



ZOOM
應用程式
使用建議

01 使用最新版本的
Zoom 軟件和保安軟件

02 提防任何不明的連結

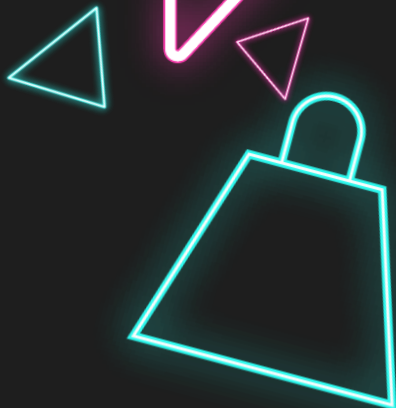
03 切勿在課堂期間分享
機密資訊或不合當資
訊

04 使用指定的顯示名稱

05 小心保護你的Zoom
帳戶及留心可疑的帳
戶活動


01 使用最新版本的 Zoom 軟件和保安軟件

- 只在官方網站或官方應用程式商店下載軟件
- 經常保持ZOOM軟件至最新版本
- 經常更新操作系統（包括桌面電腦及流動裝置）
- 安裝防毒軟件及保持更新




02

提防任何不明的 連結



○ 不要點擊任何可疑的連結



03 切勿在課堂期間 分享機密或不合 當資訊



在課堂期間，應避免分享或
討論機密資料或不合當訊息

04 使用指定的顯示名稱

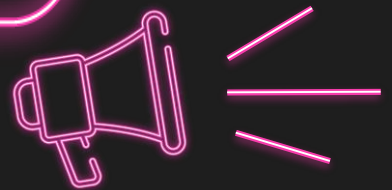
避免使用誤導性名稱或網上暱稱，把名稱改為班別、學號、姓名 (例如：1A01 陳大文)，讓老師更容易識別參與的同學



05

小心保護你的 Zoom 帳戶及留心 可疑的帳戶活動

- 應設立一個高強度的帳戶密碼
- 若發現可疑情況，請登出所有 Zoom 用戶端（如遺失電腦或手機，應立即登出所有用戶端，並更改登入密碼）
- 切勿隨意分享或公開會議ID和密碼



參考資料

1. HKCERT <建議10招保障 Zoom 網上會議安全>
https://www.hkcert.org/my_url/zh/blog/20040201
2. 個人資料私隱專員公署 <Zoom的資料保安事故>
https://www.pcpd.org.hk/tc_chi/media/media_statements/press_20200401.html