115年9月公務機密維護宣導

如何迎戰AI資安疫情

AI正在快速改變資安攻防的遊戲規則，在過去駭客需要投入大量時間進行資訊蒐集、漏洞研究、程式撰寫與攻擊測試；而現今AI正逐漸降低這些複雜工作的門檻，讓攻擊者可以更快、更大量地尋找目標與弱點。更值得注意的是，攻擊能力正在快速普及；惟防禦能力的成熟需要時間。

在AI時代，不要心存僥倖，就是最基本的防禦：

一、減少暴露在外的攻擊面：少一個入口，就少一個風險。

二、注意供應鏈安全：避免病從口入。

三、建立多層防護：不要期待系統永遠不會被攻破。

四、降低洩密傷害：保護最重要的數位資產。

五、做好營運維持：最重要的是確保組織活得下去。

六、冷靜應變：不要把時間花在找戰犯。

七、即時通報與聯防：一起阻止災害蔓延。

AI資安威脅已經不是未來式，而是現在進行式。我們不需要恐慌，但必須提高警覺。沒有人能保證自己的系統永遠不會被攻擊，也沒有人能預測下一個AI工具會把攻擊能力提升到什麼程度。

真正重要的是，在攻擊能力快速進化的今天，我們能不能更快盤點自己的弱點、更快發現異常、更快隔離風險、更快恢復營運，也更

願意把自己發現的威脅告訴其他人。這場數位疫情不可能只靠一家機構解決。政府、企業與整個資安社群都必須一起提高防禦韌性，才能把每一次攻擊的傷害控制在最小範圍。

資料來源：摘錄自 國家資通安全研究院 最新公告 2026/8/12「AI 資安疫情全球蔓延，機關與企業如何迎戰？」