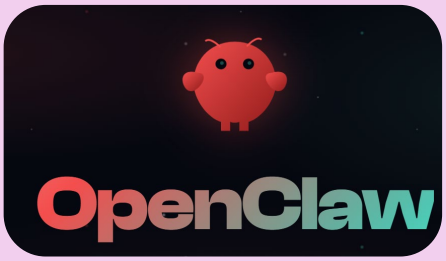
資安宣導　養龍蝦與資安風險

養龍蝦(AI)可以做什麼事？

- 可以管理行事曆，但行事曆有工作會議、孩子的生日……
- 可以當小幫手，但他也可能正在看帳號密碼、金融資訊……
- 可以收發郵件，但附件常包含證件、合約還有公務資料……
- 當我們以為【還好吧!】，這隻小龍蝦卻不小心被駭客拿去用….

我們以為只是小幫手，但可能正讓我們赤裸地活在駭客眼中！

「你養龍蝦了嗎？」
爆紅AI工具能幫你工作 資安專家提醒下載風險



一款名為「龍蝦（OpenClaw）」的AI工具，
它不像過去只能「陪你聊天」的機器人，
而是真正具備「手腳」的代理式AI（AI Agent）。

根據欣盾資安（XFCS）的技術觀測，這類主打「自動化操作」的軟體，雖然大幅提升了便利性，但在系統安全上卻存在潛藏的風險，龍蝦最強的功能是模仿人類動作，這意味著它必須擁有「視覺權限」來讀取你的螢幕。欣盾資安技術團隊指出，**一旦使用者下載到被駭客動過手腳的版本，你在螢幕上輸入的網銀密碼、私人訊息或公司商業機密，在對方眼裡就像並肩坐在一起看一樣清楚。**　資料來源:科技島

我們可以怎麼做？

- 秉持安全性、隱私性與資料治理等原則，重視隱私與資料安全
- 不揭露未經公開或同意之資訊、重要資訊、敏感資訊、公務資訊
- 不分享個人隱私資訊（個資、身分證字號、金融、健康等等）
- 避免輸入任何可識別您本人或他人的資訊（PII）、公務資訊
- 秉持批判性思考，不可完全信任生成資訊。
- 機密文件親自撰寫。
- 不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。
- 使用生成式 AI 應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。

參考資料：行政院及所屬機關（構）使用生成式AI參考指引