

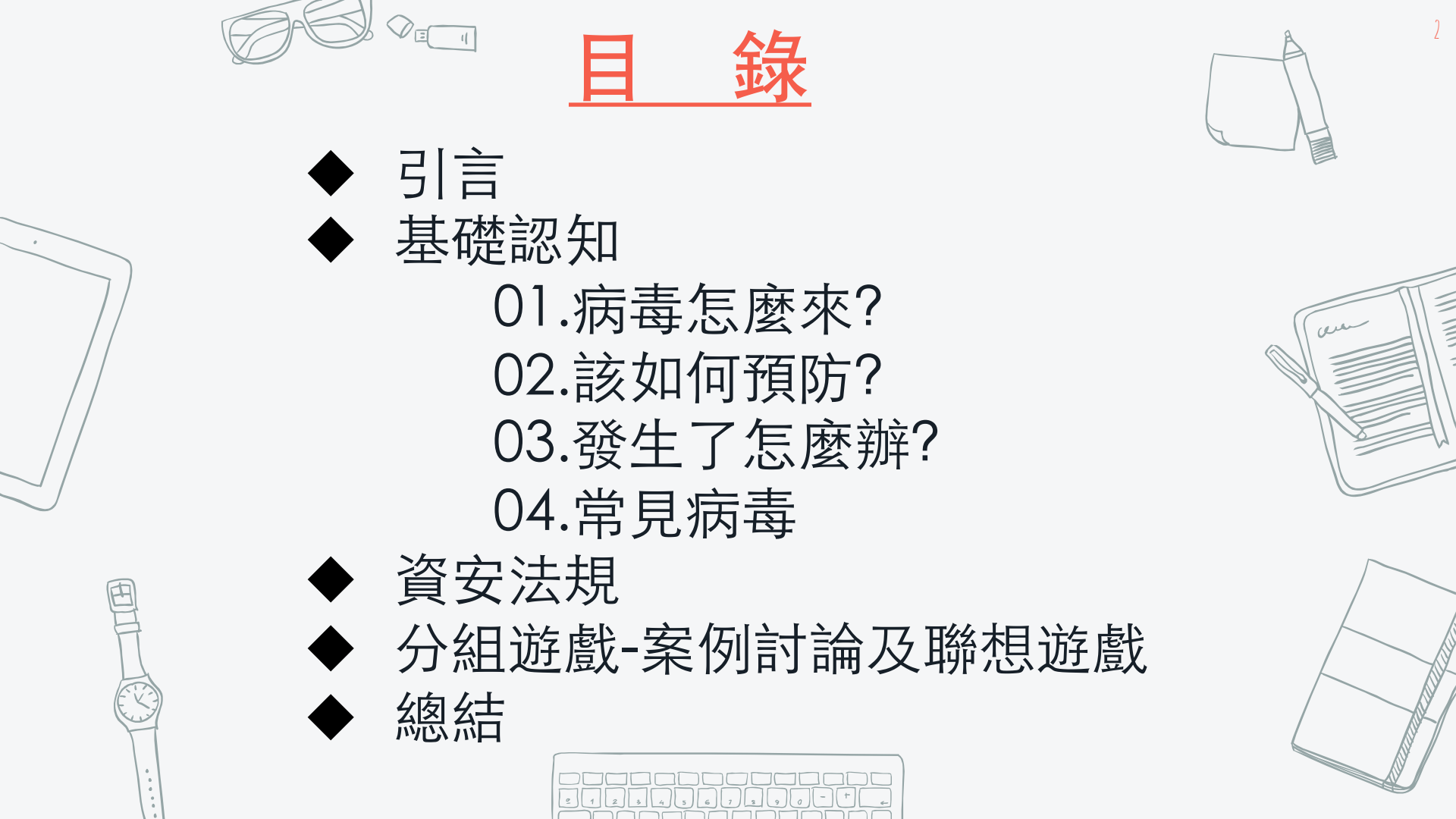


資訊安全

Information Security

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

2021.09



目錄

- ◆ 引言
- ◆ 基礎認知
 01. 病毒怎麼來?
 02. 該如何預防?
 03. 發生了怎麼辦?
 04. 常見病毒
- ◆ 資安法規
- ◆ 分組遊戲-案例討論及聯想遊戲
- ◆ 總結

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網站發布重大訊息，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。

文/周峻佑 | 2021-10-28發表

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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網站發布重大訊息，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。

序號	1	2	3
發行人	張嘉文	張嘉文	張嘉文
副發行人	張嘉文	張嘉文	張嘉文
主編	張嘉文	張嘉文	張嘉文
符合條款	第 26 版	第 26 版	第 26 版
事實發生日	110/10/27	110/10/27	110/10/27
發售時間	17:25:51	17:25:51	17:25:51
發言人職稱	行政副總經理	行政副總經理	行政副總經理
發言人電話	0767118244	0767118244	0767118244

1. 事實發生日 110/10/27
2. 發生事由 本公司輔助性伺服器遭受病毒攻擊。
3. 處理過程 本公司資訊部對輔助性伺服器遭受病毒攻擊，本公司資安團隊已於第一時間發現攻擊跡象，並立即啟動防禦機制，目前系統運作正常。

圖片來源: 中鴻鋼鐵

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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

文/周峻佑 | 2021-10-27發表

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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

技嘉 (Gigabyte) 於 10/20/2021 發布重大訊息，稱其位於台灣的研發中心遭到勒索軟體攻擊。這是技嘉在 2021 年第二次遭遇勒索軟體攻擊。此外，帝寶 (Audi) 也遭遇了資安事件。

圖片來源: Tomkappe

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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

文/周峻佑 | 2021-10-26發表

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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

宏碁 (Acer) 於 10/26/2021 發布重大訊息，稱其客戶資料遭到勒索軟體攻擊。此外，TWCERT/CC 設立了勒索軟體防護專區。

圖片來源: Phency Affairs

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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，但命令稽核工具含有與編碼沒能阻止錯誤命令執行的情況下，先導致臉書全球分發網路節點，接著DNS伺服器開始崩潰宣告，讓臉書在全球網路大崩潰，進而引發臉書內網全斷、內部工具無法使用的骨牌式災難。

文/陳煥利 | 2021-10-09發表

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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，但命令稽核工具含有與編碼沒能阻止錯誤命令執行的情況下，先導致臉書全球分發網路節點，接著DNS伺服器開始崩潰宣告，讓臉書在全球網路大崩潰，進而引發臉書內網全斷、內部工具無法使用的骨牌式災難。

圖片來源: 維基

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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的研析，GriftHorse是今年他們發現最龐大範圍的惡意程式活動，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專家發現GriftHorse的存在。

文/陳煥利 | 2021-09-30發表

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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的研析，GriftHorse是今年他們發現最龐大範圍的惡意程式活動，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專家發現GriftHorse的存在。

圖片來源: Tomkappe

新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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

日前宏碁電腦 (Acer) 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。

文/陳煥利 | 2021-10-19發表

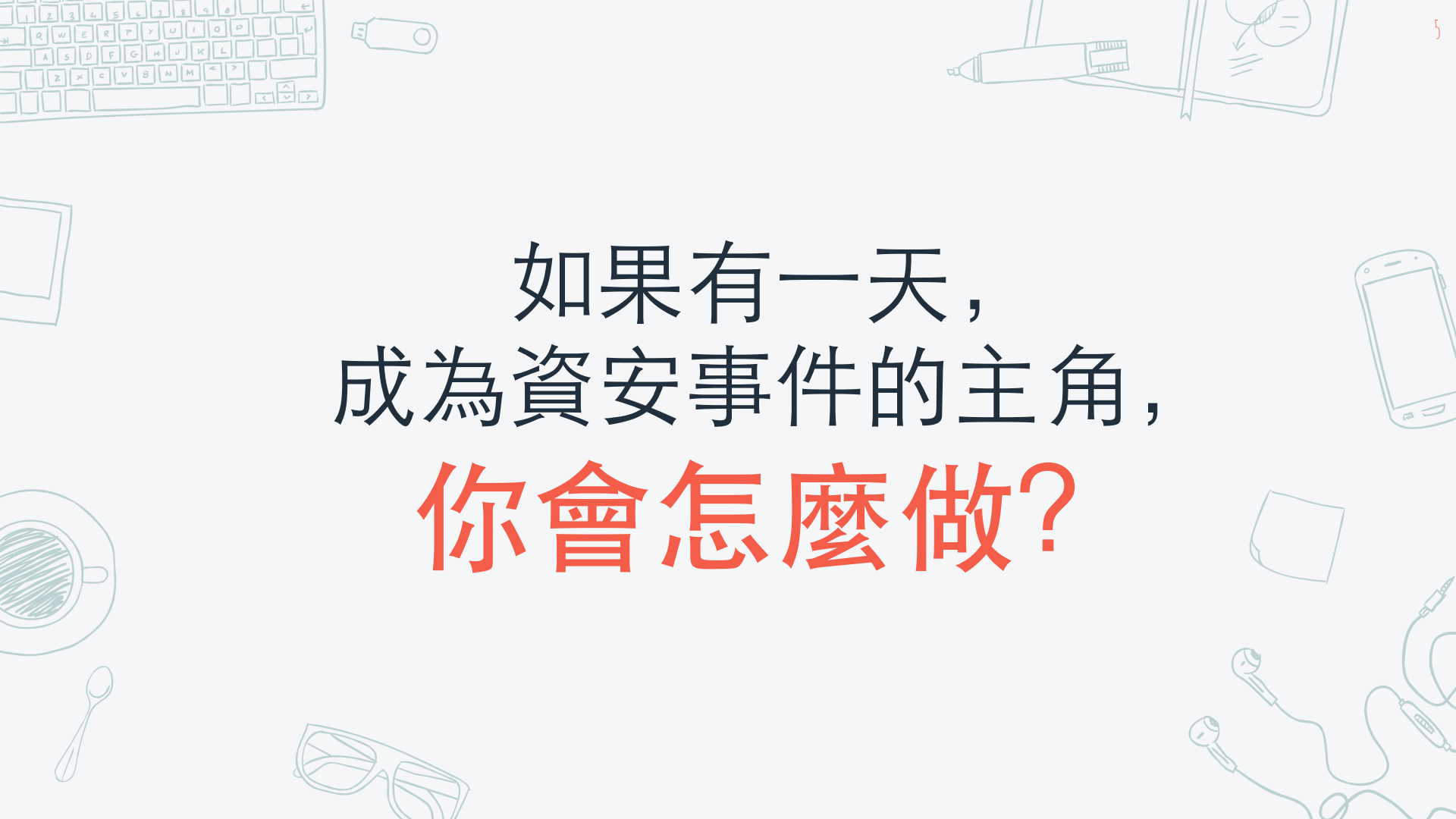
新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

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

日前宏碁電腦 (Acer) 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。

圖片來源: Phency Affairs



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

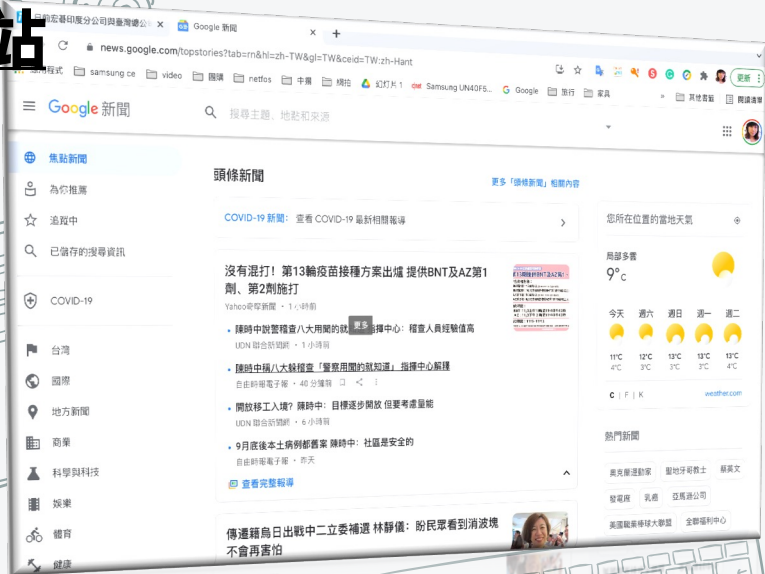
01. 病毒怎麼來?



常見來源

WEB網

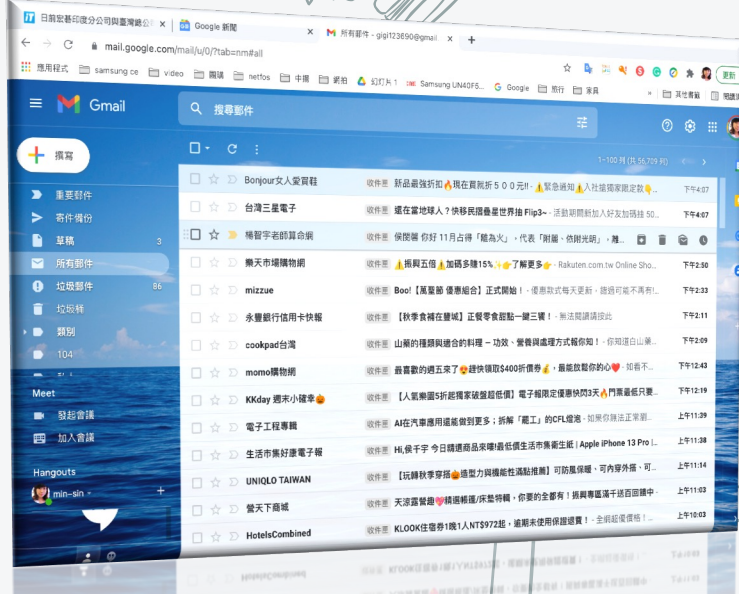
站



被置入病毒之網頁

異常網頁

電子郵件

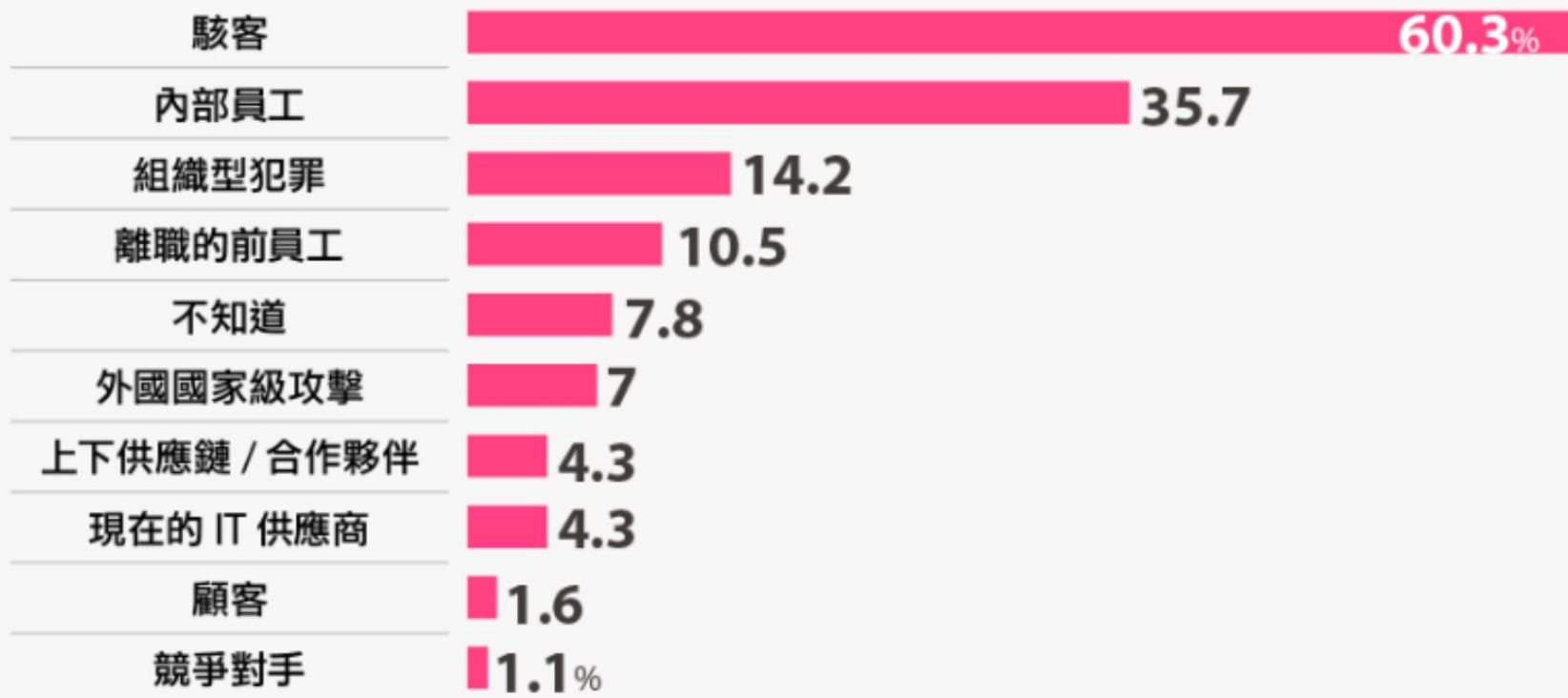


釣魚信件

巨集附檔信件

2019 年企業資安事件主要攻擊來源

6 成企業自評駭客攻擊是主因，比去年更多



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

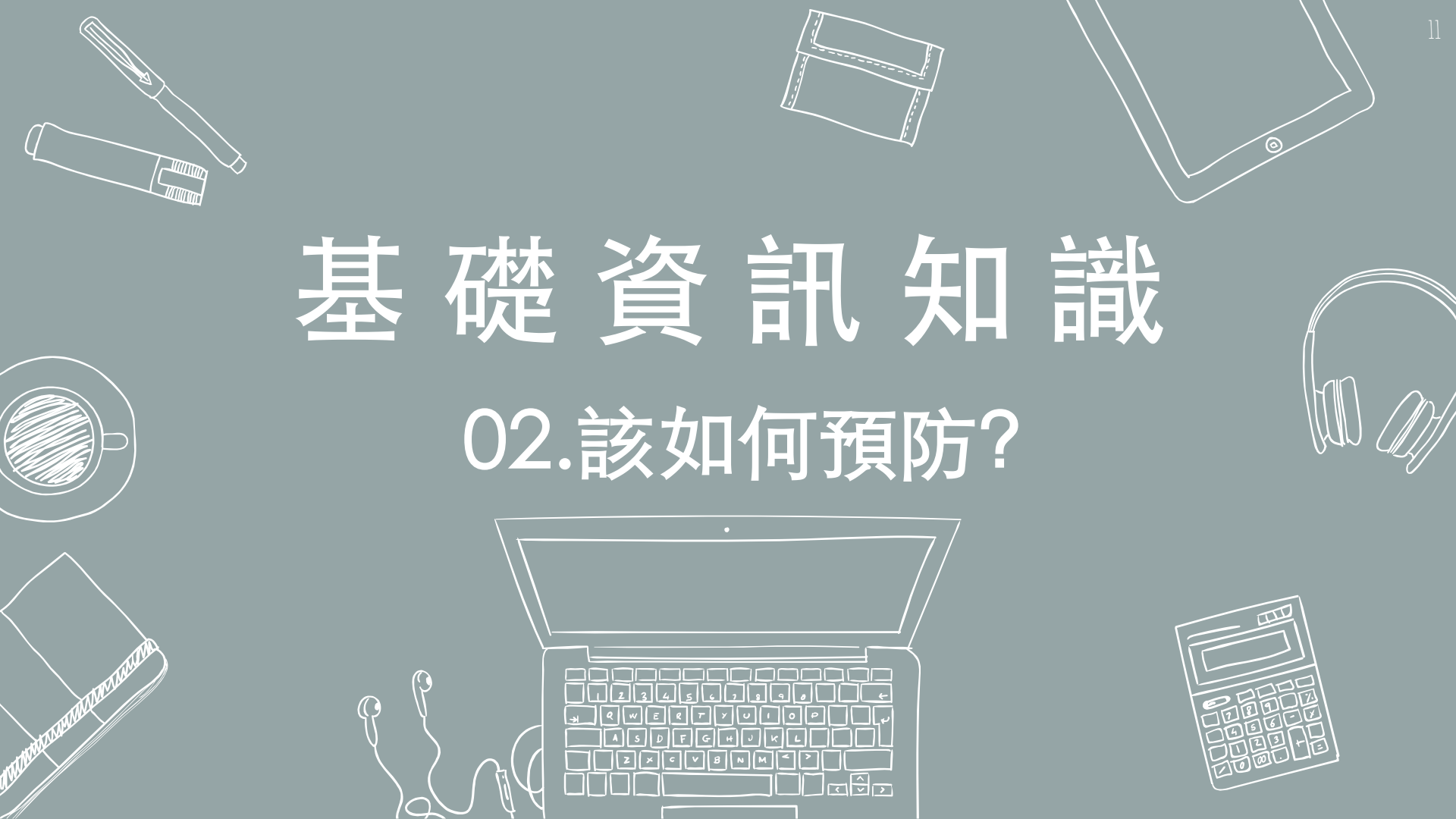
- 不安全的家庭路由器或 IoT 設備

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

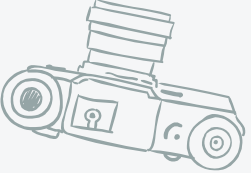

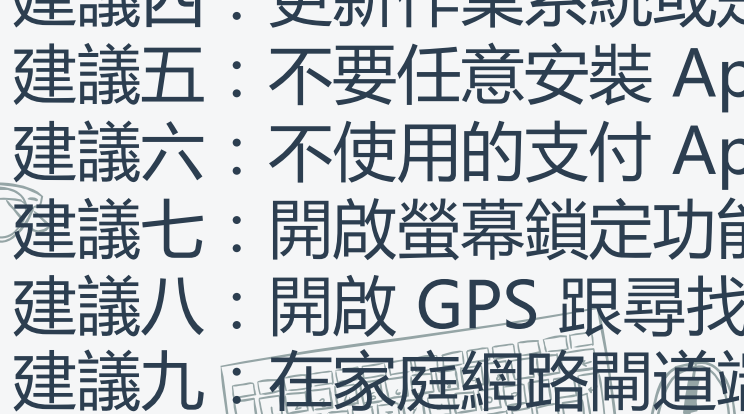

開啟螢幕鎖定功能

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

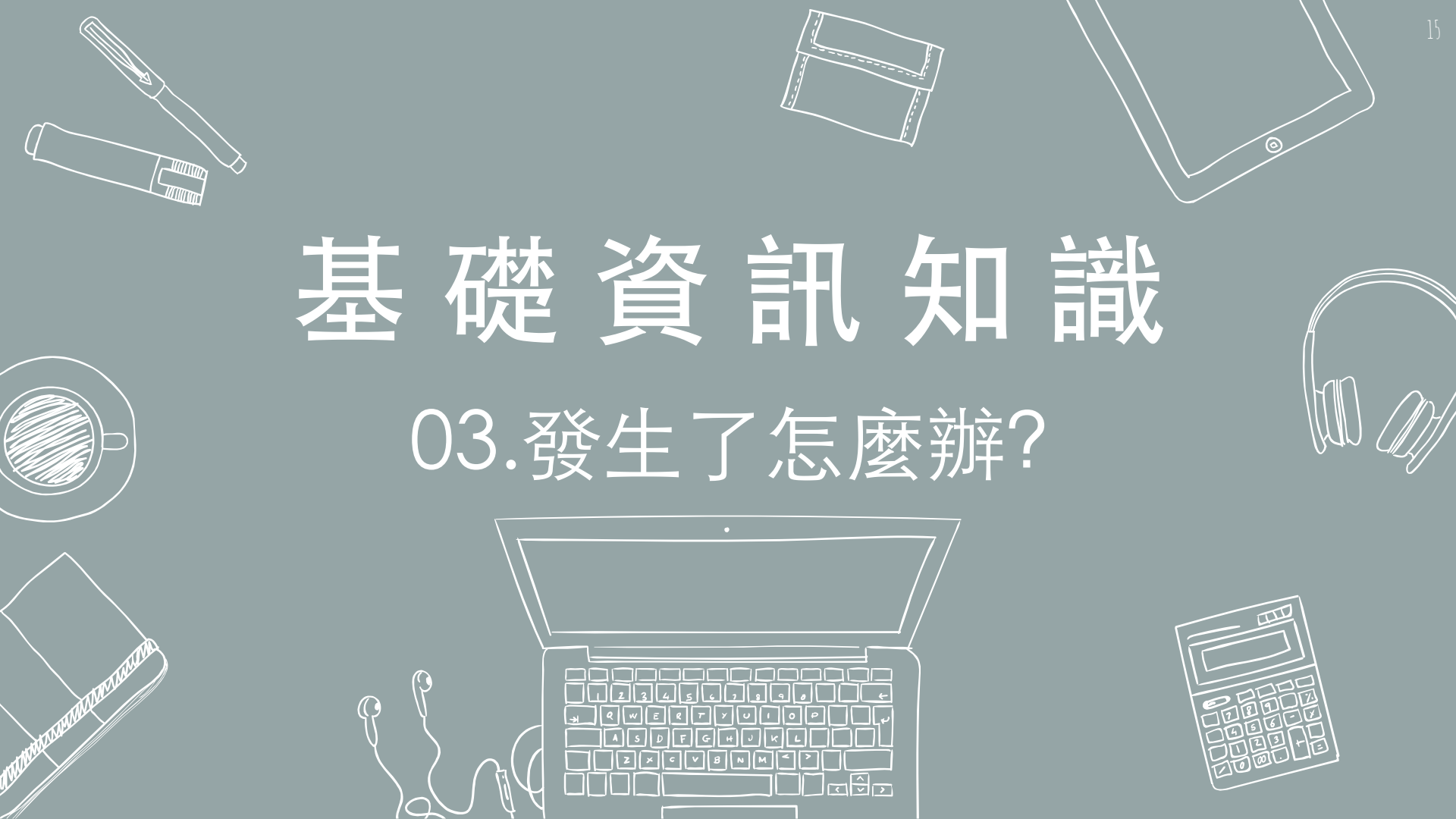


預防九大建議

- 
- 
- 
- 
- 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

中斷網路

通知管理人員

通知維護廠商

查找記錄

掃毒

產出追蹤報告

復原設備及複掃

結案

基礎資訊知識

04.常見電腦病毒



常見電腦病毒



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

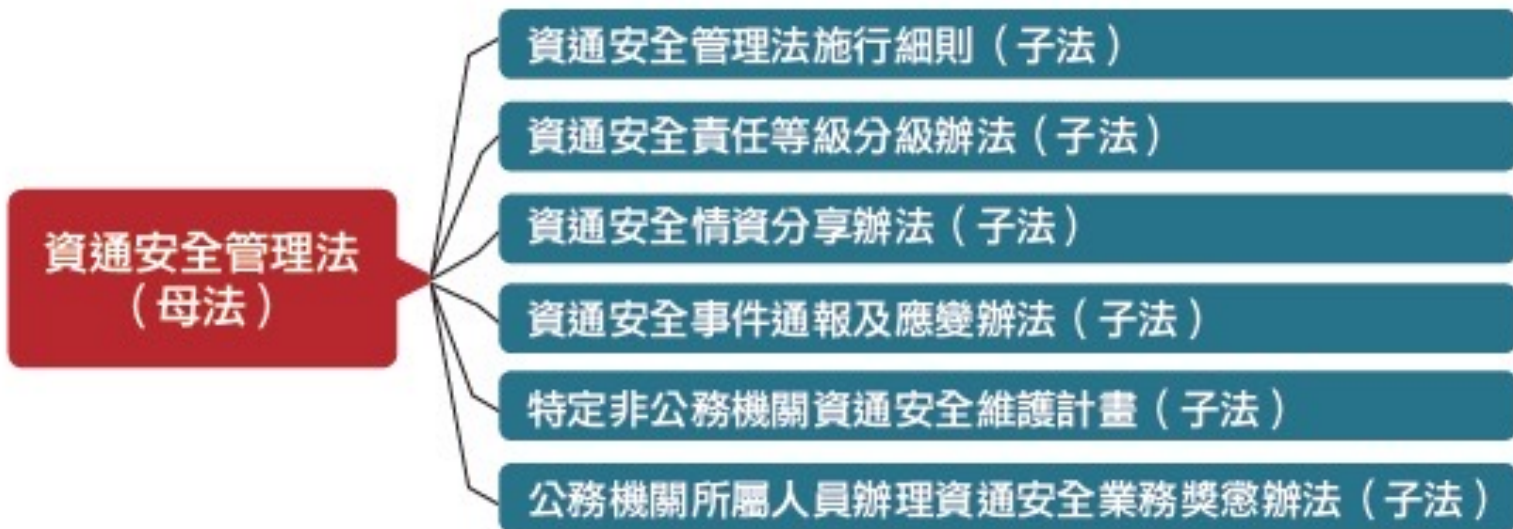
資訊安全法規



資訊安全法規



臺灣資通安全管理法的架構



常見資訊安全法規-臺灣個人資料保護法

個資法

總則

第 1 條～第 14 條
用詞定義、當事人權利、委外、蒐集、處理、利用、書面同意、告知義務、個資維護

公務機關對個人資料的蒐集、處理、利用

第 15 條～第 18 條
蒐集、處理、利用的要件、個人資料檔案公開、安全維護義務

非公務機關對個人資料的蒐集、處理、利用

第 19 條～第 27 條
蒐集、處理、利用的要件、國際傳輸、行政檢查、安全維護義務

損害賠償與團體訴訟

第 28 條～第 40 條
民事賠償責任、團體訴訟

罰則

第 41 條～第 50 條
刑事責任、行政處罰

附則

第 51 條～第 56 條
例外情形、其他規定

行為規範

規範個人資料的蒐集、處理及利用

立法目的 1

避免人格權被侵害

立法目的 2

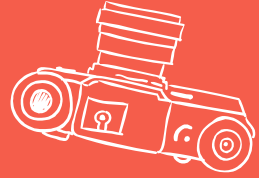
促進個人資料合理利用

- ◎保障人格權、隱私權
- ◎個人資料自主決定權

個資法並非只是限制個人資料的使用，進一步要促進個人資料的合理利用。

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

