檔　　號：
保存年限：

財團法人資訊工業策進會　函

地址：106台北市和平東路二段106號11樓
承辦人：李懿修
電　話：(06)3032260#105
電子信箱：ryanyhlee@iii.org.tw

裝

受文者：文藻學校財團法人文藻外語大學

發文日期：中華民國115年6月12日
發文字號：資慧字第1150001089號
速別：普通件
密等及解密條件或保密期限：
附件：1150626_AIx資安工作坊　(XC760004240000000_1150001089A125_ATTACH1.png)

主旨：本會受AIT美國在台協會委託，於中華民國115年6月26日(五)合作辦理「AI x 資安工作坊 III - AI 與網路安全職業與教育：打造數位經濟新世代」專題論壇暨實體工作坊，敬請貴校協助公告周知並鼓勵師生踴躍報名參與，請查照。

訂

說明：

一、本會將辦理「AI x 資安工作坊」系列活動，以臺灣青年及職涯初期產業人士為主要對象，邀集跨國產業專家與各界學術夥伴，以專題論壇結合實作課程形式，引導參與者親身體驗AI技術應用與資安實務。

線

二、活動資訊：

(一)活動名稱：「AI x 資安工作坊 III - AI 與網路安全職業與教育：打造數位經濟新世代」專題論壇暨實體工作坊。

(二)活動時間：中華民國115年6月26日(五)13:30至16:30。

(三)活動地點：資安暨智慧科技研發大樓1樓（第一會議室），地址：臺南市歸仁區歸仁十三路一段6號。

(四)報名期限：自即日起至115年6月22日(一)止。

(五)報名網址：https://ievents.iii.org.tw/EventS.aspx?t=0&id=3303。

(六)語言：全程以中文進行。

(七)備註：完整參與活動者可獲得AIT美國在台協會核發之電子參與證明。

三、敬請協助公告並鼓勵貴校師生踴躍報名參加，如有活動相關問題，請洽本案聯絡人：資策會AI院李先生，電話：（06）30322260#105，電子郵件：ryanyhlee@iii.org.twtw。

正本：文藻學校財團法人文藻外語大學

副本：電子公文交換章 2026/06/12 12:31:02

AI x 資安工作坊 III

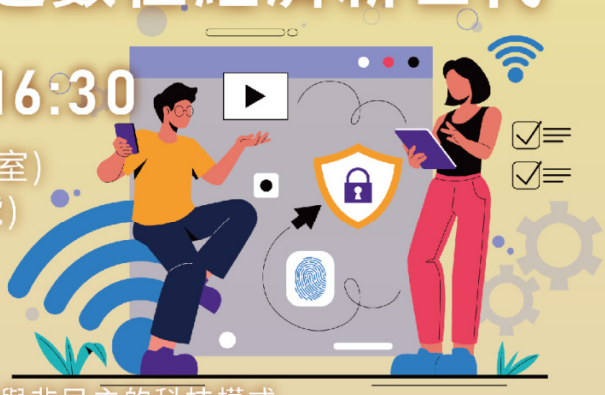
AI 與網路安全職業與教育：打造數位經濟新世代

活動日期 2026.06.26 13:30-16:30

活動地點 資安暨智慧科技研發大樓1樓 (第一會議室)
(地址: 臺南市歸仁區歸仁十三路一段6號)

活動目標 透過跨國專家討論與實作體驗，幫助青少年了解：

1. AI與資安領域的教育與職業發展路徑
2. 美國與台灣在職業技術教育上的發展方向
3. 如何培養數位經濟下的關鍵技能，抵禦強制性與非民主的科技模式



Time	Program	Speaker
13:30-13:35	Opening	
13:35-13:55	尋找魔法石： 在人工智慧時代裡施法(與不施法)的理由	台灣駭客協會 Poren Chiang
13:55-14:15	AI 叢林中的生存法則： 當 AI 開始替您做決定時的因應之道	TWCSA台灣數位安全聯盟 蔡一郎　理事長
14:15-14:20	交流&休息	
14:20-15:20	資安實作工作坊: 釣魚網址偵測與對抗攻擊 **單元 1：社交工程攻擊與釣魚偵測** 探討生活中常見的詐騙與社交工程風險，帶出網址偵測的重要性 **單元 2：特徵工程與模型建置** 將網址轉換為神經網路可讀的特徵向量並建立並認識深度學習架構，完成模型訓練相關前置工作	國立臺北科技大學 魏銷志 副教授兼計網中心主任 助教:陳映璇、胡語庭
15:20-15:30	交流&休息	
15:30-16:30	資安實作工作坊: 釣魚網址偵測與對抗攻擊 **單元 3：模型效能評估指標** 模型訓練完成後，運用指標進行效能評估。觀察 AI 模型在未知測試集上標記釣魚與惡意網址的效能 **單元 4：模型對抗式攻擊實作** 說明梯度上升攻擊原理，透過微調輸入特徵生成對抗樣本，觀察如何成功欺騙模型發生誤判，藉此強化資安攻防思維	國立臺北科技大學 魏銷志 副教授兼計網中心主任 助教:陳映璇、胡語庭
16:30-	賦歸	

以上活動規劃內容，由主辦單位依據實際情況調整，並保有最終釋義權；如遇不可抗拒之因素，主辦單位保留修訂及取消之權利。

主辦單位 | 美國在台協會 American Institute in Taiwan | American Spaces | 執行單位 | 財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY | 協辦單位 | 國立高雄科技大學 | 國立臺北科技大學 TAIPEI TECH