
K-12 教師研習

教師資訊安全基礎課程

國小至高中 | 帳號密碼、單一簽入、網路防護、師生隱私



新北市政府
Education Department,
New Taipei City Government

教育局

研習議程

單元	主題
1	開場：為什麼老師容易成為目標？
2	帳號密碼的風險
3	單一簽入（SSO）的優點
4	保護網路資訊安全的措施
5	學生的隱私權
6	教師自身的隱私權
7	臺灣本地案例與法規
8	總結與行動清單

為什麼老師容易成為目標？

學校常被視為資安防護較弱的單位

使用者多且行為複雜

使用者身分複雜，數量龐大且流動性高，資安意識參差不齊，設備管理困難。

系統架構與環境的先天限制

校園網路環境高度開放，老舊系統與孤兒網站眾多，物聯網（IoT）設備爆發。

資源、預算與人才短缺

資安預算與編制嚴重不足，缺乏專職的資安專家，多由教師兼任，難以應付日新月異的駭客攻擊。

為什麼老師容易成為目標？

老師的帳號權限高，手上的個資多

個資多

學生成績、家庭資料、輔導紀錄、健康資料，都在校務行政系統裡面。

波及廣

老師帳號能存取的系統、數位學習資源多，被盜後影響整個班級甚至全校。

有法規

學校屬公務機關，需遵循《資通安全管理法》與《個人資料保護法》。

檢查自己的電子郵件地址、電話號碼或密碼是否曾在網路資安事件（Data Breach）中外洩
[Have I Been Pwned](#)

02 帳號密碼的風險

多數帳號被盜，源自弱密碼與重複使用

- 密碼太簡單，例如生日、123456
- 多個系統共用同一組密碼
- 密碼寫在便利貼，貼在螢幕旁
- 釣魚信或假登入頁騙取帳密
- 共用帳號，例如辦公室共用電腦登入、志工共用系統帳號密碼、代課教師與原任課教師共用帳號密碼

攻擊手法與好習慣

常用攻擊手法

- 暴力破解、字典攻擊
- 撞庫攻擊：拿大量外洩的密碼去試其他網站
- 釣魚：假信件、假登入頁

建立好習慣

- 使用長密碼或密語（passphrase）
- 使用密碼管理器
- 啟用多因子驗證（MFA）
- 公共電腦要登出
- 離開座位即鎖定螢幕系統與軟體定期更新，
避免使用來路不明的 USB
- 備份重要資料(3-2-1 備份原則)

一組外洩的密碼，被拿去試遍其他服務

撞庫攻擊：某網站外洩的帳密，被拿去嘗試登入其他服務，是全球常見手法。

遠距教學：2020–2021 年，各國都有線上課堂連結外流、陌生人闖入播放不當內容的事件，臺灣疫情停課期間也有類似報導。

03 單一簽入 (SSO)

登入一次，用多個系統

只記一組強密碼

減少重複使用與外洩的風險。

集中管理權限

到職、離職、調動時，同步開通或停用。

集中防護與稽核

可統一啟用兩步驟驗證與登入紀錄稽核。

減少忘記密碼

降低客服與行政負擔。

03 單一簽入 (SSO)

帳號一旦被盜影響大，要有配套

風險與配套

- 單一帳號被盜，波及多個系統
- 搭配兩步驟驗證
- 權限最小化原則
- 需要異常登入偵測

使用情境

- 新北市單一簽入
- 教育部教育雲單一身分驗證 (OpenID)

案例對照

- 離職教師帳號未停用而被濫用，是常見的稽核缺失
- 某些學校發生大量異常申請 Adobe 軟體授權的狀況

案例 | 新北市校務行政系統資安防護措施

安全措施項目	教師（教職員工 / 非學生身分）	學生
雙因子驗證 (2FA)	強制啟用，登入時需經由手機簡訊、電子郵件或校園通 APP 進行第二階段驗證。	未強制啟用（雙因子驗證僅針對非學生身分使用者）。
預設密碼修改期限	自設定起 3 日內未修改，系統將限制登入。	自設定起 3 日內未修改，系統將限制登入。
自行重設密碼前提	需預先完成驗證備用信箱或行動電話才能使用「忘記密碼」功能。	需預先完成驗證備用信箱或行動電話才能使用「忘記密碼」功能。
無法自行重設時之還原管道	請學校資訊業務承辦人或主要學校系統管理人員協助還原為預設密碼。	由班級導師協助還原為預設密碼，或由學生帳號監護人使用「忘記密碼」功能處理。
未完成驗證之緩衝機制	提供 3 次「直接登入」機會供登入後補做聯繫資訊驗證。	不適用（未強制雙因子驗證）。
信任裝置設定	簡訊與電郵驗證可勾選信任此裝置 30 天以略過二步驟驗證。	不適用（未強制雙因子驗證）。
單一簽入 (SSO) 密碼變更	需回到校務行政系統源頭執行變更或重設密碼。	需回到校務行政系統源頭執行變更或重設密碼。

多數攻擊從一封信或過期軟體開始

電子郵件與釣魚

- 檢查寄件者與連結網址
- 留意是否催促操作
- 不隨意開啟附件

裝置與軟體

- 作業系統與軟體定期更新
- 安裝防毒軟體
- 不使用來路不明的軟體

保護資料、備份，並知道向誰通報

網路與資料

- 公共 Wi-Fi 不處理敏感資料
- 重要資料定期備份，遵循 3-2-1 原則
- 隨身碟加密，或避免存放個資
- 防範勒索軟體：離線備份、不亂點連結

通報

發現異常時，立即向校內資訊組通報。

學校被勒索軟體攻擊，可能整個學區停課

2020 年，美國馬里蘭州巴爾的摩郡公立學校遭勒索軟體攻擊，學校停課。

2022 年，洛杉磯聯合學區（LAUSD）遭勒索軟體攻擊並外洩資料。

學生個資受法律保護，日常教學要留意

個資範圍

姓名、照片、成績、家庭背景、輔導與特教資料。

老師的日常注意事項

- 班級群組與社群貼文，不隨意公開學生照片與名單
- 成績與名單不以明碼傳送，也不公開張貼
- 使用第三方教學軟體前，確認授權與家長同意
- 螢幕投影時，注意是否露出他人資料

05 學生的隱私權

不同學段，隱私重點不同

學段	重點
國小	家長同意與監護關係更重要
國中、高中	學生本身也有隱私期待，輔導與感情相關事件更需保密

合作廠商與日常貼文，都可能外洩學生資料

Blackbaud（2020 年）：教育服務商資安事件，影響多所學校與機構的資料。

PowerSchool（2024 年底）：資料外洩，涉及大量學生與教職員資料。

日常貼文：老師在社群貼出含學生個資的班級照片或成績單，是常見的個資爭議。

老師的個資同樣受保護

- 個資範圍：住址、電話、身分證字號、薪資
- 社群媒體：公私帳號分開，避免與學生私下用個人帳號聯絡
- 學校監控與錄影，有告知義務
- 校內系統是否蒐集老師個資，及蒐集目的

法規與資源

法規

- 《個人資料保護法》：蒐集、處理、利用需有特定目的與告知
- 《資通安全管理法》：公務機關資安責任與通報

案例

- 學校或教育系統的個資外洩新聞
- 學校網站遭入侵或被置換頁面

教育體系資源

- 新北市資訊業務入口網-資訊安全專區
- 新北市政府資訊安全資源

回去後做到這五件事

1. 使用強密碼，並啟用兩步驟驗證
2. 不亂點連結與附件
3. 學生個資不公開、不亂傳
4. 資料定期備份
5. 發現異常立即通報

Q&A 交流與討論

共同守護校園資安新未來

謝謝各位老師，歡迎提出在校園遇到的資安情境。