資訊安全宣導_11404

什麼是 DeepSeek AI？DeepSeek 資料外洩事件/網址首段是「gov.tw」結尾的，才是政府專用網址！

114 年 04 月 07 日

中國信託證券股份有限公司

文件制／修訂記錄

版次	日期	說明	作者	修訂中	定稿
1.0	114.04.07	初稿	何彥甫		V

【目　　錄】

【圖 目 錄】

壹、什麼是 DeepSeek AI？了解 DeepSeek 資料外洩事件

DeepSeek AI 是一家中國人工智慧公司，專注於大型語言模型和深度學習。由於地緣政治的關係，外界對其用戶隱私保護抱持著高度疑慮。

近期，DeepSeek 陷入風波，超過一百萬用戶的敏感數據遭到洩漏。研究人員在發現 DeepSeek 旗下的一個公開資料庫後，意外獲得了完整的資料庫控制權，能夠訪問內部資料並執行操作。這次事件中，包含超過百萬條日誌記錄，內含聊天記錄、API 金鑰、後端細節等高敏資訊。更嚴重的是，此漏洞可能允許攻擊者提升權限，進一步掌控 DeepSeek 環境。

這並非 DeepSeek 首次遭遇資安攻擊。事實上，該公司在成立僅一週後就曾遭遇大規模攻擊。此外，DeepSeek 已被多個國家和組織禁用，而這次數據洩漏事件進一步證明了該應用程式的潛在風險。

圖1　AI 廠商示意圖

貳、 資通安全考量!行政院要求公務機關全面禁用 DeepSeek AI 服務!

行政院院長表示，DeepSeek AI 的資料來源取得有違反著作權法相關法規等疑慮，並且其模型訓練上也有思考審查、限制資料的問題。

此外，使用其服務可能使資料傳送至中國，在尚未釐清及排除疑慮之下，可能違反個資保護、侵害隱私等...

因此，基於國家資通安全考量，數位部已警示公務機關及關鍵基礎設施限制使用 DeepSeek AI 產品。

圖 2　DeepSeek 禁止使用示意圖

參、 網址首段是「gov.tw」結尾的，才是政府專用網址！

最近網路上傳出民眾收到未繳交通罰款的詐騙簡訊，簡訊上用偽造的監理服務網，並且刻意混淆，以民間商業縮網址服務加上不屬於政府網站的網址，將其結尾改為「gov.tw」，意圖冒充政府專用網域 https://gov.tw/ 。

網址是指網路上完整的地址，在網址首段的「網域」使用時是需要進行申請的，因此網址首段為 gov.tw 結尾的才是政府網站（例如 https://moda.gov.tw），其他出現在任何地方都有可能是偽冒（例如 https://xxx/mvdis.gov.tw），提醒同仁切勿點擊來源不明的簡訊或訊息連結，避免上當受騙。

數位部推出的政府縮短網址服務（https://url.gov.tw）網址首段也是 gov.tw 結尾，請認明政府機關專用網址，若收到不明連結或詐騙簡訊，也請務必不要轉傳，造成親友上當受騙。

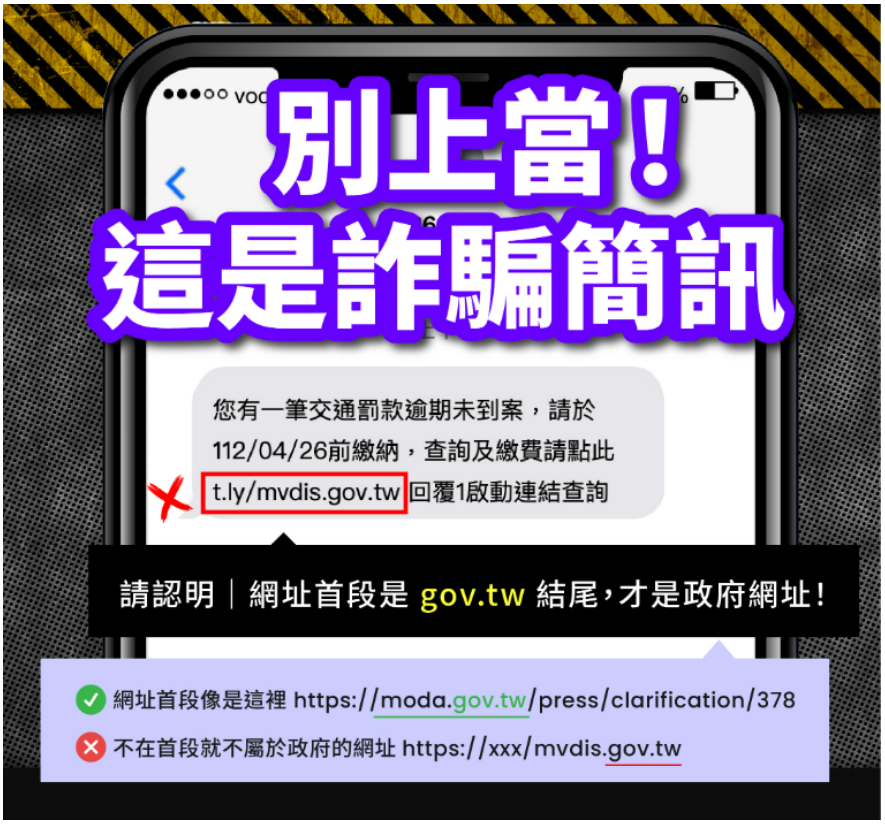

圖 3　gov.tw 需在網頁首段處

肆、 個人電腦使用其他注意事項

一、 參考附錄：

1. 個人密碼屬機密資料，由個人所有並需加以保護，密碼長度必須為 8 碼以上並且英文及數字混合，不可明碼儲存、記錄於書面、張貼於電腦螢幕、鍵盤、隔版、桌面...等可視區域；不得共用且不可公開，個人電腦之登入密碼必須定期變更。(CTSWI0027 個人電腦與周邊設備管理規範)、(CTSWI0025 行動資訊設備管理辦法)

2. 為防止他人窺視、不當使用或竄改資料，應設定電腦於五分內啟動內建之螢幕保護程式並設定密碼保護；離開使用中之電腦時，應先啟動內建之螢幕保護程式鎖定螢幕，並視情況結束連線登出(LOGOFF)。(CTSPY0005 資訊安全政策)

3. 考量各營業單位隨時輸單之需求，有關 Key-In 及營業員之個人電腦將不執行螢幕保護程式之設定，但仍需於離開座位時手動執行鎖定電腦功能(請同時按[Ctrl]鍵 ＋[Alt]鍵 ＋[Delete]鍵後，點選[鎖定電腦]之功能)，以確保資訊資源之安全。(CTSPY0005 資訊安全政策)

4. 電腦軟體之安裝與使用悉依本公司軟體採購(使用)標準，詳細軟體安裝清單請參閱(CTSFR0071 個人電腦標準安裝軟體清單)。新軟體之使用須經資訊單位評估無虞並納入採購(使用)標準後方可採購(使用)。(CTSWI0027 個人電腦與周邊設備管理規範)

5. 使用類似網路磁碟功能分享資料時，請符合下列事項。(CTSWI0027)個人電腦與周邊設備管理規範)

6. 非業務執行需求，避免設定資源分享。

7. 不應將整顆硬碟（C槽或D槽）設定為資源分享，以避免電腦系統及資料檔案遭到不可預期之複製及破壞。

8. 設置資源分享之資料夾，均應設置密碼及設定存取權限，並於使用後立即關閉分享。

9. 於本公司使用行動資訊設備(僅限各部門申請之筆記型電腦等設備，非公司採購之設備嚴禁攜帶至公司使用)，使用人均需填寫 OA 系統之[(CTSFR0070)資訊設備 IP 位址暨行動資訊設備申請單]，經需求單位主管簽核後，向資訊部權責單位提出需求申請。(CTSWI0025 行動資訊設備管理辦法)

10. 使用行動通訊設備必須設定硬碟密碼鎖，無此功能之行動資訊設備則不需設定。(CTSWI0025 行動資訊設備管理辦法)

11. 行動資訊設備若為該單位公用電腦，使用人員必須於歸還前清除個人資料以確保該行動資訊設備之資訊安全。(CTSWI0025 行動資訊設備管理辦法)

12. 未經資訊單位核准，具備連接本公司網路或存取本公司資訊資源能力之資訊設備，在本公司辦公處所使用時，不得再同時連接無線網路(WiFi)、行動網路與撥接網路(Dial-Up)串連公司以外網路。(CTSWI0027 個人電腦與周邊設備管理規範)

13. 敏感資料（如客戶資料）不應儲存於個人電腦。如因執行業需要暫存，於作業完成後應立即移除，如必須留存時，建議使用壓縮軟體來加密封存該敏感資料。((CTSWI0027)個人電腦與周邊設備管理規範）

14. 使用行動通訊設備必須設定硬碟密碼鎖，無此功能之行動資訊設備則不需設定。(CTSWI0025 行動資訊設備管理辦法)

15. 行動資訊設備若為該單位公用電腦，使用人員必須於歸還前清除個人資料以確保該行動資訊設備之資訊安全。(CTSWI0025 行動資訊設備管理辦法)

16. 未經資訊單位核准，具備連接本公司網路或存取本公司資訊資源能力之資訊設備，在本公司辦公處所使用時，不得再同時連接無線網路(WiFi)、行動網路與撥接網路(Dial-Up)串連公司以外網路。(CTSWI0027 個人電腦與周邊設備管理規範)

17. 敏感資料（如客戶資料）不應儲存於個人電腦。如因執行業務需要暫存，於作業完成後應立即移除，如必須留存時，建議使用壓縮軟體來加密封存該敏感資料。((CTSWI0027)個人電腦與周邊設備管理規範）

18. 資料檔案列印時應確認輸出的印表機裝置是否正確，確認無誤後再行列印，取回列印文件或報表時如有發現其他列印資料時，應協助確認該列印資料為何人列印並通知取回，如確認後仍無人認領應協助銷毀該列印資料。

19. 使用電子郵件傳送機敏資料時，需對機密性及敏感性資料加密後再傳送。

20. 避免使用公司電子郵件住址註冊各種網站之會員，以防止收取垃圾郵件及詐騙信件。

21. 嚴禁透過網咖、學校...等公共場所之網路環境使用遠程簽到，以避免遠程簽到登入帳號與密碼遭留存而致他人利用。(CTSWI0039)遠程簽到管理規範

表1　各地區電腦聯絡人員

單　位	電腦連絡人員	電子信箱	駐點分機
總　公　司	符前智	adam.fu@ctbcsec.com	2715 2584
三重分公司	陳威羽	harvey.chen@ctbcsec.com	199
忠孝分公司	陳威羽	harvey.chen@ctbcsec.com	199
永康分公司	李永宏	luhpro@ctbcsec.com	199
文心分公司	李奇峰	clay.le@ctbcsec.com	199
新竹分公司	鄧和榮	helong.den@ctbcsec.com	199
松江分公司	陳威羽	harvey.chen@ctbcsec.com	199
嘉義分公司	李奇峰	clay.le@ctbcsec.com	199
中壢分公司	鄧和榮	helong.den@ctbcsec.com	199
高雄分公司	鄭宗武	jan@ctbcsec.com	199
資　訊　部	張志鴻	cch@ctbcsec.com	2380
資訊安全小組	吳　洲	chou.wu@ctbcsec.com	2390

二、 社交工程演練相關懲處建議：

期間	觸發條件	對應措施及建議懲處方式
一年 (12 個月/次) 區間： Q4 ~ Q3	未開啟任一封郵件者，視為相對安全人員	無須對應
	僅開啟郵件，而未開啟郵件內連結或附件者，視為低風險人員	無須對應
	累計開啟任一封郵件內連結或附件者，視為中風險人員	1. email 通知該員及部門主管、資訊安全長、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數

	累計開啟任兩封郵件內連結或附件者，視為高風險人員	1. email 通知該員及部門主管、資訊安全長、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數 3. 記警告乙次 4. 重新執行資安教育訓練
	累計開啟任三封郵件以上，且皆有開啟郵件內連結或附件者，視為極高風險人員	1. email 通知該員及部門主管、資訊部主管、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數 3. 記警告(含)以上乙次 4. 直屬主管陪同重新執行資安教育訓練

特此提醒同仁收到不尋常的 email 信件，務必提高警覺並依以下建議因應：

1. 同仁可檢視 email 主旨欄，若被標示【外部郵件】，則該 email 係來自外部，而非內部寄件者，請謹慎確認後再開啟。
2. 同仁可檢視 email 主旨欄，若標示【中信銀行郵件】，則該 email 寄件者係來自中信銀行，依此類推。
3. 同仁可檢視 email 主旨是否與工作業務相關，如若與公務無關應直接刪除，勿任意開啟。

伍、參考資料

https://blog.trendmicro.com.tw/?p=86788#more-86788
https://www.ithome.com.tw/news/167184
https://hk.news.yahoo.com/country-agency-ban-deepseek-103537515.html
https://blog.trendmicro.com.tw/?p=77418
https://blog.trendmicro.com.tw/?p=49155
https://moda.gov.tw/press/clarification/4791