

資安教育訓練線上課程操作手冊

※請使用公務信箱登入後點網址進行線上課程及評量

每年一般使用者與主管人員至少須接受 3 小時資通安全通識教育訓練課程

說明：為提升本市教師資訊安全知識及強化資安觀念，並依數位發展部資通安全責任等級分級辦法應辦事項規定，每年一般使用者與主管人員（組織編制表內人員，或得接觸、使用機關資通系統或服務之各類人員）應接受 3 小時資通安全通識教育訓練課程，特辦旨揭研習。

二、本次研習採錄製影片至雲端資料夾(<https://s.tyc.edu.tw/RJoZoe>)自行瀏

覽，並於課後填寫評量(<https://forms.gle/oRE6Gr9WfZ6Fu4Sj6>)，其資訊如下：

(一)參加對象：本市各級**學校之校長、主任及教職員**。

(二)研習時數：參與本次研習並**填寫評量者核予 3 小時**

(三)**觀看影片及填寫評量時請使用@ms.tyc.edu.tw 網域之帳號**，評量截止時間至

114 年 12 月 12 日 止，未填寫評量者無法核予研習時數。

1.登入「公務信箱 Gmail」

公務信箱 Gmail 登入方式(**與平常使用 Gmail 方式一樣只是帳密有固定規範**)

帳號格式：**單一認證平台的帳號@ms.tyc.edu.tw**

密碼格式：**單一認證平台的密碼**



▲以一般 Gmail 方式登入

▲快速傳送門【[網址連結](#)】

3.若發現公務信箱**尚未啟用**或**密碼忘記**可自行手動操作，操作如下：

登入單一認證授權平台→辦公室自動化系統→公務信箱啟用/同步



Gmail教育公務信箱啟用

Hi, 陳XX ~ 您好
歡迎使用桃園市教育公務信箱，請進行啟用程序以使用您的公務信箱。

- 本功能可啟用Gmail公務信箱或同步公務信箱密碼，您的公務信箱為「XXX@ms.tyc.edu.tw」，請點選「**啟用信箱或同步密碼**」按鈕以啟用信箱或同步信箱密碼。

啟用信箱或同步密碼

【資訊安全】

114 年度本市所屬學校資訊安全教育訓練課程-網路安全與新興數位威脅之應對課後評量參考答案

✓ 新興數位威脅中，AI生成的深偽 (Deepfake) 技術可能被用於下列哪項 *20/20
攻擊情境？

- ☒ 偽造高階主管影像進行財務詐騙。 ✓
- ☐ 暴力破解網站帳號密碼。
- ☐ 快速定位系統漏洞進行攻擊。
- ☐ 利用IoT裝置發動大規模DDoS攻擊。

✓ 關於應對新興數位威脅，零信任 (Zero Trust) 架構的推廣主要解決下列哪項問題？ *20/20

- ☐ 降低硬體維護成本。
- ☒ 防範內外部未經驗證的存取行為。 ✓
- ☐ 提升網站載入速度。
- ☐ 簡化員工遠端辦公流程。

✓ 「供應鏈攻擊」最常利用企業的下列哪一種安全弱點作為入侵途徑？ * 20/20

- ☐ 最終用戶端點防護失效
- ☒ 委外廠商或第三方服務提供者的安全漏洞 ✓
- ☐ 應用程式授權錯誤配置
- ☐ 備份機制頻率不足

✓ 下列哪一種網路攻擊手法最常利用分散式節點發起大量請求，導致目標伺服器資源耗盡而無法提供正常服務？ *20/20

- ☐ SQL注入攻擊。
- ☐ 中間人攻擊。
- ☐ 跨網站指令碼攻擊。
- ☒ 分散式阻斷服務攻擊。



✓ 2024年過後，可以預見下列哪一種威脅將會更加突出？ * 20/20

- ☐ 傳統的病毒和蠕蟲感染。
- ☐ 針對過時作業系統和軟體的漏洞利用。
- ☒ 結合物聯網 (IoT) 設備漏洞的複合式網路攻擊。
- ☐ 大規模的垃圾郵件和網路釣魚郵件。

