

濫發垃圾信被斷網怎麼辦

發生原因

工科系過往處理的類似案例通常都是

1. Windows 系統允許遠端桌面連線
2. 帳號密碼太好猜被破解
3. 駭客利用原本的使用者or新創一個使用者下載 Turbo-Mailer (大量發信程式)並執行
4. 計中發現異常後，將該 IP 阻斷

解決方法

- 如果平時沒有遠端連線的需求就關閉這功能 ([控制台\所有控制台項目\系統\進階系統設定])，



有需求建議改用 Teamviewer
(<https://www.teamviewer.com/zhTW/>)

- 在[控制台\使用者帳戶]檢查有沒有多出不明的使用者，有的話將之刪除；另外記得將原先的使用者

密碼更改為強度70分以上的 (<http://password.mx500.com/>)

密碼強度測試

[home](#)
[feed](#)

測試你的密碼		密碼最低要求
待測密碼:	*****	
密碼隱藏:	<input checked="" type="checkbox"/>	
分數:	76%	
評語:	強	<ul style="list-style-type: none"> 密碼最低要求8字元 最少符合下列四項中三項規則: <ul style="list-style-type: none"> - 大寫英文字元 - 小寫英文字元 - 數字字元 - 符號字元

- 搜尋 Turbo Mailer 把找到的資料夾跟檔案都刪除，駭客就是用這個軟體大量發垃圾信(但不會被防毒程式判定為病毒)
- 利用學校提供的防毒軟體(推薦卡巴斯基)或[下載 Avira Free Antivirus 徹底全系統掃毒](#)，看有沒有潛藏的威脅
- **進行「網路回報」作業**(須有中心 mx0z0my 或 m 系列的電子郵件信箱帳號)，**系統執行自動阻斷解除的作業時間為每週週一至週五的 08:00、12:00 與 17:00 整點**。不便之處，敬請見諒。

以上資料，感謝工科系單位網管何孟軒先生提供

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/security:attack:mail_spam

Last update: **2017/01/09 15:32**