🎓🚀 **資安超新星，從這張 Google 證書開始！**

想進入科技業、走資安這條高薪又搶手的道路嗎？

Google Cybersecurity Certification 是你邁向資安職涯的第一道大門！

計畫亮點：

- 無需經驗，跨入資安領域
- 由 Google 資安專家打造的全面性資訊安全培訓課程，因應趨勢新增 AI 相關課程，全方位強化技能！
- 取得 Google 資安專業證書，提升工作競爭力！

💡 零經驗也沒關係！無論你是理科咖、程式新手還是對資訊安全有興趣的跨領域同學，只要願意學、跟著課程走，就能掌握實戰技能，打造職場起跑線優勢！

📈資安業界超缺人，學起來就對了！

🎓 學生專屬福利，彈性學習、超值收穫！

💥敢想、敢學、敢守護

從你開始，為數位世界加上安全鎖 🔐

🌟還等什麼？現在就讓你自己，站上資訊防線的第一線！

報名網址：**https://forms.gle/Zrpvbij6jmRbpLTGA**

📌 完成這張證書後，你將有機會投身以下熱門職缺：

1. **資安分析師（Cybersecurity Analyst）**

   負責監控網路與系統安全狀況，分析資安事件並提出應對建議，是本證照最直接對應的職務。

2. **資安工程師（Security Engineer）**

   專注於建置、維護與強化資訊系統的安全防護，包括入侵偵測系統、防火牆設定與漏洞修補。

3. **SOC 分析人員（Security Operations Center Analyst）**

   在資安監控中心執勤，負責即時處理資安警示與可疑活動，撰寫事件報告並提供事件回應建議。

4. **IT 支援專員（IT Support Specialist with Security Focus）**

   協助企業員工解決技術問題，同時維護基礎資訊環境的安全性，包含權限設定、設備管理等。

5. 風險與合規分析師（Risk & Compliance Analyst）

   針對企業資安政策、資料保護與法規遵循進行稽核與改善建議。

6. 入門資安顧問（Junior Security Consultant）

   協助資安顧問團隊進行環境評估、弱點掃描與企業資安提案。

7. 雲端安全助理（Cloud Security Associate）

   協助監控與維護雲端平台安全，包括帳號控制、雲端資源存取與設定最佳化。

第三梯次「Google 資安人才培育計畫-課程說明」

★計畫說明：

近來隨著數位經濟、金融科技、AI 快速發展，資訊安全人才需求增加，教育部產學連結執行辦公室-國立臺北科技大學攜手Google 合作辦理「資安人才培育計畫」，免費提供「Google 資安專業證書」的課程，讓台灣加速培育出更多資安專家。

Google Cybersecurity 專業證書是由 Google 的資訊安全專家建立及負責授課，旨在幫助學生培養基礎資訊安全工作所需的高需求技能。這項線上訓練計畫沒有經驗方面的要求，並可在 3 個月內完成。在過程中，學生將瞭解如何辨別常見的風險、威脅和安全漏洞並減輕其影響。

★學員報名注意事項：

國內各大專校院之在學學生、且TOEIC測驗加總需要達550分以上者(或

具有其他同等能力證明資格者)。主辦單位依報名順序擇學員500人正取，另備取學員200人。(課程報名網址：

https://forms.gle/Zrpvbij6jmRbpLTGA)

★學員上課注意事項及成果追蹤說明：

1.臺北科大產學連結執行辦公室將於後台管理資料，統計成果，學員註冊課程後的14天內，若要主動取消課程者，請寄email通知後台管理人員(linda70329@gmail.com、clcheng@ntut.edu.tw)，惟學員若連續14天未上線且未完成一個課程單元，系統將直接取消該帳號上課資格。

2.參加課程之學員，需同意主辦單位以電話、問卷或Email追蹤修畢之成果。

★Google Cybersecurity Certificate 註冊說明：

1.報名學員採實名制。

2.線上課程全部採英文教學，報名學員建議具備一定英文程度(聽、讀流利)。

3.於收到參加課程Email的第3個日曆天中午12:00以前，點選教學平台Email提供之課程鏈接，進行註冊。

4.請於114年9月30日下午17:00前完成所有課程，系統將於9月30日下午18:00直接取消該帳號的上課資格。

5.課程中測驗次數說明：

測驗次數不設上限，惟每24小時內最多可測驗3次，超過次數後須等待

8小時後方可再次測驗。請同學務必最晚於9月29日前完成相關測驗安排。

★課程內容:

《九大類線上實作課程大綱》

(1) 網路安全基礎:網路安全的演變、防範威脅、風險和漏洞、網路安全工具和程　式語言。

(2) 安全風險管理:安全領域、安全框架和控制措施、探索網路安全工具、使用操作手冊應對事件。

(3) 網路和網路安全:網路架構、網路操作、防範網路入侵、安全強化。

(4) Linux 及 SQL工具:操作系統概論、Linux 操作系統、Bash shell 中的 Linux 命令、資料庫與 SQL。

(5) 資訊資產、威脅及漏洞:資產安全概論、保護組織資產、 系統中的漏洞、對資產安全的威脅。

(6)偵測與回應:偵測與事件回應概論、網路監控與分析、事件調查與回應、使用 IDS 和 SIEM 工具分析網路流量和日誌。

(7) Python自動化任務: Python 概論、編寫高效的 Python 程式碼、處理字串和列表、Python 實踐應用。

(8)職涯準備:保護資料並通報事件、上呈通報事件、有效溝通以影響利害關係人、與網路安全社群互動、尋找並申請網路安全工作。

(9)運用 AI 加速求職:掌握如何使用 Gemini 建立亮眼的履歷與求職計畫, 並運用 NotebookLM 和 Gemini Live 準備面試。

教學目的:

教導學員如何識別常見的資訊安全風險、威脅和漏洞，以及 緩解這些風險的技術。

★培訓課程模式:

九大類模組課程，以英文為授課語言的線上學習課程。

★課程平台:

透過臺北科大產學連結執行辦公室完成報名，學員資格符合及發送註冊鏈接，課程目前開發放置於 Coursera 平台上。

適合學員:

適用於任何想要學習資訊安全知識領域的學員;學習前不需要任何的相關知識或是經驗。只要擁有解決問題的興趣與幫助他人的熱誠。

完成 Google 資訊安全職業認證的學員將學習到:

1.了解資訊安全的重要性及其對公司的影響。

2.常見資訊安全風險、威脅和漏洞的鑑別與解決的技術。

3.獲得Python、Linux 和SQL 的實務經驗。

4 .使用資訊安全管理工具(SIEM) 、網路入侵檢測系統 (IDS)及網路數據

分析包 (packet sniffing) 來保護網路、設 備、人員和數據免受未經授權的訪問和網路攻擊

★聯繫窗口

1.教育部產學連結執行辦公室 - 國立臺北科技大學 黃專員

電話：**(02)2771-2171 分機 6023**

Email：receivable0308@mail.ntut.edu.tw

2.教育部產學連結執行辦公室 - 國立臺北科技大學 鄭經理

電話：**(02)2771-2171 分機 6012**

Email：clcheng@ntut.edu.tw

3. 國立臺北科技大學資訊工程系 呂同學

Email：linda70329@gmail.com