

遠距辦公資安小錦囊-個人篇



遠距辦公資安小錦囊 個人篇



時時保持警覺

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。如遇可能的資安問題即時警示相關人員進行確認與處理。



避免被竊取資訊的可能

設定裝置閒置時鎖定並進行磁碟資訊加密，線上會議結束後，務必將相關設備關閉(ex:麥克風、視訊鏡頭)。



使用安全的網路設備

使用安全的家用網路以及無已知漏洞的網路連線設備。



及時更新軟體避免漏洞



及時更新使用之系統與各應用軟體的版本。

使用強密碼

相關密碼設定使用強密碼，含英文大小寫數字，建議不使用生日、電話等易破解之資訊作為密碼。



官網：
<https://twcert.org.tw/>



FB：
台灣電腦網路危機處理暨協調中心
- TWCERT/CC



E-MAIL：
twcert@cert.org.tw

近期因疫情影響，企業開始實施或模擬在家辦公的應變措施，以下為員工在家遠距工作指南：

1、時時保持警覺

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。如遇可能的資安問題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

使用安全的家用網路以及無已知漏洞的網路連線設備。

3、避免被竊取資訊的可能

設定裝置閒置時鎖定並進行磁碟資訊加密，線上會議結束後，務必將相關設備關閉(ex: 麥克風、視訊鏡頭)。

4、及時更新軟體避免漏洞

及時更新使用之系統與各應用軟體的版本。

5、使用強密碼

相關密碼設定使用強密碼，含英文大小寫數字，建議不使用生日、電話等易破解之資訊作為密碼。

文摘自：台灣電腦網路危機處理暨協調中心網站