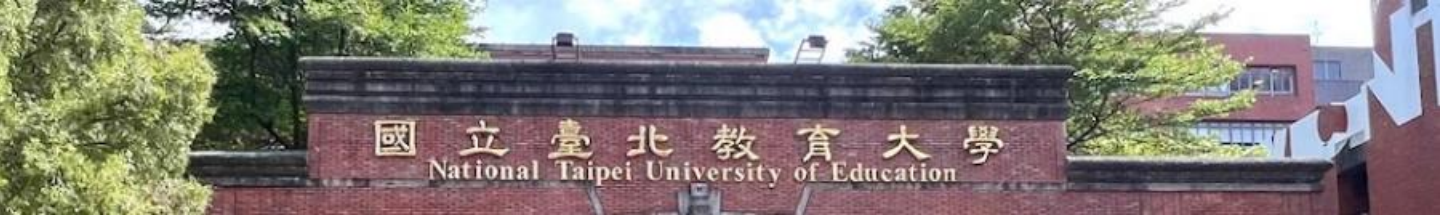


資 安 補 血 包

第 1 期
中華民國112年10月 出刊

由於資安事件頻仍，為保護本校師生免於受害，計網中心特針對本校師生量身提供 - 資安補血包，內容為校內重要資安情資及措施，視需要採不定期提供。
有鑑於勒索軟體攻擊事件層出不窮，做好資安防護、加強宣導資安防護意識並定期備份重要檔案，為預防受害的不二法門。以下提供勒索軟體的介紹、感染途徑、防護措施相關資源，作為強化資安防護之參考。

一、什麼是勒索軟體（Ransomware）

勒索軟體（Ransomware）是一種透過破壞受害者存取權限，並向受害者要求贖金的惡意程式，目前可分2類如下：

- 非加密型勒索軟體：受害者會被鎖在資訊設備裝置之外，無法登入。
- 加密型勒索軟體：感染您的電腦後，加密您電腦裡的檔案，並要求您付錢解鎖以取回您的檔案。

二、感染途徑

以下列出常見的感染途徑：

- 網站瀏覽
- 電子郵件
- 軟體安裝
- 被已受勒索軟體攻擊電腦或裝置感染（USB磁碟等）

三、感染後的緊急處理

若感染勒索軟體，建議採取以下措施：

- **請勿付費**
- 電腦主機關機
- 拔除電腦主機網路線
- 請駐點工程師協助重新安裝作業系統（**資料無法救回**）
- 還原備份資料至新作業系統

四、防護措施

可從電腦裝置及使用者行為管控等方式著手：

各式軟體安全管控	•**使用者操作行為安全管控** (含Gmail、Chrome、Edge、Line...)
防毒軟體	•定期更新病毒碼 •防護資料夾遭勒索軟體攻擊
Windows作業系統防火牆	•定期更新Windows Update •防火牆請預設「開啟」

(一) 使用者操作行為安全管控

感染途徑：網站瀏覽

阻隔方式：

- ◘ 瀏覽器（Chrome、Edge等）定期更新版本
- ◘ 不要點選可疑的網頁連結
- ◘ 防毒軟體若偵測為危險網頁，請勿強制開啓

感染途徑：電子郵件

阻隔方式１：不要開啟未經確認的郵件與附件

- ◘ **如何確認寄件者？**將滑鼠移到電子郵件的寄件者（下圖中紅色箭頭所指tzupei的位置），Gmail即會自動顯示出寄件者完整的電子郵件信箱位址。

- ◘ 確認**寄件者**完整的電子郵件信箱位址之後，可協助判定郵件是否有問題，有時**信件標題**看似正常，卻是勒索病毒信或社交工程演練測試信。

信件類別	寄件者	信件標題
時事類	1Thome<1theme@yahoo.com.tw>	駭客攻擊8 家券商 金管會：恐還有下波
知識類	黃泰豐<larry1217@gmail.com>	「食色性也」不是孔子說的
健康類	綠色地球<xm4nk499@yahoo.com>	別再用寶特瓶裝水了！各項研究告訴你它可怕的真相！
美容類	Hellen<hellen520@gmail.com>	染唇妝過時啦！2017跟著李聖經擦上微醺MLBB唇才最潮
生活類	韓流最前線<girlpretty@hotmail.com>	變更嬌小，惹人疼！「胖胖單品」逆轉勝
新奇類	李蓉芬<melody8056@msa.hinet.net>	小二生超狂造句 讓網友驚呼：他超懂人性
美女類	杜肯<kentdo5717@outlook.com>	正妹車服員神到了 曾是黑澀會美眉
科技類	新北資訊通<newtaipeinews@yahoo.com>	新北打造智慧城 力推手機無線充電服務
旅遊類	LIME news<limemews@hotmail.com>	領務局LINE 新功能 出國旅遊添保障
財經類	巨富網<richnessnet@outlook.com>	貨幣戰開打？中國單月狂拋660億美元美債！創5年新高

注意上圖中的寄件者及信件標題，
新北市政府的訊息郵件，不可能由@yahoo.com信箱寄出，
領務局訊息郵件，不可能由@hotmail信箱寄出。

◘ 下圖為惡意程式或詐騙信件的實例。

感染途徑：電子郵件

阻隔方式 2 ：關閉郵件預覽功能

◘ 下圖紅色方框標示的區域，即為**Gmail之郵件預覽區**。

◘ Gmail關閉郵件預覽功能步驟。

1. 點選Gmail頁面右上方的「設定」
2. 點選「收件匣」
   點選「不要分割」
   點選「儲存變更」

◘ 留意**詐騙信件！**

感染途徑：安裝軟體

阻隔方式：導入「資通安全弱點通報機制（VANS）資訊平台」，定期回報

◘ 檢查安裝的合法軟體，版本是否安全

◘ 回報安裝軟體清單

VANS 進度說明

◆ 全校行政單位已完成導入

(二) 安裝防毒軟體

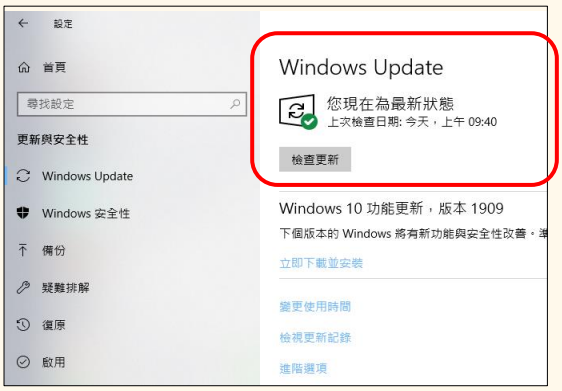
◘ 透過更新病毒資料庫監控、掃描系統，減少電腦病毒、駭客及程式漏洞等攻擊

◘ 保護重要文件**資料夾**，防止勒索軟體攻擊

◘ 本校簽訂**趨勢防毒軟體**全校授權，提供師生**在校**或**家中**使用。
網址 https://licensing.ntue.edu.tw/

(三) Windows系統安全管控

- 電腦**防火牆功能**，請設為開啟狀態。Windows10「設定」>「網路和網際網路」>「狀態」下方「Windows 防火牆」
- 作業系統**Windows Update**請設定自動更新，隨時保持最新狀態



- 電腦登入帳號及密碼，密碼至少 **8 碼**以上，並混合**英文、數字、特殊符號**（例如：Peal@3801）
- 在Windows10「設定」>「隱私權」內，確認**相機**、**麥克風**的權限是否只提供**授權的應用程式**開啟

五、備份檔案

定期備份檔案，採用「3-2-1原則」來備份重要檔案：

- 重要資料至少備份 3 份
- 使用 2 種不同形式媒體（外接硬碟/電腦/雲端）
- 其中 1 份備份存放異地

六、結語

沒有軟體是保證安全的！使用軟體、瀏覽網站或開啓郵件，需保持**資安意識**，若有疑慮或可疑現象，請立即停止操作，並尋求計網中心的協助。