資訊安全
Information Security

侯閔馨 0939-825-875
minhsin.hou@joyyoung.com.t

2021.09

目　錄

這些年還有哪些威脅再發生?

新聞

鋼鐵大廠中鴻備份系統遭到病毒攻擊，駭客留下勒索訊息

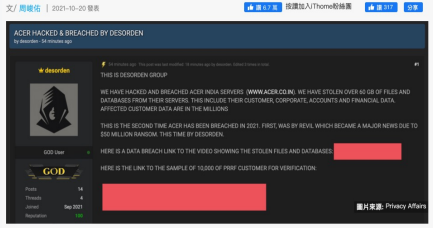
中鴻鋼鐵於股市公開資訊觀測站發布重大訊息，該公司的資料備份伺服器遭到攻擊，他們在發現攻擊跡象時即啟動防禦機制因應

新聞

資安一周第169期：技嘉驚傳二度遭勒索軟體駭客攻擊。車燈大廠帝寶遭遇資安事件

新聞

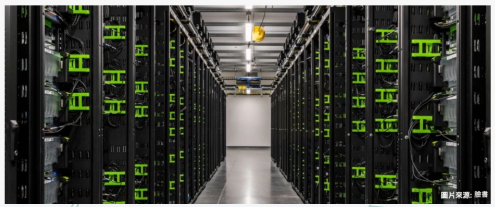
資安一周第168期：宏碁驚傳資料外洩。TWCERT/CC設立勒索軟體防護專區

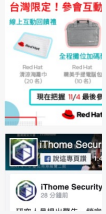


新聞

臉書公布大當機始末報告：日常維護出錯所引發的骨牌效應

臉書工程師在例行性維護時發布了錯誤的命令，但命令權核工具含有具蟲而沒能阻止錯誤命令執行的情況下，先導致臉書全球骨幹網路斷線，接著DNS伺服器關閉BGP宣告，讓臉書在全球網路上消失，進而引發臉書內網全斷、內部工具無法使用的骨牌式災難





新聞

GriftHorse感染千萬臺Android裝置，影響臺灣等70多國用戶

根據資安廠商Zimperium的研判，GriftHorse是今年他們發現覆蓋範圍最大的惡意程式活動，採用複雜的架構及不重覆使用的網域來躲避偵測及封鎖，且過去9個月來完全沒有資安業者發現GriftHorse的存在

新聞

日前宏碁印度分公司與臺灣總公司遭攻擊，該公司發布重大訊息證實，但細節並未說明

日前駭客組織Desorden接連宣稱竊取宏碁印度網站的客戶資料60GB，以及入侵宏碁臺灣總公司伺服器，取得國內員工個資與產品資訊，今日宏碁發布相關重大訊息證實該駭客組織後續也攻擊了臺灣系統。

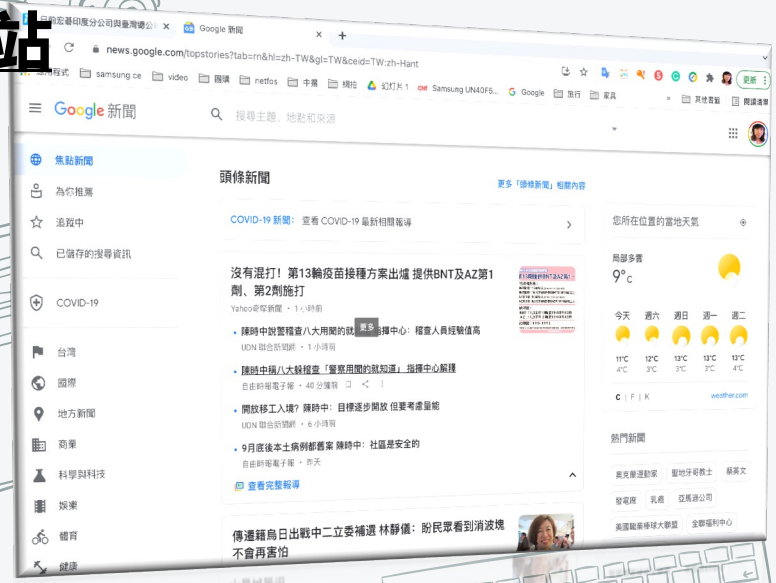
如果有一天，
成為資安事件的主角，
你會怎麼做?

基礎資訊知識

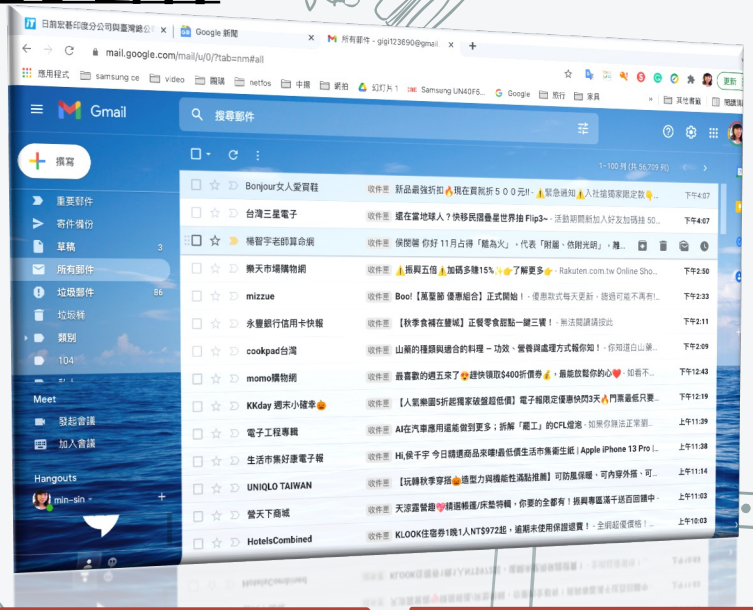
01.病毒怎麼來?

常見來源

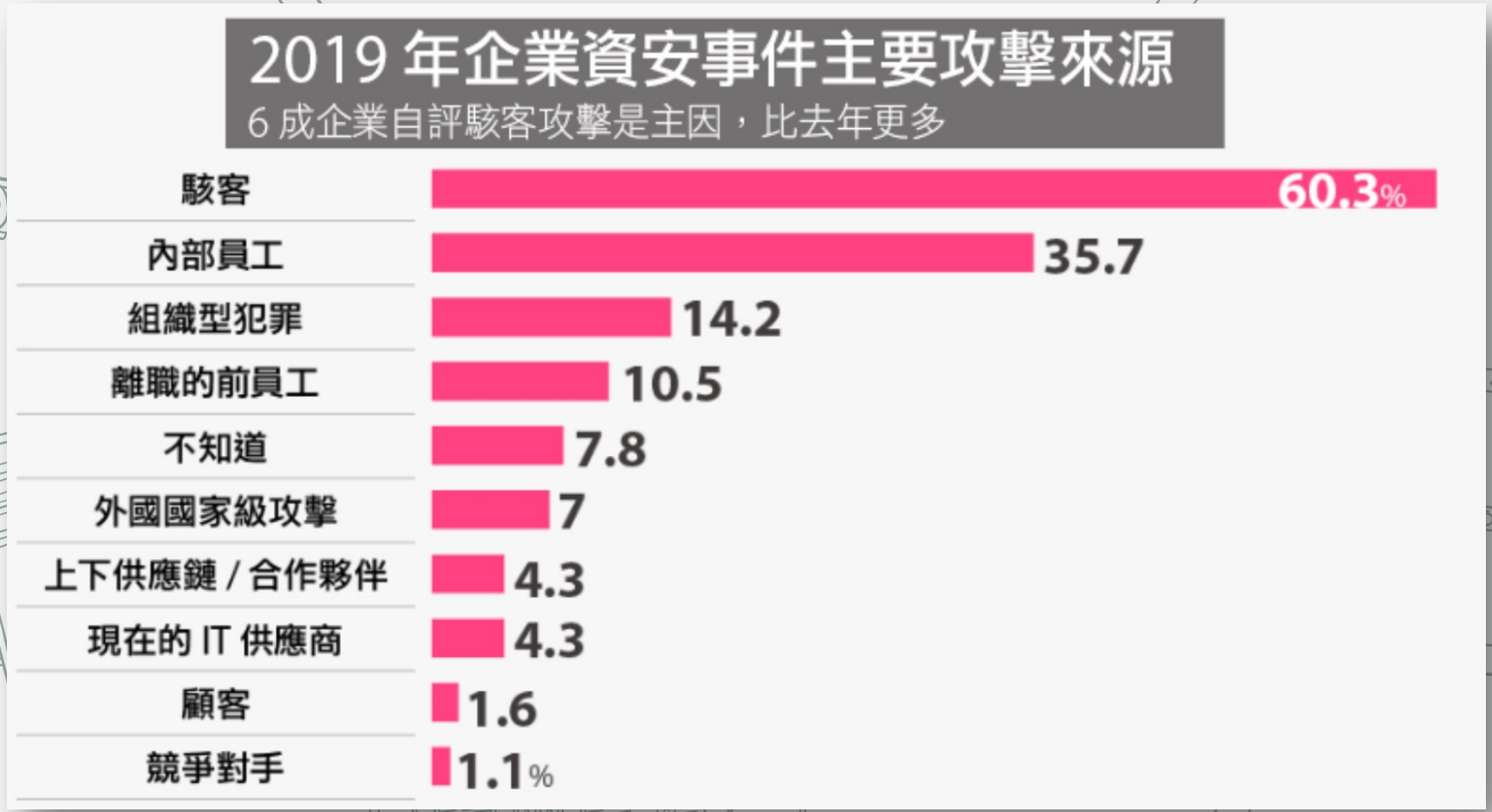
WEB網站



電子郵件



被置入病毒之網頁 → 異常網頁 → 釣魚信件 → 巨集附檔信件



ithome參考來源:https://www.ithome.com.tw/article/136641

八大風險來源

風險一
- 網路釣魚

風險二
- 連接公共 Wi-Fi

風險三
- 惡意 App

風險四
- 軟體漏洞攻擊

風險五
- 軟體漏洞攻擊

風險六
- 瀏覽被入侵的網站或惡意連結

風險七
- 詐騙訊息

風險八
- 不安全的家庭路由器或 IoT 設備


霧蓮釋迦
哼哼 我已經取得所有物聯網的連線了

基礎資訊知識

02.該如何預防?

電腦使用預防辦法

- 安裝防毒軟體
- 更新作業系統及軟體修補
- 不開啟不明來源信件及附檔
- 帳號密碼定期更新及妥善管理
- 輸入帳密前再三確認是否為官方網站

手機使用預防辦法

- 不要任意安裝 App
- 不使用的支付 App 請適時解除安裝
- 開啟螢幕鎖定功能
- 開啟 GPS 跟尋找裝置功能
- 更新作業系統或是軟體修補或更新程式

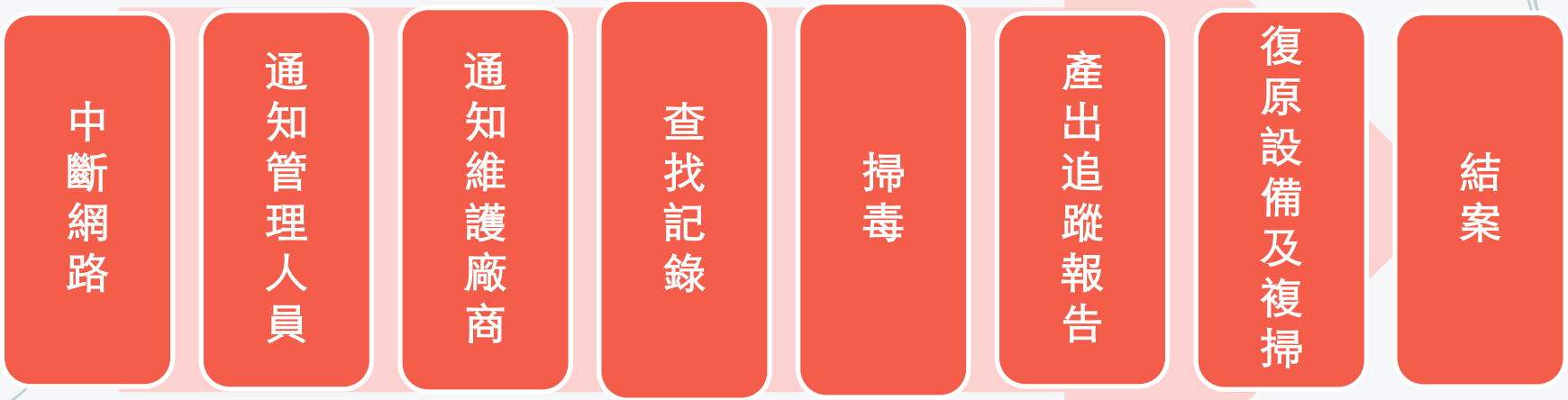
預防九大建議

建議一：運用防毒軟體防範
建議二：輸入帳密前再三確認是否為官方網站
建議三：嚴謹管理自己帳號
建議四：更新作業系統或是軟體修補或更新程式
建議五：不要任意安裝 App
建議六：不使用的支付 App 請適時解除安裝
建議七：開啟螢幕鎖定功能
建議八：開啟 GPS 跟尋找裝置功能
建議九：在家庭網路閘道端建立保護機制

基礎資訊知識

03.發生了怎麼辦?

中毒建議解決方案



基礎資訊知識

04.常見電腦病毒

常見電腦病毒


木馬 病毒
蠕蟲 病毒
勒索 病毒
指令 病毒
玩笑 病毒
系統 病毒
後門 病毒
綁架型 病毒
巨集 病毒
破壞性 病毒
Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
bitcoin
Check Payment

電腦病毒說明

- **系統病毒-**
  可以**感染Windows作業系統的 *.exe 和 *.dll 檔案**，並通過這些檔案進行傳播
- **蠕蟲病毒-**
  特性是**通過網路或者系統漏洞進行傳播**
- **木馬病毒-**
  通過網路或者**系統漏洞進入使用者的系統並隱藏**，然後向外界洩露使用者的資訊。
- **勒索病毒-**
  專門將本機與網路儲存上的**重要檔案加密之後要求支付贖金才能解開檔案。**

電腦病毒說明

- **指令病毒-**
  使用指令碼語言編寫，通過**網頁進行的傳播的病毒**。
- **巨集病毒-**
  特性是能**感染OFFICE系列文件**，然後通過OFFICE通用模板進行傳播。
- **後門病毒-**
  特性是**通過網路傳播，給系統開後門**，給使用者電腦帶來安全隱患。

電腦病毒說明

- **破壞性病毒-**
  特性是**本身具有好看的圖示來誘惑使用者點選**，當用戶點選這類病毒時，病毒便會直接對使用者電腦產生破壞。
- **玩笑病毒-**
  特性是**本身具有好看的圖示來誘惑使用者點選**，當用戶點選這類病毒時，病毒會做出各種破壞操作來嚇唬使用者，其實病毒並沒有對使用者電腦進行任何破
- **綁架型病毒-**
  特性是**病毒會使用特定的捆綁程式將病毒與一些應用程式如QQ、IE捆綁起來**

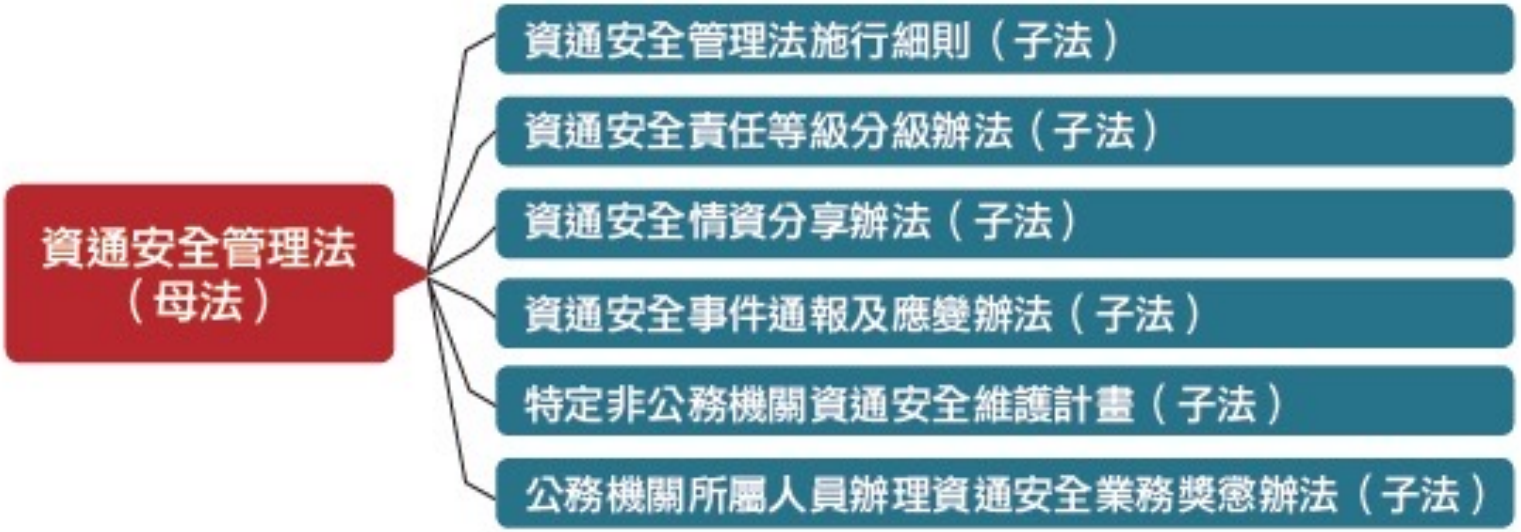
資訊安全法規

資訊安全法規


2014美國聯邦資訊安全現代化法
2014日本網路資訊安全基本法
2015德國資訊科技安全法
2016台灣個人資料保護法
2016歐盟GDPR
2017新加坡網路安全法規
2017英國新資料保護法草案
2018台灣資通安全管理法
• ISO 27001 ISMS 資訊安全管理系統
• BS 10012 PIMS 個人資訊管理系統

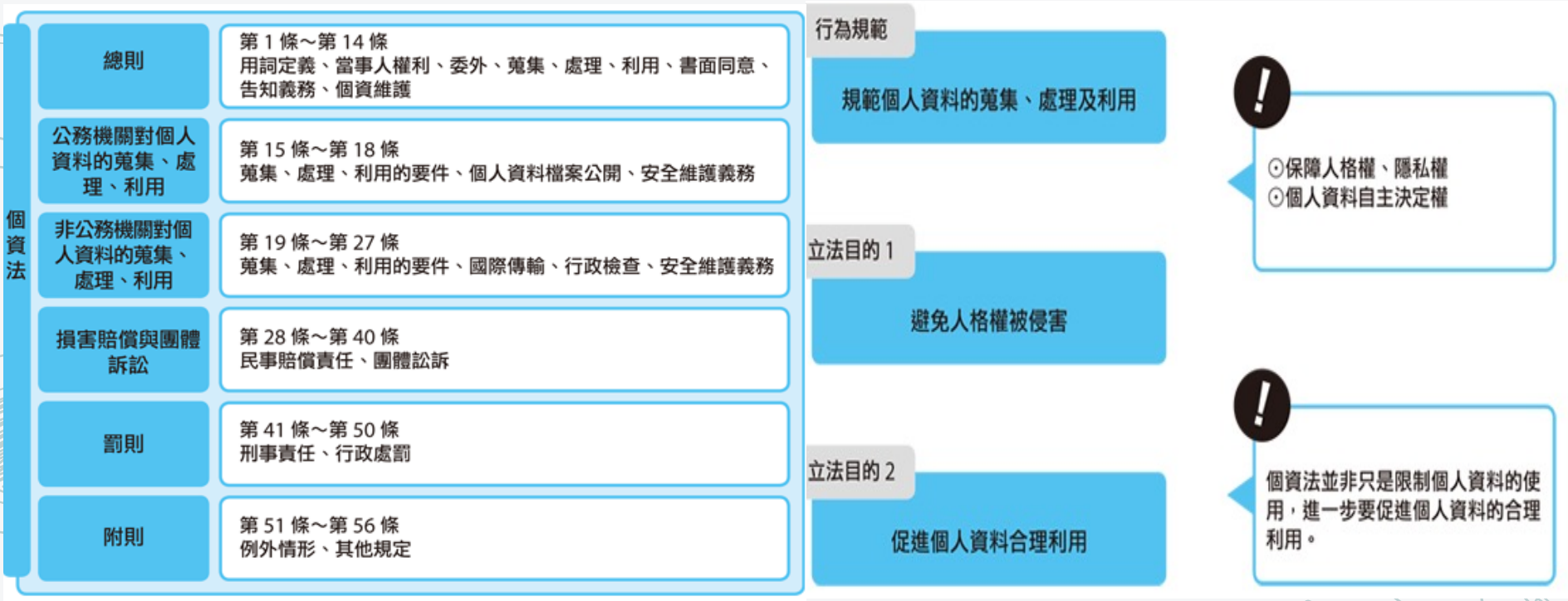
常見資訊安全法規-臺灣法資通安全管理法

臺灣資通安全管理法的架構



資料來源：iThome整理，2018年5月

常見資訊安全法規-臺灣個人資料保護法



總結

- 建議一：運用防毒軟體防範
- 建議二：輸入帳密前再三確認是否為官方網站
- 建議三：嚴謹管理自己帳號
- 建議四：更新作業系統或是軟體修補或更新程式
- 建議五：不要任意安裝 App
- 建議六：不使用的支付 App 請適時解除安裝
- 建議七：開啟螢幕鎖定功能
- 建議八：開啟 GPS 跟尋找裝置功能
- 建議九：在家庭網路閘道端建立保護機制

- 風險一：網路釣魚
- 風險二：連接公共 Wi-Fi
- 風險三：惡意 App
- 風險四：軟體漏洞攻擊
- 風險五：軟體漏洞攻擊
- 風險六：瀏覽被入侵的網站或惡意連結
- 風險七：詐騙訊息
- 風險八：不安全的家庭路由器或 IoT 設備

Q & A