



## 有關網上視像會議應用程式資訊保安建議

德愛中學潘家興老師

就早前有關 Zoom 實時網上授課應用程式/平台的安全問題，我綜合了網上資料，並提供建議給教師參考。

如何在 Zoom 作保安設定安全地進行網上教學 (inside.com.tw, 2020)：

1. 使用 Zoom 進行會議時，請務必啟用點對點加密，因此請勿關閉預設功能。
2. 建議從 Zoom 官方版網頁下載軟體，並且隨時保持讓程式更新到最新版本。
3. 在 Zoom 系統中註冊專屬的帳號，並且設定未曾使用過的專屬密碼，請勿使用以既有 Facebook 或 Google 帳號登入的方式進行認證。
4. 進行會議時，請務必設定會議密碼（建議每場會議均不一樣），以防不相關人士擅入；同時，會議主持人的密碼，也須避免重複使用，並須注意密碼設置的強度。
5. 邀請與會者時，會議室的連結及會議密碼不要以同一封電郵送出，如果是重要的會議，會議密碼須採用其他的通訊方法告知，例如電話簡訊或 WhatsApp 等。
6. 在個人的電腦作業系統中，另設一個一般權限的使用者帳號，並使用這個使用者帳號去參加 Zoom 會議，等會議結束後，再切換為原本的使用者帳號。
7. 無論使用任何實時網上授課應用程式，都應注意以上各項保安設定。

### 參考資料：

- Verge, T. (2019, 7 8). Serious Zoom security flaw could let websites hijack Mac cameras. Retrieved from <https://www.theverge.com/2019/7/8/20687014/zoom-security-flaw-video-conference-websites-hijack-mac-cameras>
- unwire.hk. (2020, 3 28). Zoom 更新 iOS App 不再向 Facebook 分享數據. Retrieved from <https://unwire.hk/2020/03/28/zoom-ios-app-stops-sending-facebook-data/software/ios-app/>
- inside.com.tw. (2020, 3 27). 有關 Zoom 的資安疑慮與建議. Retrieved from <https://www.inside.com.tw/article/19347-Security-concerns-and-suggestions-about-Zoom>