公務機密宣導

遠距、居家辦公的
資安防護重點

遠端、居家辦公的資安防護重點

隨著分流辦公、居家辦公形式興起，有許多實體會議改以線上會議方式辦理，遠端視訊會議(video-teleconferencing,VTC)相關系統的使用量與日遽增的同時，亦產生相關資安議題。

身為遠端視訊會議的使用者，我們該如何做好資安防護呢？

針對「**遠端視訊會議**」和「**居家辦公**」，以下有數點資安防護重點提醒：

遠端視訊會議的資安防護重點

1、選用無資通安全疑慮的視訊會議軟體

選用遠距會議軟體時，需考量其安全性，避免使用有資安漏洞和疑慮的軟體，例如 ZOOM；而應以國內產品及共同供應契約所列品項為優先，目前公部門常使用且相對安全之會議視訊軟體有Google Meet、Hangout、Microsoft Teams、Cisco Webex等。

2、選擇可信賴的下載軟體管道

在可信賴的官方網站或app store下載軟體，避免安裝到含有惡意程式的偽冒軟體或APP。

3、謹慎確認會議邀請與連結

來路不明的會議邀請或連結，極有可能是惡意連結，請勿點選，以免受駭。

遠端視訊會議的資安防護重點

4、限制會議參與者

建議所有的會議都設定密碼限制，並由會議發起人於會議開始前確認參與成員的身分。

5、避免在公開社群分享會議連結

請將連結直接提供給與會者，最大限度地避免不相關人員得知會議、甚至潛入竊取機密內容。

6、謹慎使用螢幕共享的功能

會議中若需使用螢幕共享的功能，請限制僅有經指定之人士才可使用並共享。

遠端視訊會議的資安防護重點

7、更新至最新的視訊會議軟體版本

軟體會因應各種資安漏洞進行修補更新，請記得隨時更新到最新版本。

8、確保使用設備的安全性

使用者參與線上視訊會議所使用的資訊設備以及網路連線方式，皆須符合各機關適用之資安法規及所訂定之資安標準（如僅能使用限定之資訊設備、不使用公開、免費之網路連線等）。

居家辦公的資安防護重點

1、時時保持對於社交工程、不明軟體之警覺

隨時對惡意郵件或軟體保持警覺心，看見有疑慮的郵件或連結，請勿點擊。電子郵件應取消預覽，預設以純文字讀取。來路不明之電子郵件勿輕易開啟、點選內容連結或下載其附件；非必要閱讀之郵件則應逕行刪除。如遇可能的資安問題，請即時警示相關人員進行確認與處理。

2、使用安全的網路設備

網路連接方面，盡量不要使用公共Wi-Fi連接公司或機關網路，或公共電腦登入公司或機關系統，必要時可使用手機熱點或透過VPN連接網際網路，以免被側錄或竄改等。連線時，確認取得之內部網路或網際網路的IP位址是否正確無誤；若在公共區域工作時，請將電腦的藍牙等非必要連線管道關閉，可避免有心人士透過該管道攻擊個人裝置。

居家辦公的資安防護重點

3、避免被竊取資訊的可能

請將裝置設定為閒置時自動鎖定。線上會議結束後，務必將相關設備關閉（如麥克風、視訊鏡頭）。可以為個人筆電安裝螢幕防窺片，或離開電腦時立即設定螢幕保護程式並鎖定。同時，設備請盡量不外借予其他人員接觸使用。重要檔案定期備份保存，以避免資料遺失或遭勒索。

4、及時更新以避免漏洞

及時更新作業系統與所使用之各項應用軟體的版本。設備上請安裝與定期更新正版防毒軟體，並定期掃描，防止駭客利用病毒程式入侵並竊取個人資料。

居家辦公的資安防護重點

5、使用強密碼

設定密碼時，請使用具有足夠長度與複雜度之強密碼，混合大小寫英文字母、數字及特殊符號，密碼亦應無明顯含義，建議亦不使用個人生日、電話等易破解之資訊，並請記得定期更新。

6、機密檔案應加密

因業務保有機密性、敏感性檔案者，應加強安全保護措施，如進行加密。

7、帳號密碼應妥善收存

不得將識別碼或帳號密碼直接張貼於個人電腦、螢幕上、或桌面上等容易洩漏之場所。

資料來源：

1.台灣電腦網路危機處理暨協調中心-遠距辦公資安小錦囊-遠距會議篇

https://www.twcert.org.tw/tw/cp-142-3528-62838-1.html

2.台灣電腦網路危機處理暨協調中心-遠距辦公資安小錦囊-個人篇

https://www.twcert.org.tw/tw/cp-142-3509-bed4a-1.html

3. 臺東縣政府政風處-【110年度資訊安全及公務機密維護線上宣導】

https://ethics.taitung.gov.tw/News_Content.aspx?n=13538&s=100923

——花蓮縣政府政風處關心您！