

# 公務機密維護

10大資安鐵則讓你遠離勒索病毒



苗栗縣政府政風處  
2月份公務機密維護宣導

資料來源：SecBuzzer  
作者：林致婷

## 看似無礙的使用習慣，恐助「駭」為虐

「面對勒索軟體的攻擊威脅，政府單位、企業組織乃至醫療院所該如何應對？」在探討這個問題之前，無論是企業內部管理者、IT人員或一般基層員工，可以先透過三個基本的問題做初步的自我檢視。

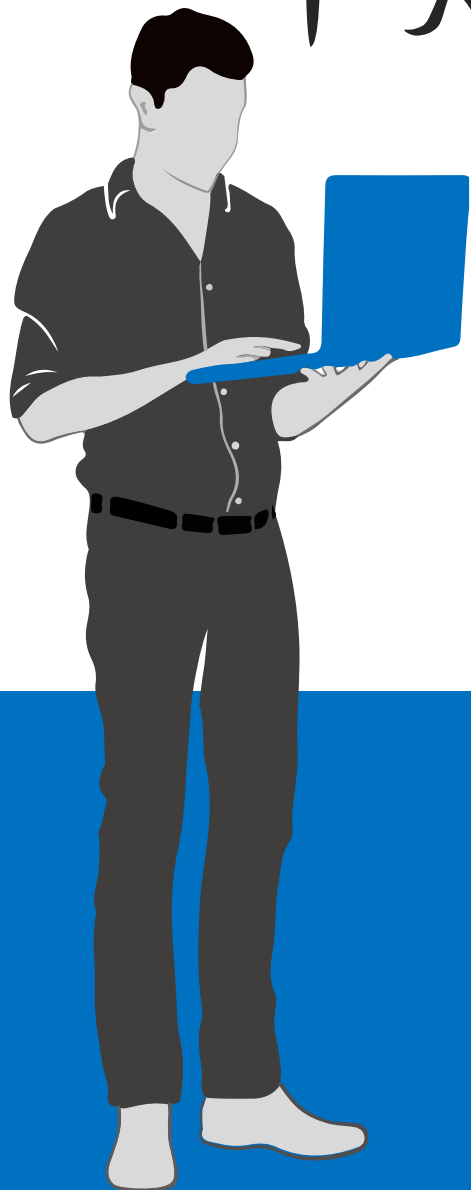
您是否曾使用同事遞來未經掃毒的USB隨身碟讀取檔案？

您是否曾開啟未經掃毒過濾的電子郵件附檔？

您是否曾點下電子郵件中不明的外部連結？

上述問題，相信多數人至少有一個答案是肯定的，換句話說，你我都曾不自覺的為駭客開後門，讓個人甚至所屬企業組織落入陷阱，成為待宰的肥羊。一個企業組織該如何有效防禦勒索軟體的攻擊威脅，絕非組織內IT、MIS部門一肩扛的責任，而是**上從高階主管，下至基層員工「人人有責」**，才能拉出防駭的強力封鎖線，讓駭客無路可進。

# 十大鐵則拉起嚴密資安防線



預防勝於治療，如何有效防禦勒索軟體的入侵，無論是高階主管還是基層員工，都應切記**五必要、五不要的十大鐵則**，看似不經意的小習慣都能有效拉起資安防線。

# 五不要、五必要

五個不要：

- 1、不要瀏覽不信任網站
- 2、不要下載、執行不明軟體或檔案
- 3、不要隨意分享不明檔案或軟體
- 4、不要安裝非法或過時軟體或作業系統
- 5、不要將電腦連接到已被感染網路



# 五不要、五必要

五個必要：

- 1、電子郵件附檔開啟前務必掃毒過濾，收到可疑信件檔案主動通報
- 2、必須經常建立新的備份且離線儲存
- 3、無論是系統、軟體還是病毒碼都必定持續更新
- 4、必須設定強密碼且定期更新
- 5、必須要有辨識網路釣魚、勒索軟體攻擊等威脅的能力，且定期進行社交工程演練



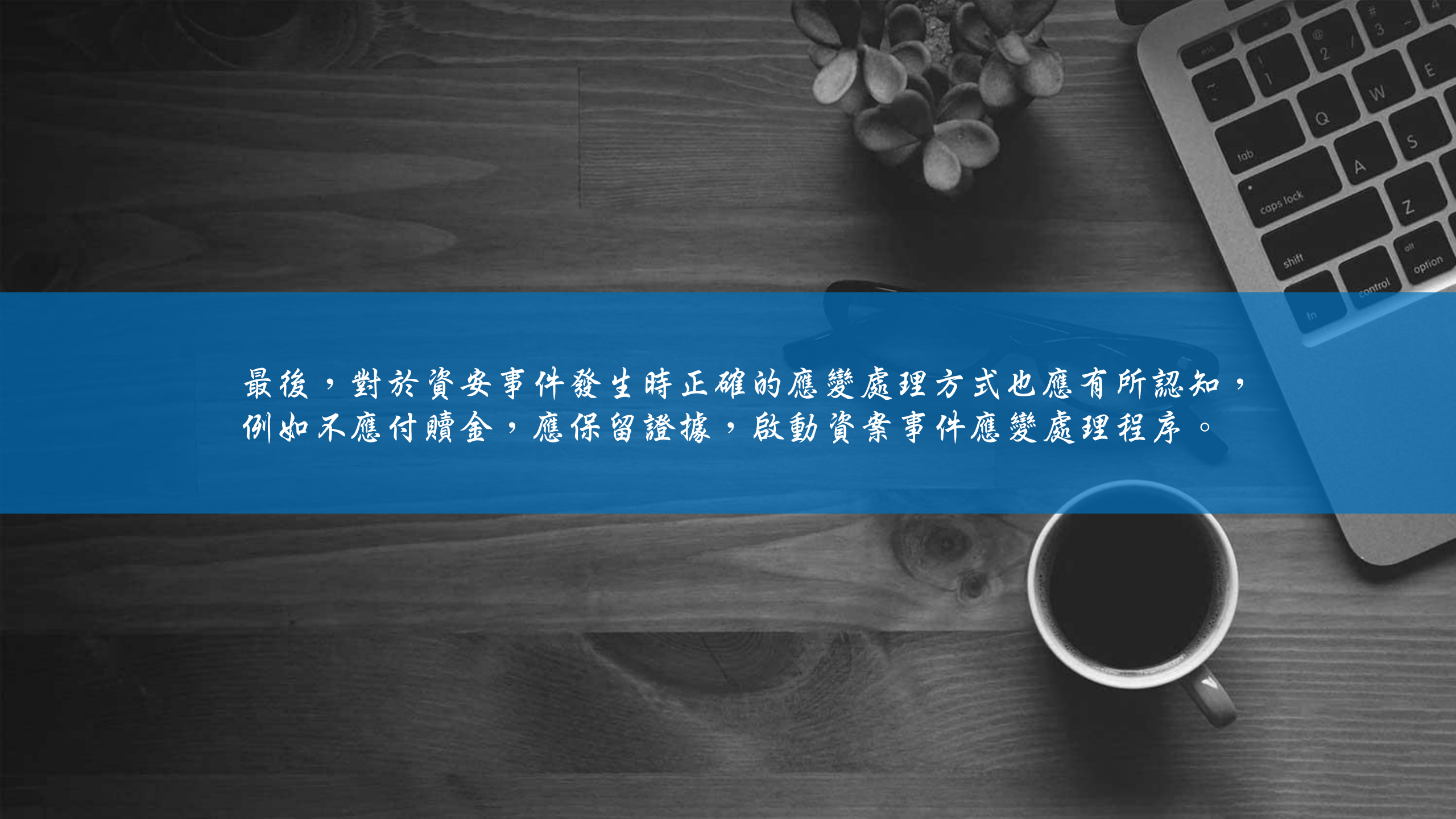
# 勒索軟體入侵！緊急應變四字訣：

## 拍、斷、關、報



若是不幸仍遭到勒索病毒的攻擊，謹記四字訣：拍、斷、關、報。

- 將加密勒索訊息視窗與已加密資料夾檔名予以**拍照截圖存證**；
- 立即**切斷網路**，避免將網路磁碟機或共享目錄上的檔案加密；
- 關閉電腦電源**不讓勒索病毒繼續加密電腦中的檔案；
- 通報資訊人員**接手進行處理，將硬碟取出以另外有安裝防毒軟體主機將未受害檔案搬移作業。

A top-down view of a wooden desk. In the upper right, a portion of a silver laptop is visible, showing keys like 'tab', 'caps lock', 'shift', 'control', 'option', 'fn', 'in', 'z', 'x', 'c', 'v', 'b', 'n', 'm', 'comma', 'period', 'slash', 'backslash', 'asterisk', 'at', 'number', 'underscore', 'hash', 'dollar', 'percent', 'ampersand', 'at', 'number', 'underscore', 'hash', 'dollar', 'percent', 'ampersand'. In the upper center, there is a small potted succulent with thick, rounded leaves. In the lower right, a white ceramic cup filled with dark coffee sits on the desk. A blue horizontal band is overlaid across the middle of the image, containing white text.

最後，對於資安事件發生時正確的應變處理方式也應有所認知，  
例如不應付贖金，應保留證據，啟動資安事件應變處理程序。



廉政專線：037-356639

苗栗縣政府政風處

關心您~