教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026051209054545	發佈時間	2026-05-12 09:43:47
事故類型	ANA-攻擊預警	發現時間	2026-05-12 09:43:47
影響等級	中		

[主旨說明:]【攻擊預警】Canvas 供應商 Instructure 遭駭客組織 ShinyHunters 入侵

[內容說明:]

近日國外多所學校通報，攻擊者針對 Canvas 線上教學平台進行帳號盜用與釣魚攻擊，可能透過偽造登入頁面、假冒課程通知信件或第三方外掛程式，誘騙使用者輸入帳號密碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

Canvas 所有產品

[建議措施:]

為避免帳號遭盜用及資料外洩，請使用者提高警覺，並配合以下安全措施：

一、確認登入網址：請透過學校官方入口或書籤登入 Canvas，避免點擊來路不明之郵件連結。

二、勿於可疑頁面輸入帳號密碼：若頁面出現異常登入要求、重新驗證或 MFA 驗證通知，請先確認網址正確性。

三、啟用多因素驗證（MFA）：建議已支援 MFA 功能之使用者儘速啟用，以降低帳號遭盜用風險。

四、留意異常通知：請注意是否有非本人登入紀錄、收到異常驗證碼通知、課程出現不明公告或訊息，帳號自動寄發異常郵件等現象。如發現上述情形，請立即修改密碼並通知資訊單位。

五、避免重複使用密碼並更改密碼：

請勿將 Canvas 密碼與其他網站或系統共用，並建議定期更換密碼，以提升帳號安全性。

如發現帳號遭盜或資料外洩情形，請遵循資通安全事件通報應變及演練辦法之規定，進行通報。

六、有關本次事件處理進度如官網公告。
https://www.instructure.com/incident_update

[參考資料:]
1. https://www.instructure.com/incident_update
2. https://data.dailycal.org/2026-05-07-shiny-hunters
3. https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=12906
4. https://www.ithome.com.tw/news/175580