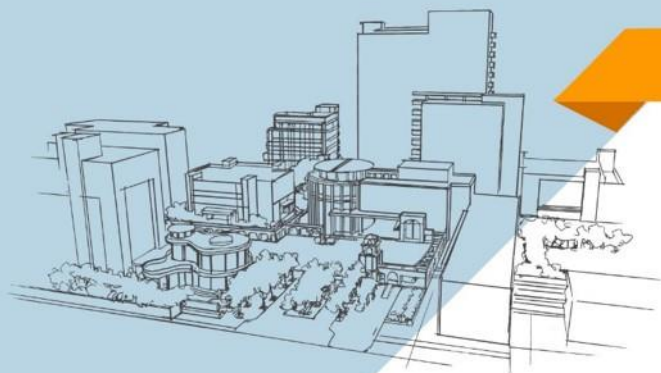




臺北醫學大學
TAIPEI MEDICAL UNIVERSITY

資訊安全宣導

資訊處



TMU60
1960-2020

北醫六十 邁向榮耀

緣 由

近日網路組收到多位老師及同仁致電告知收到釣魚網站之詐騙信件，請各位**無須驚慌，勿支付款項**，希望透過此宣導來建立正確資安觀念，防範勒索詐騙。



釣魚網站與電子郵件範例(一)

There is an overdue payment under your name. Please, settle your debts ASAP.  收件匣 x



寄給我 ▾

冒充本人寄信給自己，恐嚇當事人，需支付比特幣



根據貴機構的設定，系統將這封郵件歸類為正常郵件，而非垃圾郵件。

移至垃圾郵件

Hi!

Sadly, there are some bad news that you are about to hear.
About few months ago I have gained a full access to all devices used by you for internet browsing.
Shortly after, I started recording all internet activities done by you.

Below is the sequence of events of how that happened:
Earlier I purchased from hackers a unique access to diversified email accounts (at the moment, it is really easy to do using internet).
As you can see, I managed to log in to your email account without breaking a sweat: (cweijen1@tmu.edu.tw).

Within one week afterwards, I installed a Trojan virus in your Operating Systems available on all devices that you utilize for logging in your email.
To be frank, it was somewhat a very easy task (since you were kind enough to open some of links provided in your inbox emails).
I know, you may be thinking now that I'm a genius.

With help of that useful software, I am now able to gain access to all the controllers located in your devices (e.g., video camera, keyboard, microphone and others).
As result, managed to download all your photos, personal data, history of web browsing and other info to my servers without any problems.
Moreover, I now have access to all accounts in your messengers, social networks, emails, contacts list, chat history - you name it.
My Trojan virus continues refreshing its signatures in a non-stop manner (because it is operated by driver),
hence it remains undetected by any antivirus software installed in your PC or device.

So, I guess now you finally understand the reason why I could never be caught until this very letter...

During the process of your personal info compilation, I could not help but notice that you are a huge admirer and regular guest of websites with adult content.
You endure a lot of pleasure while checking out porn websites, watching nasty porn movies and reaching breathtaking orgasms.
Let me be frank with you, it was really hard to resist from recording some of those naughty solo scenes with you in main role and compiling them in special videos that expose your masturbation sessions, which end with you cumming.

In case if you still have doubts, all I need is to click my mouse and all those nasty videos with you will be shared to friends, colleagues, and relatives of yours.
Moreover, nothing stops me from uploading all that hot content online, so all public can watch it too.

釣魚網站與電子郵件範例 (二)



郵件內的部分影像無法顯示 | 新增至安全的寄件者清單 | 顯示影像

10GB Mailbox
HiNet (pse [redacted] n.tw) 新增連絡人

收件者: undisclosed-recipients:

好康優惠訊息郵件通知

尊敬的用戶，

感謝您長久以來對HiNet電子郵件服務的支持。為了提供您更好的服務品質

「[點擊這裡 加大HiNet 郵件信箱儲存空間儲存空間至10GB](#)」

郵件系統升級後，將可提供您加大(至10GB)的信箱空間以及更便利的垃圾信件防護功

祝您 身體健康 萬事如意

中華電信數據通信分公司 敬上
客服專線：0800-080-412

釣魚網站與電子郵件範例 (三)



台灣電子郵件支持管理中心 <support@fit.edu.tw>
寄給 ▾

冒充學術單位寄信，並附上釣魚連結

根據貴機構的設定，系統將這封郵件歸類為正常郵件，而非垃圾郵件。

移至垃圾郵件

尊敬的帳戶電子郵件用戶，

您的郵箱已超出台灣郵箱管理員系統設置的存儲限制，您將無法接收新郵件，除非您重新驗證立即收到您的電子郵件，這就是您最近沒有看到新郵件的原因。

點擊這裡：<https://form.jotform.com/221498216581056>

請重新驗證您當前正在使用的電子郵件帳戶，因為我們正在刪除所有舊的和未使用的帳戶，未能回覆您可能會丟失您的電子郵件帳戶

注意：這是台灣消息系統的新規則

2022 版權所有台灣電子郵件支持管理員團隊重新驗證您的帳戶

--


This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

...



常見問題

收到勒索信件的正確處理方式

1. 不要付贖金。因一旦付了贖金，就會被鎖定，攻擊者會改用其他方式勒索。
2. 不要開啟未知的 URL 連結或附檔。自我保護是最重要的資安觀念之一，若隨意開啟可能就會被植入惡意程式。
3. 個人電腦應安裝防毒軟體，且作業系統及防毒軟體應隨時更新，以避免漏洞產生
4. 更改密碼網址：[\[北醫首頁\]](#)-[\[教職員\]](#)-[網通聯絡](#)[\[Email密碼變更或同步\]](#)。
5. 導入Google雙因子認證。密碼加上手機即時驗證碼  強化安全

防毒軟體下載連結(限校內，需登入)：

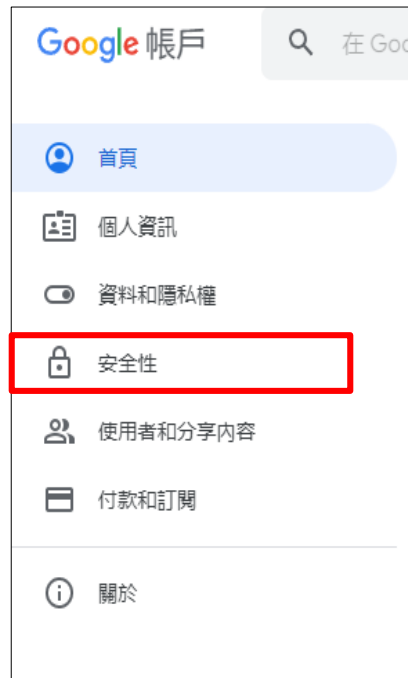
[\[資訊處網站\]](#)-[\[服務項目\]](#)-[\[授權下載\]](#)-[\[線上下載\]](#)-[\[卡巴斯基防毒軟體\]](#)

如何導入雙因子認證

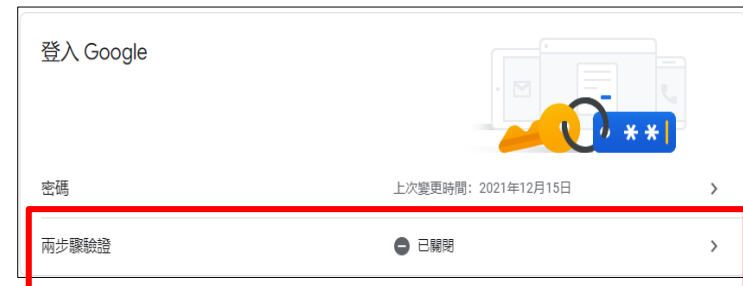
1. 點選右上圖示，
並點選管理你的
GOOGLE帳戶



2. 點選左方“ 安全性”



3. 於頁面中，找到兩步驟驗證





防制措施



加強宣導：

網路組將不定期以電子郵件發送宣導訊息

禁止連線上網：

校內電腦皆有進行流量管控，若系統偵測到使用者流量異常，將會自動阻擋，限制該電腦無法上網。

未安裝校內指定防毒軟體：

如發現中毒將強制阻斷該電腦連線，待使用者安裝完成後再開放。