常運作，且電池無任何起火或爆炸情形，安全保護機制均維持有效。此外，針對手錶經常接觸學童皮膚的錶帶與背板，依據 CNS 15503 進行測試，8 項重金屬（如鉛、鎘等）及 6 種塑化劑均「未檢出」，全數符合安全要求。此結果顯示市售兒童智慧手錶在實體安全性上已有顯著提升。

然而 5 件市售兒童智慧手錶之中文標示皆不符合「商品標示法」及「電器及電子商品標示基準」規定，違規缺失包含：本體未標示商品名稱及型號、未標示原產地及製造年份、缺乏進口商資訊（名稱、地址、電話），甚至未標示使用方法與注意事項（或警語）。消保官強調，商品標示是消費者了解產品來源、規格與正確使用方式的重要途徑，標示不清不僅違反「商品標示法」，若產品日後發生故障或引發意外，消費者恐面臨求償無門的窘境。已由新北市政府經濟發展局移請業者所在地縣市政府依商品標示法命業者限期改正，若屆期未改正者，得處新臺幣 2 萬元以上 20 萬元以下罰鍰，並得按次處罰。

消保官亦呼籲廠商應落實兒童智慧手錶商品之品質安全及標示之正確性，以維護消費者權益及兒童安全。並提醒消費者千萬不要貪小宜，隨便從臉書或不知名賣場選購來路不明的兒童智慧手錶，可能造成小小生命身體安全之危險。

參、反詐宣導

各類防詐宣導管道

(摘錄自：警政署刑事警察局)

各類防詐宣導管道

警政服務APP



官網-165反詐騙官網

<https://165.npa.gov.tw/#/>



FB-165全民防騙網

<https://www.facebook.com/165bear>



LINE-165防騙宣導

<https://liff.line.me/1645278921-kWRPP32q/?accountId=tw165>



內政部
警政署 刑事警察局

肆、 公務機密維護宣導

導入 OpenClaw 應落實五項資安防護

(摘錄自:數位發展部資通安全署)

具備自主執行能力的 AI 代理工具 (AI Agent, 如 OpenClaw, 俗稱龍蝦) 已被廣泛應用於日常自動化任務。此類工具在提升作業效率的同時, 因具備極高的系統權限與 24 小時自主運作特性, 若未妥善設定防護機制, 極易成為駭客入侵個人主機與企業網路的破口, 可能導致使用者個資、機敏資訊如帳號密碼及金融資料等外洩, 引發身分冒用與財產損失風險。提醒使用者導入 OpenClaw 時, 應落實資安防護與環境隔離。AI 代理的資安風險並非單一漏洞問題, 而是涉及架構層面的系統性風險。例如 ClawJacked 漏洞, 攻擊者僅需誘導使用者瀏覽惡意網頁, 就能在不觸發瀏覽器安全警報的情況下, 對 AI 代理的管理員權限進行暴力破解。

(一) 在評估 AI 代理工具的風險時, 應特別注意以下幾類資安威脅情境:

1. 惡意指令可能出現在外部網頁:

AI 代理在瀏覽外部網頁或讀取社群留言時, 若內容中暗藏攻擊者預埋的惡意指令, AI 代理有可能執行刪除檔案、竄改系統設定等危險操作。

2. 第三方技能包暗藏惡意程式:

AI 代理可以安裝名為「技能 (Skill)」的擴充來執行訂票、製作影片等複雜任務。網路上已有開放平台供使用者分享自製的擴充包, 攻擊者可將惡意行為指令寫入其中並偽裝成正常的 Skill 上架, 一旦安裝即可能被植入後門或惡意程式。

3. 長時間運作導致安全守則遺失:

AI 代理能處理的資訊量有限, 長時間運作後會自動壓縮早期內容以騰出空間。在此過程中, 原本設定好的安全規則與權限設置可能被刪減, 導致 AI 代理逐漸「忘記」哪些事不該做, 產生失控行為。

(二) 評估與導入此類新型的 AI 代理工具時, 應提高警覺並落實下列實務措施:

1. 落實環境隔離:

避免將 AI 代理安裝於存放機密資料或日常作業的環境。應將其部署於全新、已格式化的獨立電腦, 或專屬的虛擬機或容器中, 以此進行有效的風險管控。

2. 外部帳號權限最小化:

為 AI 代理註冊專屬的獨立帳號, 避免將個人日常使用的帳號與密碼直接提供給 AI 代理。若必須登入外部服務, 建議設定具有時效性的臨時授權憑證, 時間一到權限即自動失效, 避免日後因疏於管理而導致帳號遭竊。

3. 設置人類審核機制：

針對高風險操作（如存取憑證、發送郵件或執行系統指令），應於系統設定中強制啟用人工審核，要求每次執行前必須經由人員手動確認方可放行。

4. 親自審查 Skill 擴充套件：

在安裝任何第三方技能擴充套件前，應先對其內容說明與程式碼進行完整的安全掃描。若發現內容中有要求下載不明檔案、連線至不明網站等可疑行為，應立即停止安裝並向平臺檢舉，同時企業用戶應於組織內部進行資安通報。

5. 將安全守則寫入「長期記憶」：

定期審閱且備份 AI 的長期記憶檔。務必將重要的安全限制直接寫入「核心記憶檔案」（如：OpenClaw 的 MEMORY.md）中，確保每次運作時都會強制載入安全守則，避免因記憶壓縮而遺忘設定好的防護設定。

數位發展部資安署強調，AI 代理技術能帶來顯著的創新效益，但須在「環境隔離」、「人工審核」的前提下進行測試與應用，方能兼顧數位發展與資訊安全。



小心AI代理變資安破口

資安署提醒

導入OpenClaw前 資安署提醒您落實下列防護

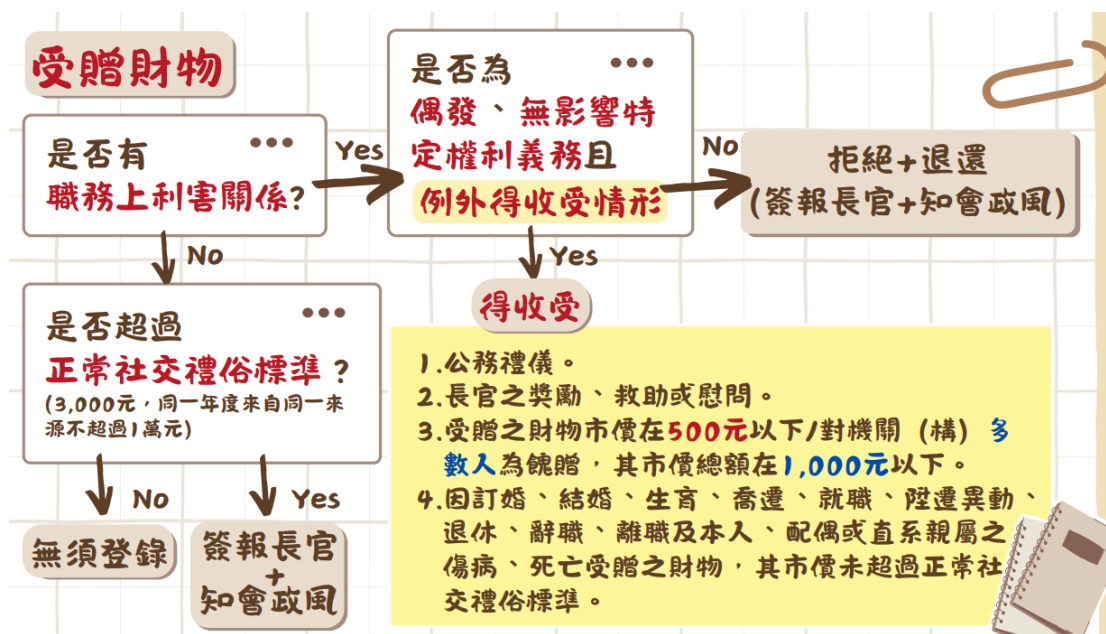
1. 落實環境隔離
2. 外部帳號權限最小化
3. 設置人類審核機制
4. 親自審查Skill擴充套件
5. 將安全守則寫入「長期記憶」

moda 數位發展部
Ministry of Digital Affairs

伍、 廉政宣導

受贈財物規範

(摘錄自：新北市政府政風處)



受贈財物得例外收受之情形

