

114 年教育體系資安專業課程訓練-資通安全概論

壹、課程簡介

本講座將與學員介紹大語言模型可能帶來的資訊安全危機，強化學員的資安意識。課程首先講解大語言模型為何產生幻覺、駭客使用什麼方法繞過安全限制對使用者進行攻擊，讓學員了解大語言模型資安問題的產生原因。接續將講解使用者可能被洩漏的隱私資訊，以及如何防範，讓學員了解此資安危機可能造成的損失。最後會介紹非官方模型所帶來的威脅，培養學員的風險評估與識別能力。

貳、辦理單位

指導單位：教育部

主辦單位：逢甲大學資通安全研究中心(ICSRC)

參、參與對象

1. 以各縣市教育網路中心、高中以下資安相關負責人為優先。
2. 臺灣學術網路區域網路中心、大專院校資安相關負責人員。

肆、課程時間

114 年 10 月 31 日(五) 13:00 - 16:00

伍、課程資訊及大綱

主題：資通安全概論：大語言模型的資安危機

講師：林子婷

大綱：

1. 幻覺與越獄
2. 隱私洩漏
3. 非官方模型威脅

陸、課程地點：

逢甲大學 資訊電機館 B15 電腦教室，如有異動將由主辦單位另行通知。

柒、報名相關資訊：

1. 報名日期 114 年 10 月 01 日中午 12:00 起至 114 年 10 月 24 日下午 18:00 止
(名額限制 20 人，額滿提前結束)。
2. 提供 3 小時公務人員研習時數 或 教師研習時數。
3. 報名網址：<https://forms.gle/LMQzBQk4tZJUdCXH9>
4. 關於校內停車事宜，由於校內平面車位不足，請與會者前往逢甲大學收費停車場停車。
5. 主辦單位保有最終修改、變更、活動解釋及取消本活動之權利，若有相關異動將會另行發信通知。

逢甲大學交通路線圖

地址：台中市西屯區文華路100號



※火車：

- 台中火車站請搭西部幹線山線。
- 火車站轉公車：從火車站轉車請搭統聯客運 25 號、37 號；中台灣客運 25 號；台中客運公車 8 號、33 號、35 號；全航客運 5 號。

※台灣高鐵：

- 至高鐵台中站六號出口，12 號公車月台，搭乘高鐵快捷公車和欣客運--僑光線，逢甲大學站下車。
- 高鐵台中站，搭計程車經中彰快速道路至逢甲大學約 25 分鐘，約 300 元。

※客運：

- 搭統聯客運巴士，請在統聯客運中港轉運站下車，換搭 79 線公車。
- 台中市區公車台中客運 33、35 路或統聯客運 25、37、125 線公車。
- 搭其他客運巴士，請在台中市中港路朝馬站下車，可轉搭計程車約 5-10 分鐘至本校。

※中山高速公路(國道一號)：

- 中港交流道：178.6K 處下(台中 | 沙鹿)交流道，往台中市方向，進中港路，過黎明路橋，左轉進河南路，左轉進福星路，至逢甲路右轉進逢甲大學。
- 大雅交流道：172.4K 處下(台中 | 大雅)交流道，往台中市方向，進中清路，右轉進文心路三段，右轉進河南路，右轉進福星路，至逢甲路右轉進逢甲大學。

※福爾摩沙高速公路(國道三號)：

- 快官交流道：202.1k 處下台中快官交流道接台 74 線省道，在 10.2k 處下西屯路交流道，往台中市方向，左轉進逢甲路直進逢甲大學

逢甲大學停車示意圖

■ 汽車停車場 ■ 機車停車場 ■ 自行車停車場 ■ 週邊停車場

