系所網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 校園網路架構
- 校園網路管理
- 網站弱掃服務
- 資安案例分享

大 綱

- 校園網路架構
- 校園網路管理
- 網站弱掃服務
- 資安案例分享

校園網路架構

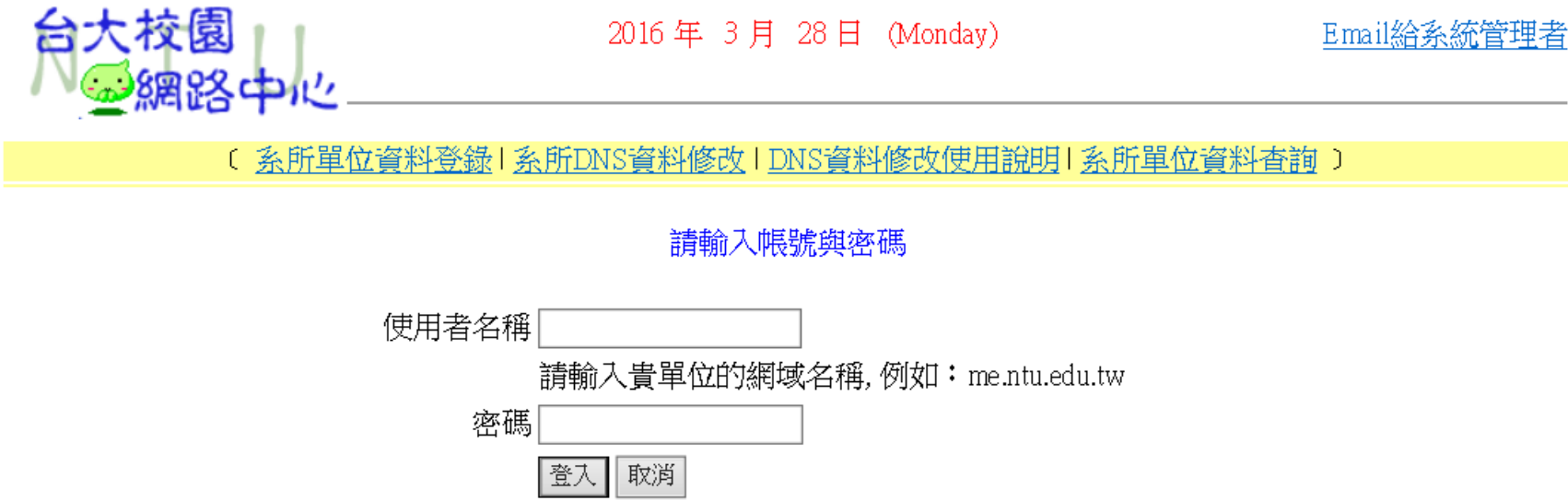
- 本校內網
  - 校園骨幹網路各以**20Gbps**連接校園核心網路
  - 水源校區以**2G bps**與校總區連接
  - 醫學校區、 醫院各以**2G bps**與校總區連接
  - 公衛校區以**1G bps**與校總區連接
  - 行遠樓及竹北校區以**100M bps**與校總區連接
- 本校外網
  - 國際專屬頻寬 **2Gbps**
  - 國際專屬服務 **2Gbps(是方電訊)**
  - 連接教育部、中研院 各 **10 Gbps**
  - 連接TWAREN **10 Gbps**
  - 本校與ISP介接
    - 中華電信 Hinet – 10G bps，遠傳電信 FETnet - 2G bps，台灣固網 TFN – 1G bps，中嘉和網KBT– 1G bps，亞太電訊 – 1G bps

大 綱

- 校園網路架構
- **校園網路管理**
- 網站弱掃服務
- 資安案例分享

校園網路管理

- 臺大校園網路管理系統整合平台
  - http://netmng.cc.ntu.edu.tw/admin
  - 系所與單位網管可自行管理
    - 進入”**網路管理系統**”
      - 以”**台大校園網路中心**” http://netadm.cc.ntu.edu.tw **帳密**登入



校園網路管理

- **臺大校園網路管理系統整合平台**
  - **重要伺服器清單確認**
    - 請將重要伺服器IP設定於例外清單
    - 請每1年檢視一次，更新例外清單
    - **新系統109年7月1日啟動**
      - 每年1月1日~1月31日開放更新， 1月31日到期後**自動從例外清單內移除**
      - **請補充說明內容**
        - » IP使用地點、負責人、聯絡方式、申請說明、到期時間

計資中心
校園網路管理系統
整合平台

網路管理系統

網路註冊系統

流量管制網段流量查詢報表

異常統計查詢依單位

異常統計查詢依IP

網路異常歷史查詢報表

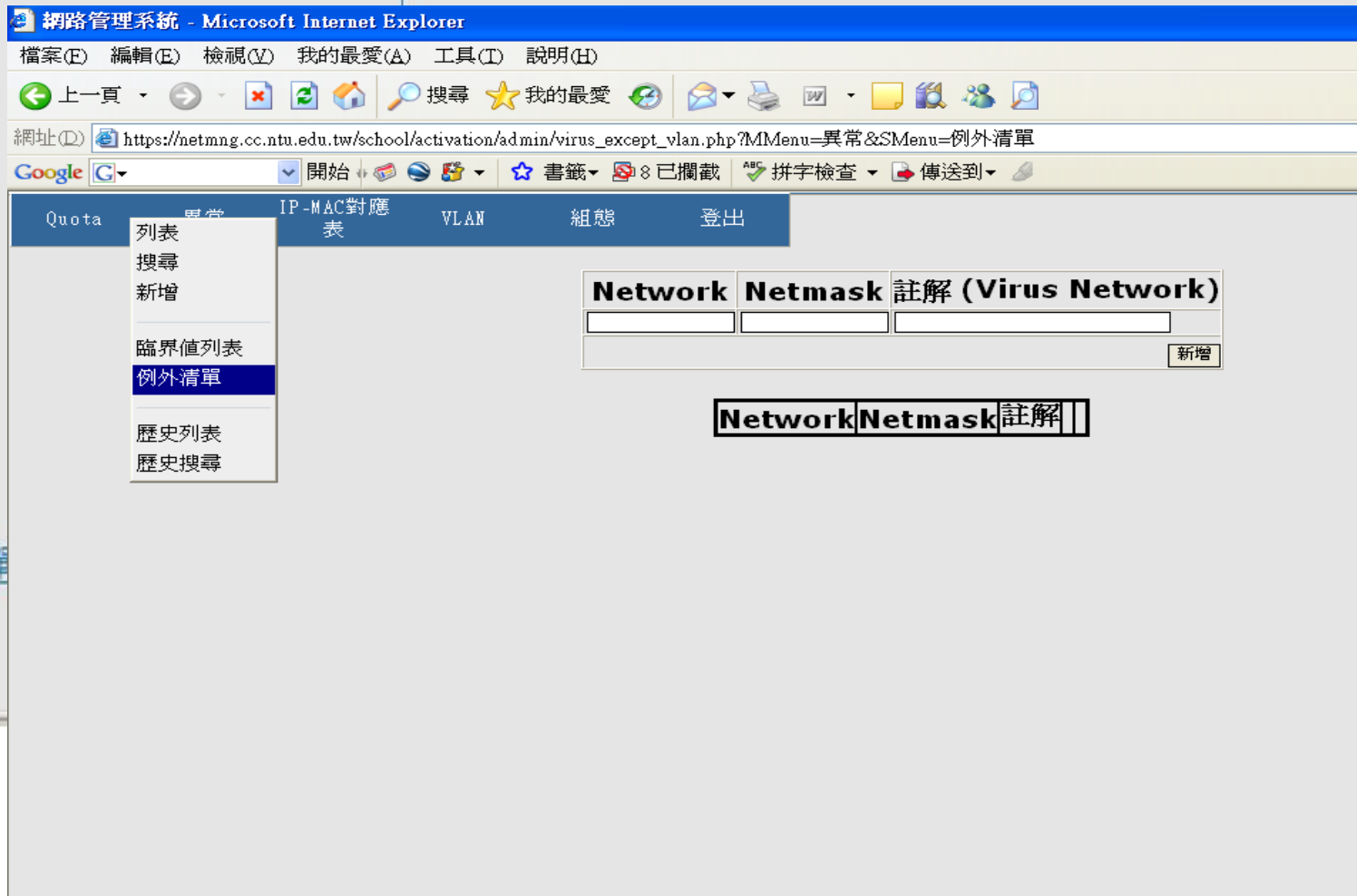
網路異常分析報表

超過流量限制與流量異常清單

外部流量異常清單

各單位使用率統計

各IP使用量統計圖表



校園網路管理

Network	Netmask	有效日期	使用地點	負責人	聯絡方式	申請說明
	255.255.255.	31/01/2021				
新增						

			Network	Netmask	登記時間	保留日數	刪除時間	
修改	✕		140.112.3.250	255.255.255.255	2020-02-01	367	2021-02-02 5:00	ASOC
修改	✕		140.112.3.76	255.255.255.255	2020-03-17	320	2021-01-31 5:00	測試
修改	✕		140.112.3.85	255.255.255.255	2020-02-01	365	2021-01-31 5:00	ASOC connector 18012

網路管理系統 - Mozilla Firefox

https://netmng.cc.ntu.edu.tw/nms/

Network	140.112.3.76
Netmask	255.255.255.255
有效日期	2021-01-31 5:00
使用地點	計中
負責人	Mo
聯絡方式	33663366
申請說明	測試

關閉此視窗

校園網路管理

Network	Netmask	有效日期	使用地點	負責人	聯絡方式	申請說明
140.112.3.76	255.255.255.255	31/01/2021	計中	Mo	33663366	測試

修改 取消

			Network	Netmask	登記時間	保留日數	刪除時間	申請說明
	修改	✕	140.112.3.250	255.255.255.255	2020-02-01	367	2021-02-02 5:00	ASOC
		✕	140.112.3.76	255.255.255.255	2020-03-17	320	2021-01-31 5:00	測試
	修改	✕	140.112.3.85	255.255.255.255	2020-02-01	365	2021-01-31 5:00	ASOC connector 180129

校園網路管理(續)

- **臺大校園網路管理系統整合平台**
  - 系所與單位網管可自行管理
    - IP-mac address對應
      - 妥善管理內部IP，防止IP被盜用
      - 需要導入之系所或單位，**請與網路組連絡**
      - 資料輸入方式
        - » 人工鍵入
        - » IP-Mac Excel資料檔匯入

校園網路管理(續)

- **臺大資訊安全中心**
  - http://cert.ntu.edu.tw/
  - 違規主機名單
  - 解除網路限制**(請確認問題已解決)**
    - http://cert.ntu.edu.tw/Module/UnbanIP/NManager.php
      - 以”台大校園網路中心” http://netadm.cc.ntu.edu.tw 帳密登入
- **注意:網管交接，務必更新”台大校園網路中心”資料**

校園網路管理(續)


| 回首頁 | 臺大首頁 | 計中首頁 |
臺灣大學 NTU is 資訊安全中心
National Taiwan University
Information Security Center
> 最新消息
> 違規主機相關
> 網安精華區
> 下載專區
> 智財權宣導
違規主機名單
限制IP使用名單
解除中毒主機設限
資安事件通報資訊聯絡方式：
電子郵件信箱：
security@ntu.edu.tw
abuse@ntu.edu.tw
聯絡電話：
(02)3366-5010
2013-09-05 舊版Android作業系統安全堪慮
根據美國國土安全部(DHS)及聯邦調查局(FBI)的最新內部通報文件顯示，目前全世界已經有超過44%安裝Android作業系統的行動裝置都存有安全漏洞，並且極易遭受惡意程式的入侵攻擊。詳情請按此
【行政院國家資通安全會報技術服務中心】
2013-09-02 中國遭有史以來最大DDoS攻擊
中國.CN網域名稱解析(Domain Name Service, DNS)伺服器群於8/25凌晨零時起遭到分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊。詳情請按此
【行政院國家資通安全會報技術服務中心】

大 綱

- 校園網路架構
- 校園網路管理
- **網站弱掃服務**
- 資安案例分享

網站資安弱點掃描

- 教育部轄下資安團隊提供網站資安弱點掃描服務
- 本校校內系所/單位可向計中網路組申請首頁或重要網站弱點掃描服務
- 聯絡資訊
  - 負責同仁: 李墨軒 小姐
  - Email: molee@ntu.edu.tw

弱掃前注意事項

- 弱掃前，請**備份網站**，因弱掃可能造成資料遺失毀損等狀況
- 請提前公告弱掃時間，提醒使用者該時段網站服務有可能會中斷
- 請注意是否有其他資安設備，各資安設備、防火牆皆須開弱掃引擎**白名單**
- 弱掃期間，建議關閉防毒軟體
- 弱掃時間最長為**7**小時，若超過**7**小時系統會自動中斷掃描，因此建議先整理網站目錄，將不必要的檔案移除**(**例如備份檔**)**
- 因弱掃時會快速發送大量的請求(requests)，有可能造成網站服務中斷，或資安設備的異常狀況。除了提前公告弱掃時間外，建議**避免同單位多個網站都集中在同一時段弱掃**

弱掃時機

- 網站公開上線前
- 職務異動新接系統
- 開發程式過程中
- B級單位網站每年建議至少執行一次初測及一次複測

弱掃後常見異常狀況

- **掃描超過七小時**
  - 掃描時間過長，系統自動中斷掃描
  - 弱掃報告仍然有效，建議依報告修補弱點後，再進行複測
- **不論執行完成/失敗，只要掃描小於1分鐘，不會產生弱掃報告**
  - 可能原因：資安設備阻擋、該網址/IP未開啟Web服務、網路異常...
  - 建議排除上述原因後，重新申請排程掃描

宣導事項

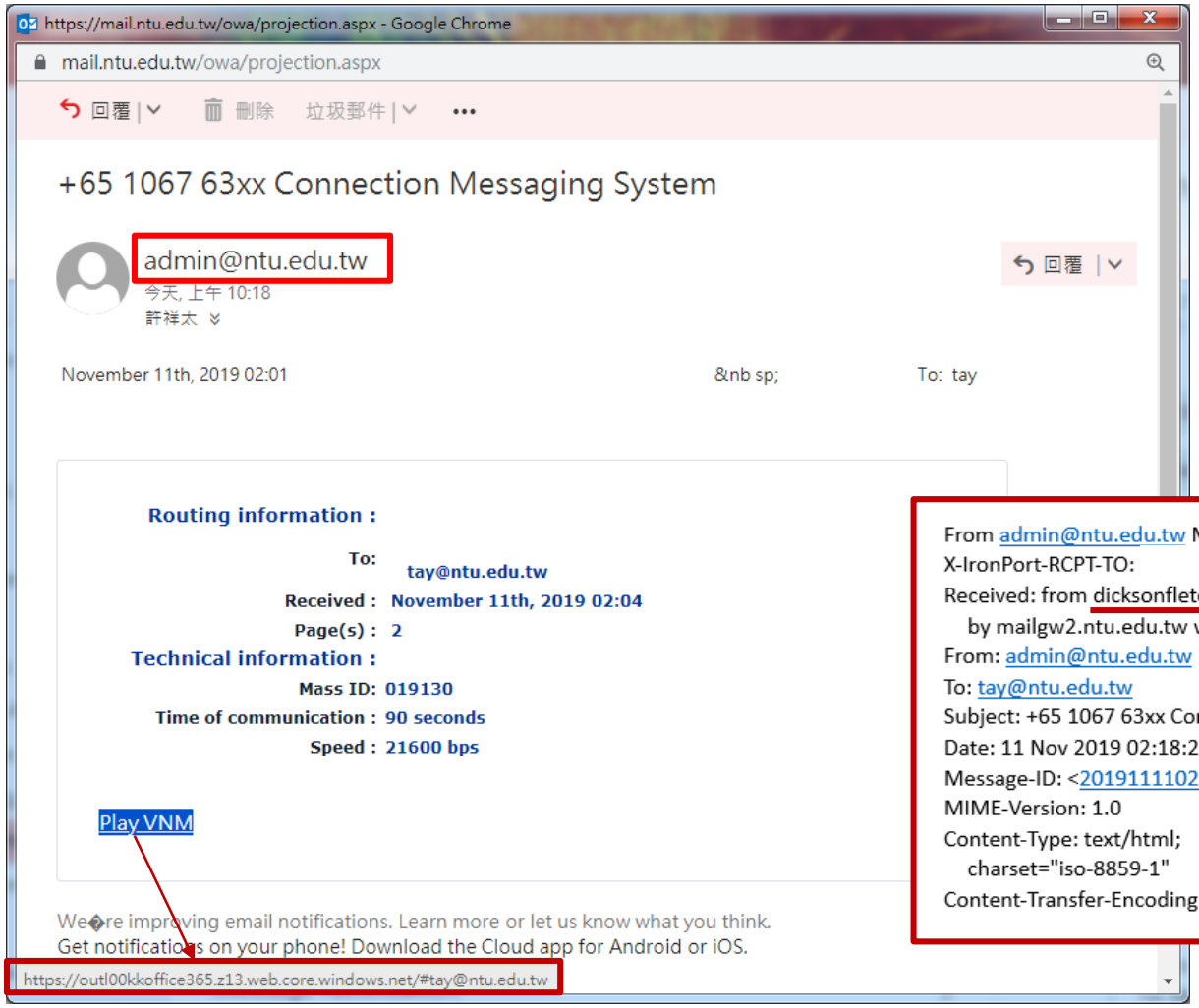
- 如發生資安事件請主動通報計中網路組
  - 聯絡資訊
    - 負責同仁: 李墨軒 小姐
    - Email: molee@ntu.edu.tw

- 資安事件須於**1小時**內完成通報

大 綱

- 校園網路架構
- 校園網路管理
- 網站弱掃服務
- 資安案例分享

釣魚郵件攻擊案例

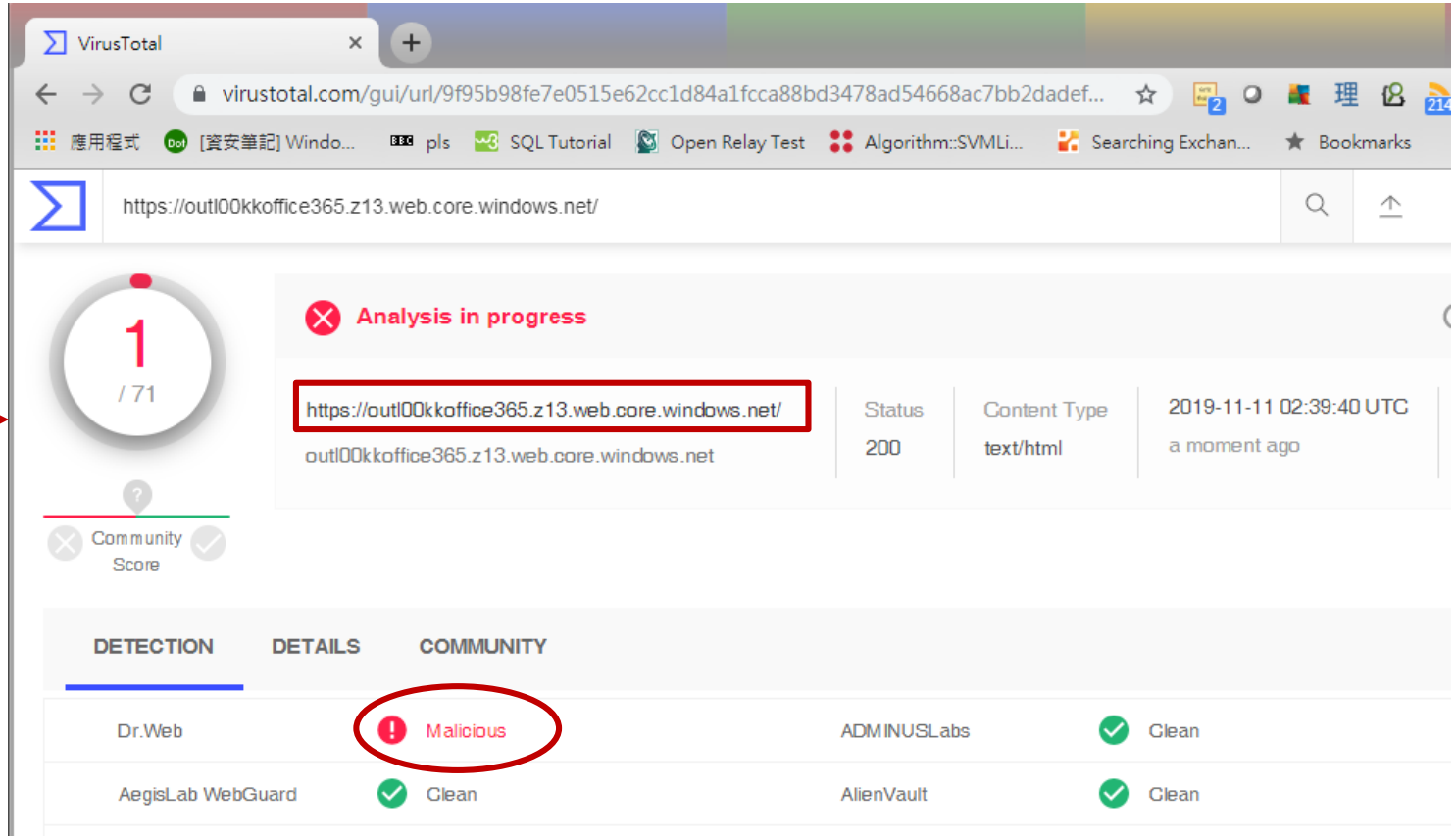


- 仿造寄信者為admin@ntu.edu.tw
- 騙取使用者點選信中連結以聆聽「電話留言」

實際寄信來源mail server

From admin@ntu.edu.tw Mon Nov 11 10:18:26 2019
X-IronPort-RCPT-TO:
Received: from dicksonfletcher6.pserver.ru (HELO slot0.tscnl.com) ([80.85.157.253])
by mailgw2.ntu.edu.tw with ESMTP; 11 Nov 2019 10:18:25 +0800
From: admin@ntu.edu.tw
To: tay@ntu.edu.tw
Subject: +65 1067 63xx Connection Messaging System
Date: 11 Nov 2019 02:18:23 +0000
Message-ID: <20191111021823.26F2EC596A310535@ntu.edu.tw>
MIME-Version: 1.0
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

將信中連結送到virustotal檢查



From: Help Desk [mailto:helpdeck@ntu.edu.tw]
Sent: Friday, December 13, 2019 7:20 AM
To: Subject: Mail Alert!

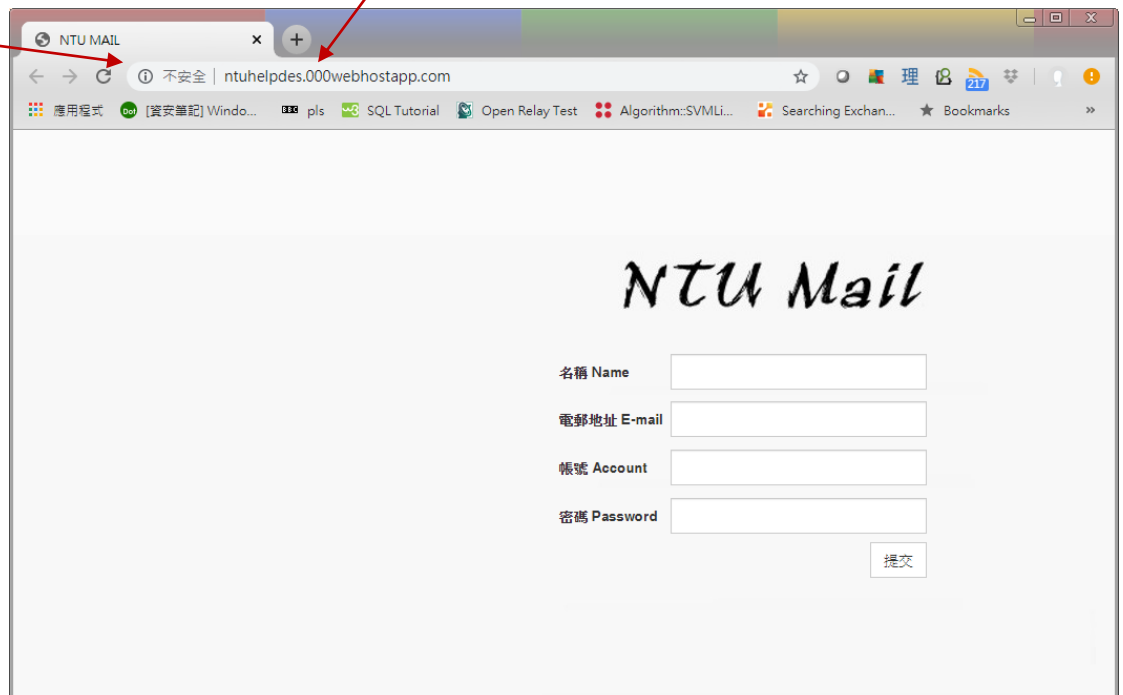
親愛的同事們，

由於最新的欺詐性網絡釣魚電子郵件病毒，所有用戶必須更新其電子郵件以自動清理其郵箱和設備。

點擊這裡

謝謝，
服務台

http://ntuhelpdes.000webhostapp.com/



仿冒 security@ntu.edu.tw
名義寄信

仿冒有NTU字眼的網址

寄件者:
寄件日期: 2023年4月18日 上午 04:07:11
主旨: 提醒通知

通知！

我們通知您，您的電子郵件位址將很快被暫停，因為您一直忽略我們發送給您的所有更新。

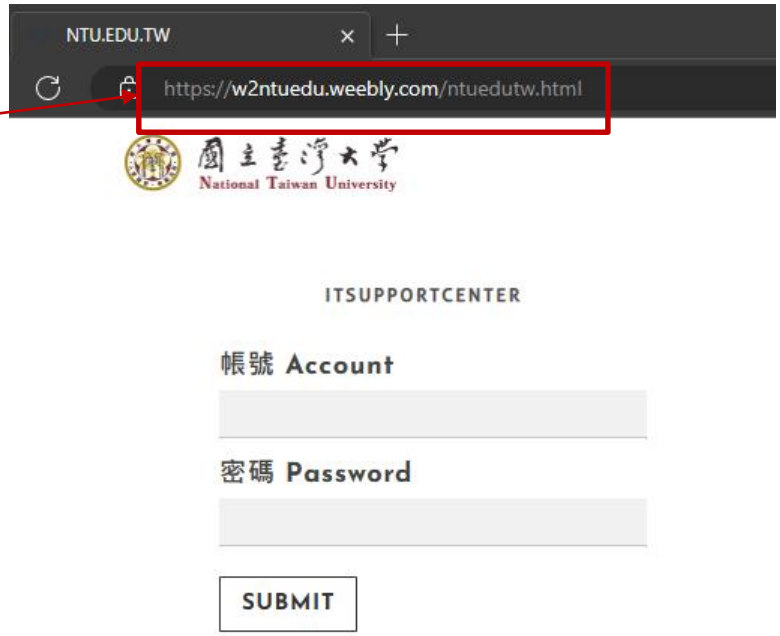
如果您希望繼續使用您的帳戶，請立即更新以繼續使用我們的服務。

這是更新電子郵件的連結

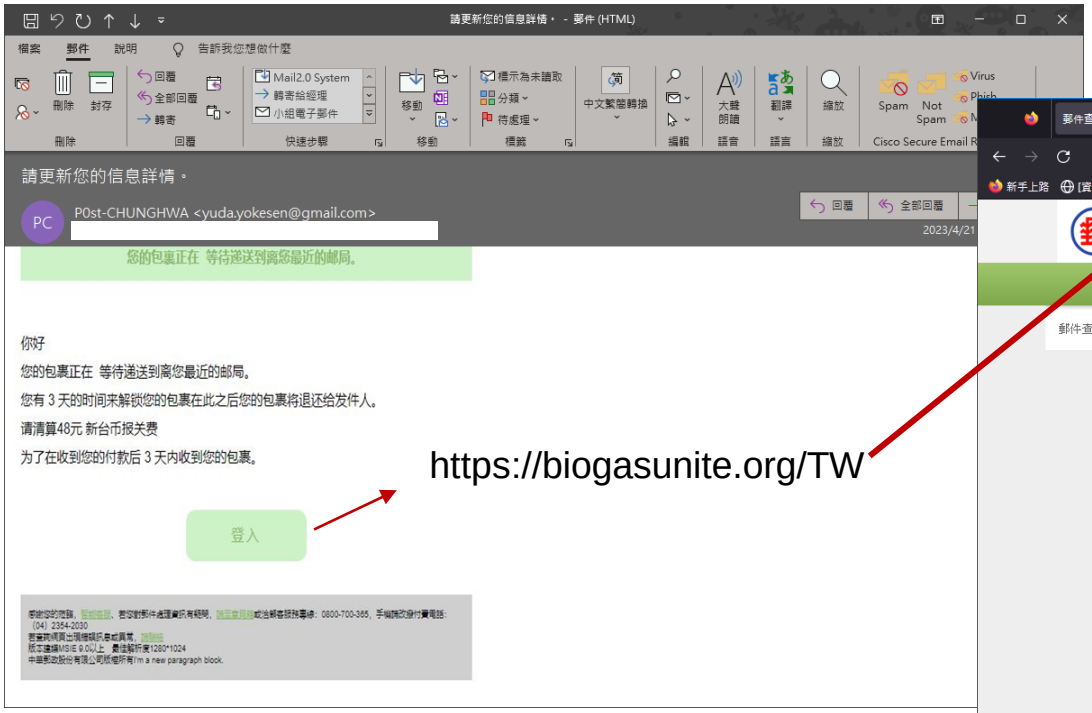
注意：忽略此消息將導致您的帳戶在當天未經您的許可而被暫停。

最好

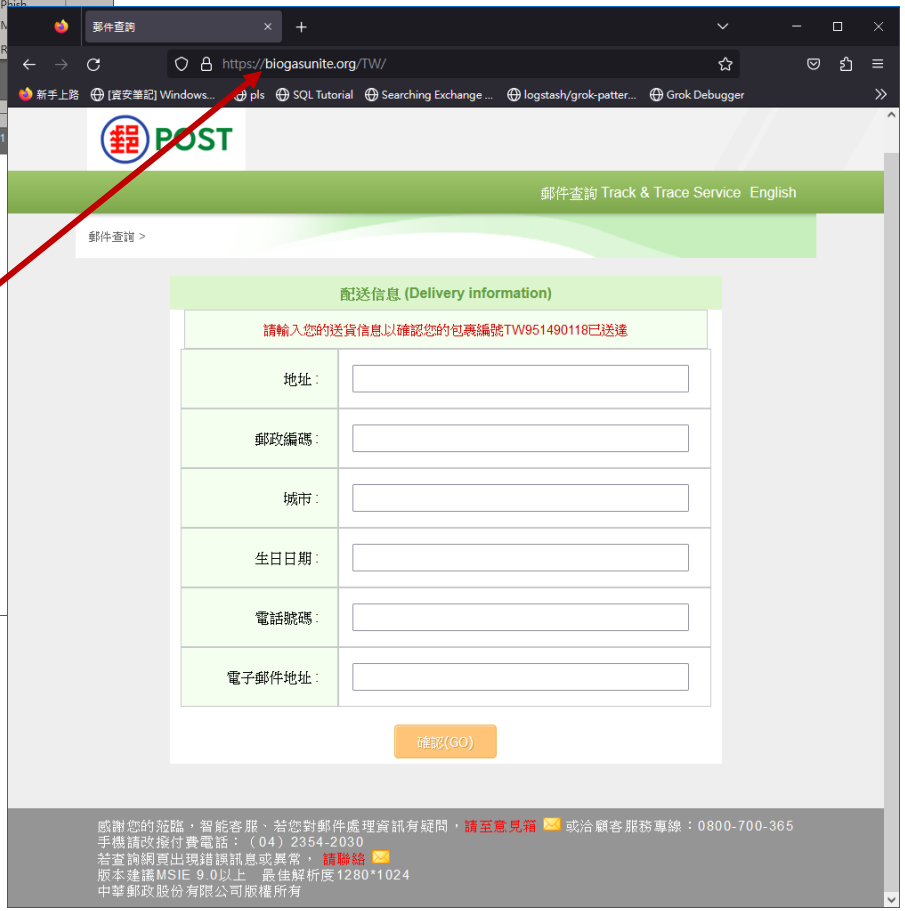
©2023 ITNtumail.edu



仿冒郵局信件



https://biogasunite.org/TW



恐嚇詐騙信件

[redacted]

Hello!
I am a hacker who has access to your operating system.
I also have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why did your antivirus not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of $1000 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: bc1qc5uqp7y0gv4f6mhq0xaxqqdg95mx7dwyn76avx

After receiving the payment, I will delete the video and you will never hear me again.
I give you 50 hours (more than 2 days) to pay.
I have a notice reading this letter, and the timer will work when you see this letter.

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.

Best regards!

suspected SPAM安全通知。 有人可以访问您的文件。

於 2021-12-25 11:25，寄自 sonali@ganti.com
詳情 純文字

您好！

我是一名黑客，我已经成功侵入了您的操作系统。
我也拥有您账号的完整访问权限。
我已经偷偷观察了您好几个月了。

事实是，因为您访问过的一个成人网站，您的电脑已经感染了恶意软件。

您可能不懂这是什么意思，让我来给您解释一下。
木马病毒能够让我获得某台电脑或其它设备的完整访问权限。
这意味着，我能在您不知道的情况下，看到您屏幕上的所有东西，并打开您的摄像头和麦克风。
我还能看到您所有的联系人信息和您所有的邮件往来。

为什么您的杀毒软件没有检测到恶意软件呢？
解答：我使用的是基于驱动的恶意软件，我每隔四个小时会更新一次它的签名，所以您的杀毒软件无法检测到它的存在。
我制作了一部视频，这部视频的左半边显示的是您正在取悦您自己的场景，而它的右半边显示的则是您当时正在观看的视频。

只要点击一下鼠标，我就能把这部视频发给跟您有来往的所有邮箱地址，以及您社交网络上的所有联系人。
我还可以公开您所有的电子邮件和您使用的聊天软件上的聊天记录。

如果您不想发生这样的事情的话， 那么就请将价值1450美金的比特币汇入我的比特币账户（如果您不知道如何操作的话，只需在谷歌上搜索："购买比特币"）。

我的比特币账户信息（比特币钱包）为： 1FtVfUoDvWVJ51oLLz8mSdd1wrSbcQKoBf

在收到钱款后，我会马上删除此视频，并永远从您的生活中消失。
请在50个小时（超过2天）内完成付款。 在您看到这封邮件后，我会立即收到一个提示，而50个小时的倒数计

恐嚇詐騙信件

計算機及資訊網路中心
Computer and Information Networking Center

最新消息 關於我們 服務陣容 服務資源 常見問答 聯絡我們

首頁 › 最新消息 › 重要資安警訊 ›

最新消息

- 重要資安警訊
- 疫情因應專區
- 校園公告
- 焦點新聞
- 中心電子報
- 校園聯播
- 失物招領

NEED HELP?

諮詢熱線:
(02)3366-5022
(02)3366-5023

諮詢信箱:

重要資安警訊

變臉偽照恐嚇勒索信件，請教職員生提高警覺!

上版日期：2023-03-28

最近部分大專院校發生教授收到勒索恐嚇郵件(訊息)之事件，為勒索集團利用深偽技術(Deep Fake)將受害者臉孔偽造成不雅照進行恐嚇勒索。深偽技術(Deep Fake)是結合人工智慧(AI，artificial intelligence)、深度學習(deep learning)與偽造(fake)技術的應用，許多有心人士藉由Deep Fake軟體合成幾可亂真的圖片、聲音或影片，讓受害者形象深陷危機。

提醒本校教職員生若收到類似恐嚇郵件請立即回報本校資安聯絡窗口(security@ntu.edu.tw)。

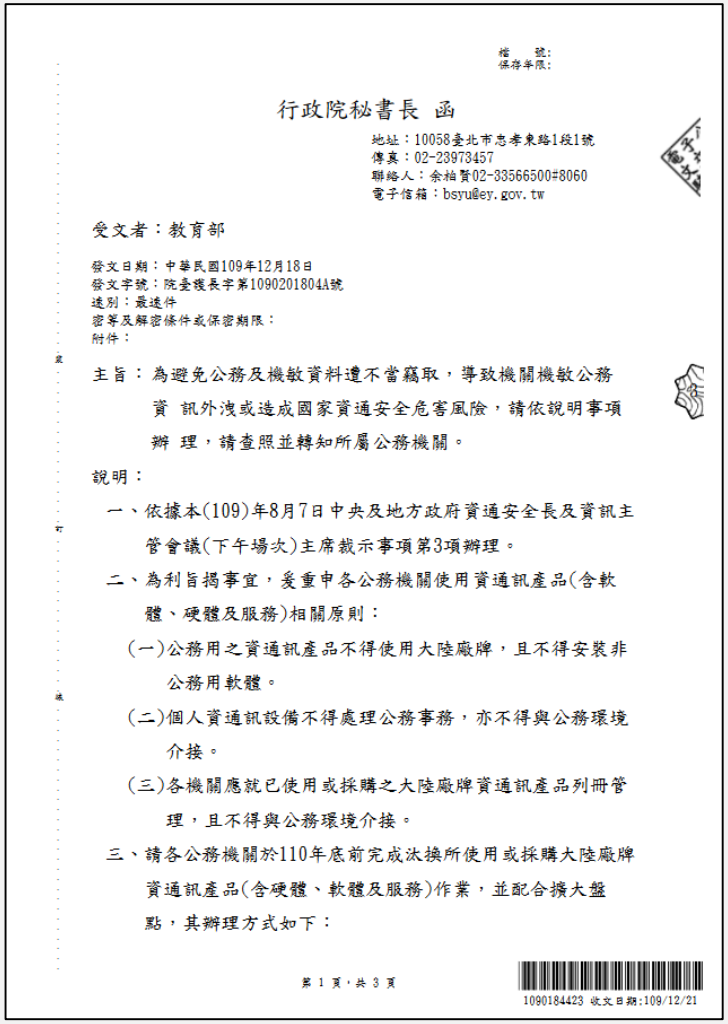
建議措施：

- 為保障自身權益，於網路上張貼照片時建議應加上浮水印，避免被盜用。
- 收到勒索郵件或訊息時請勿驚慌，並立即通報本校資安聯絡窗口(security@ntu.edu.tw)。
- 收到陌生來信應加強警覺。


大陸製品 海康威視

禁用陸製品

- 鑑於物聯網設備應用蓬勃發展，**行政院**指示公務用之資通訊產品(含軟體、硬體及服務)**不得使用大陸廠牌**，以避免機關機敏公務資訊外洩或造成國家資通安全危害風險。
- **管理介面**暴露在**公開網路**上。



檔　號:
保存年限:

行政院秘書長 函

地址：10058臺北市忠孝東路1段1號
傳真：02-23973457
聯絡人：余柏賢02-33566500#8060
電子信箱：bsyu@ey.gov.tw

受文者：教育部

發文日期：中華民國109年12月18日
發文字號：院臺機長字第1090201804A號
速別：最速件
密等及解密條件或保密期限：
附件：

主旨：為避免公務及機敏資料遭不當竊取，導致機關機敏公務資　訊外洩或造成國家資通安全危害風險，請依說明事項辦　理，請查照並轉知所屬公務機關。

說明：

一、依據本(109)年8月7日中央及地方政府資通安全長及資訊主管會議(下午場次)主席裁示事項第3項辦理。

二、為利旨揭事宜，爰重申各公務機關使用資通訊產品(含軟體、硬體及服務)相關原則：

(一)公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。

(二)個人資通訊設備不得處理公務事務，亦不得與公務環境介接。

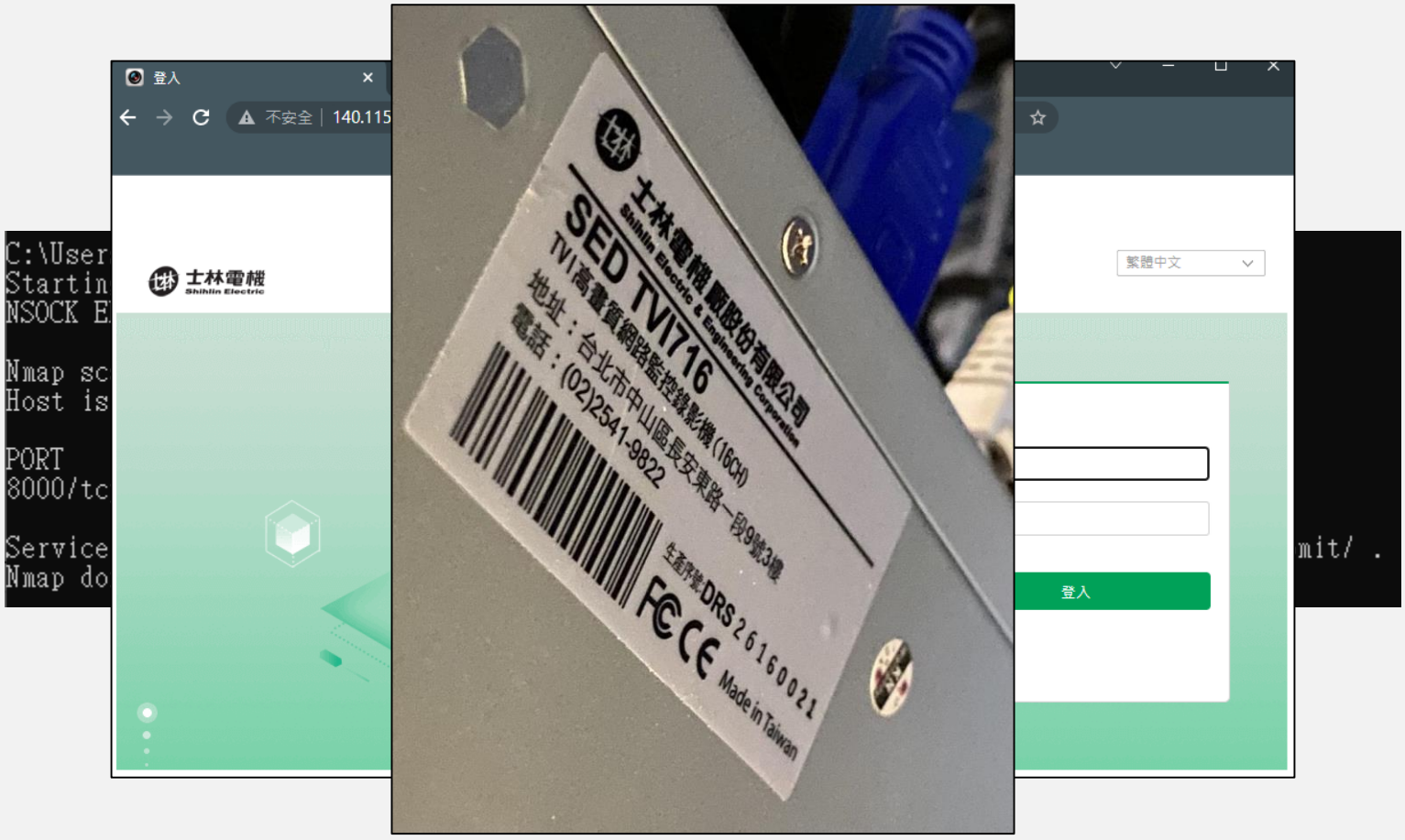
(三)各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

三、請各公務機關於110年底前完成汰換所使用或採購大陸廠牌資通訊產品(含硬體、軟體及服務)作業，並配合擴大盤點，其辦理方式如下：

第 1 頁，共 3 頁

1090184423 收文日期:109/12/21

檢測出非海康威視頁面



圖片來源:https://www.cw.com.tw/graphics/surveillance-and-security-2022/

大陸製設備與臺製設備

7大證據揭露：MIT主機是中國製貼牌

台灣Benelink、中國海康監視器主機拆機實測

天下雜誌 CommonWealth Magazine

BENELINK　　HIKVISION 海康威視

Benelink | 海康威視

```
<?xml version="1.0" encoding="UTF-8" ?>
<DeviceInfo version="1.0" xmlns="http://www.std-cgi.com/ver20/XMLSchema">
  <deviceName> Embedded Net DVR </deviceName>
  <deviceID> [redacted] </deviceID>
  <model>DFT6016E </model>
  <serialNumber> [redacted] </serialNumber>
  <macAddress> [redacted] </macAddress>
  <firmwareVersion>V4.21.002 </firmwareVersion>
  <firmwareReleasedDate>build 191230 </firmwareReleasedDate>
  <encoderVersion> V5.0 </encoderVersion>
  <encoderReleasedDate>build 191120 </encoderReleasedDate>
  <deviceType> IPC </deviceType>
  <telecontrolID> 255 </telecontrolID>
  <hardwareVersion> 0×20e4400 </hardwareVersion>
</DeviceInfo>
```

Benelink | 海康威視

```
<?xml version="1.0" encoding="UTF-8" ?>
<DeviceInfo version="1.0" xmlns="http://www.hikvision.com/ver20/XMLSchema">
  <deviceName> Embedded Net DVR </deviceName>
  <deviceID> [redacted] </deviceID>
  <model>DS-7216HQHI-K1/E </model>
  <serialNumber> [redacted] </serialNumber>
  <macAddress> [redacted] </macAddress>
  <firmwareVersion>V4.21.120 </firmwareVersion>
  <firmwareReleasedDate>build 210408 </firmwareReleasedDate>
  <encoderVersion> V5.0 </encoderVersion>
  <encoderReleasedDate>build 200727 </encoderReleasedDate>
  <deviceType> IPC </deviceType>
  <telecontrolID> 255 </telecontrolID>
  <hardwareVersion> 0×20e4400 </hardwareVersion>
</DeviceInfo>
```

- Benelink的生產公司欣永成承認是海思晶片，但表示抹去晶片logo、序號是海康產品常規，與公司無關

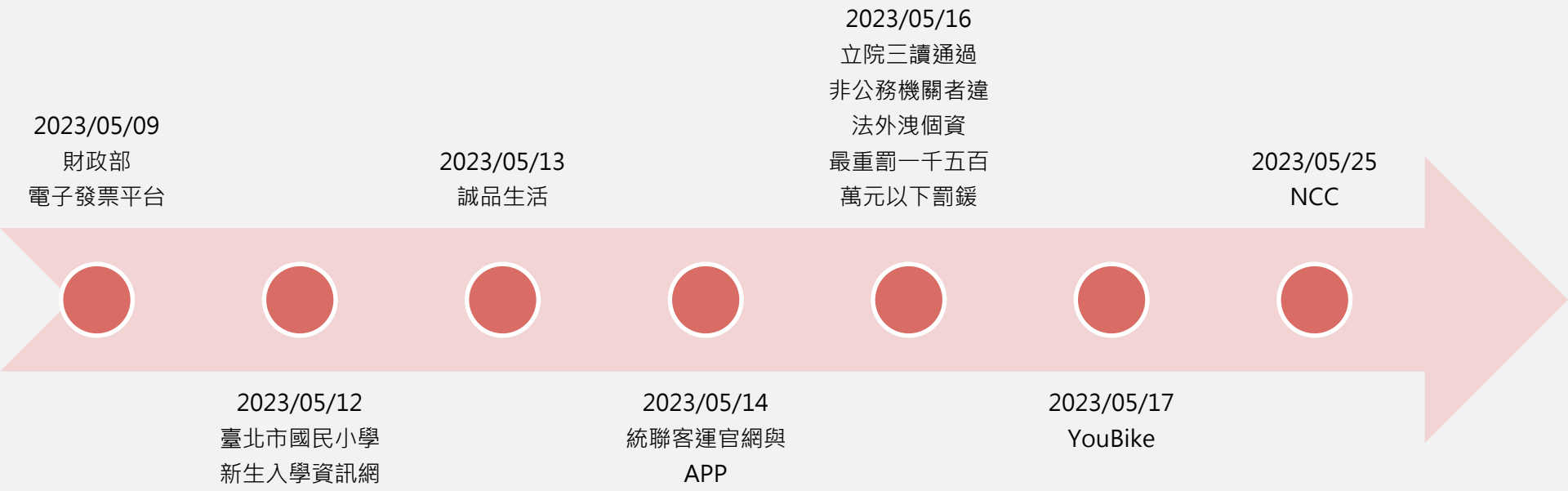
圖片來源:https://www.cw.com.tw/article/5122864

個資外洩

個資外洩事件頻傳

圖片來源：Google新聞

近期個資外洩時間軸


2023/05/09
財政部
電子發票平台
2023/05/12
臺北市國民小學
新生入學資訊網
2023/05/13
誠品生活
2023/05/14
統聯客運官網與
APP
2023/05/16
立院三讀通過
非公務機關者違
法外洩個資
最重罰一千五百
萬元以下罰鍰
2023/05/17
YouBike
2023/05/25
NCC

近期資料外洩數量

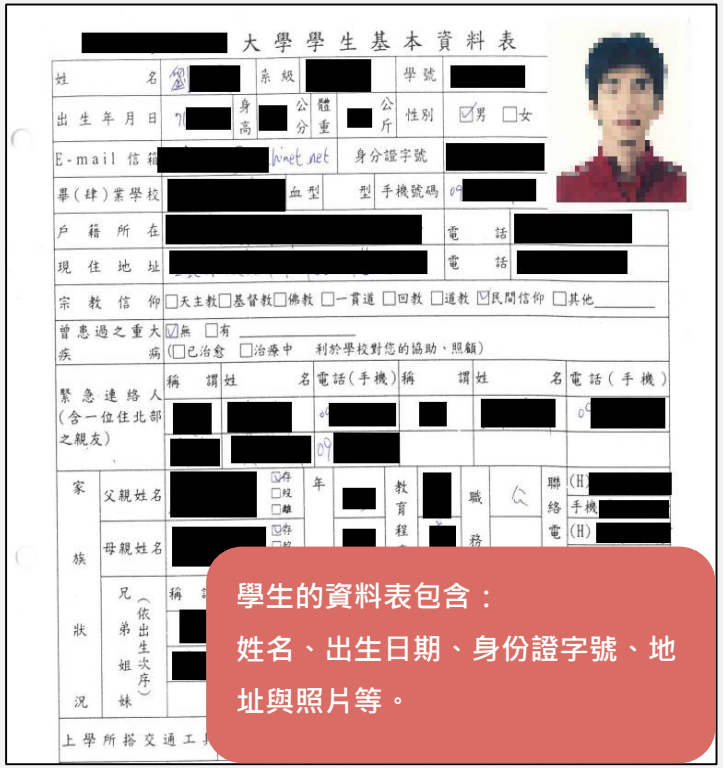
時間	單位	資料外洩	備註	罰鍰
2023/05/09	財政部 電子發票平台	公司名稱、往來廠商的發票與金額	帳號密碼預設為同一組	數發布提出改善專案報告
2023/05/12	臺北市國民小學新生入學資訊網	學生姓名、戶籍地址、設籍學校與設籍日期	變更就學編號可看到他人個資	
2023/05/13	誠品生活	姓名、電話、購書清單		10萬元
2023/05/14	統聯客運官網與APP	姓名、身分證字號、生日與電話		
2023/05/17	YouBike	姓名、電話、騎乘紀錄與電子票證卡號	遭駭客入侵 發放每個會員500元騎乘券	
2023/05/25	NCC 申報進口貨品網站	姓名、電話、身分證字號、地址	輸入報單號碼更改其尾號，便可看到其他人填的資料	
蝦皮		姓名、電話、消費資料與付款方式		20萬元

建議措施

- 避免將設備的**管理介面**暴露於**公開網路**上。
- 應定期(或請廠商協助)檢視組態設定是否符合資安要求。
- 採購設備時應請廠商修補已知的漏洞。
- 定期執行設置檔備份與更新韌體。
- 機敏性資料應作適當的遮罩。
- 重要系統(尤其是包含機敏性資料)應做完弱點與源碼檢測後再上線。

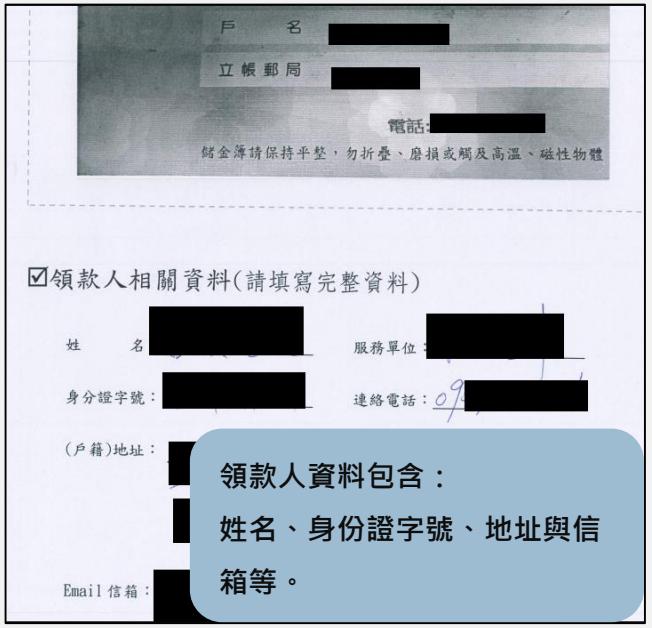
FTP設備匿名登入(弱密碼)

FTP 登入檢測(包含個資的案例)



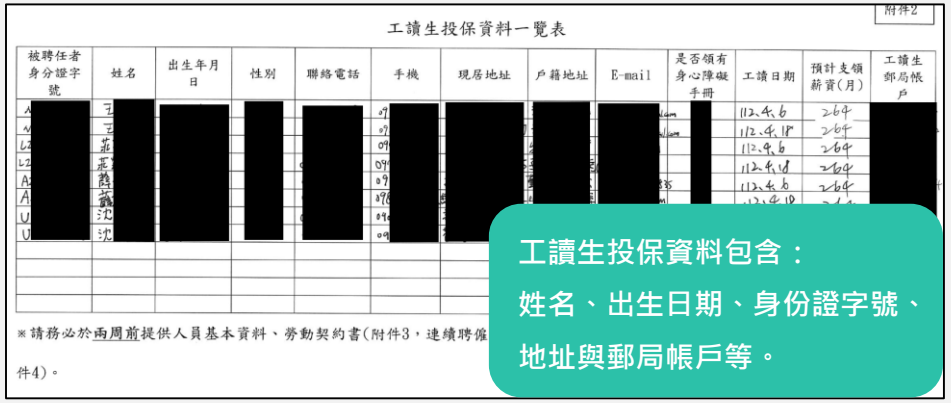
大學學生基本資料表

學生的資料表包含：
姓名、出生日期、身份證字號、地址與照片等。



☑領款人相關資料(請填寫完整資料)

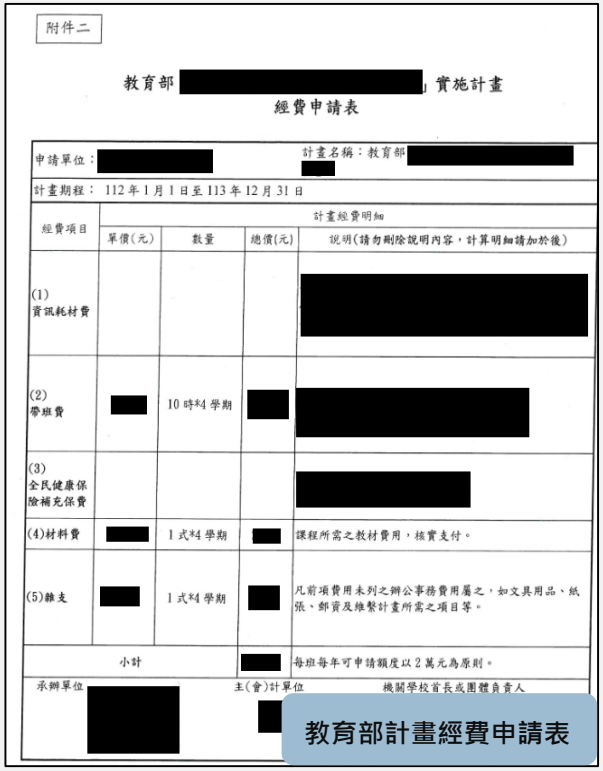
領款人資料包含：
姓名、身份證字號、地址與信箱等。



工讀生投保資料一覽表

工讀生投保資料包含：
姓名、出生日期、身份證字號、地址與郵局帳戶等。

FTP 登入檢測(包含敏感資料的案例)



附件二

教育部 [redacted] 實施計畫

經費申請表

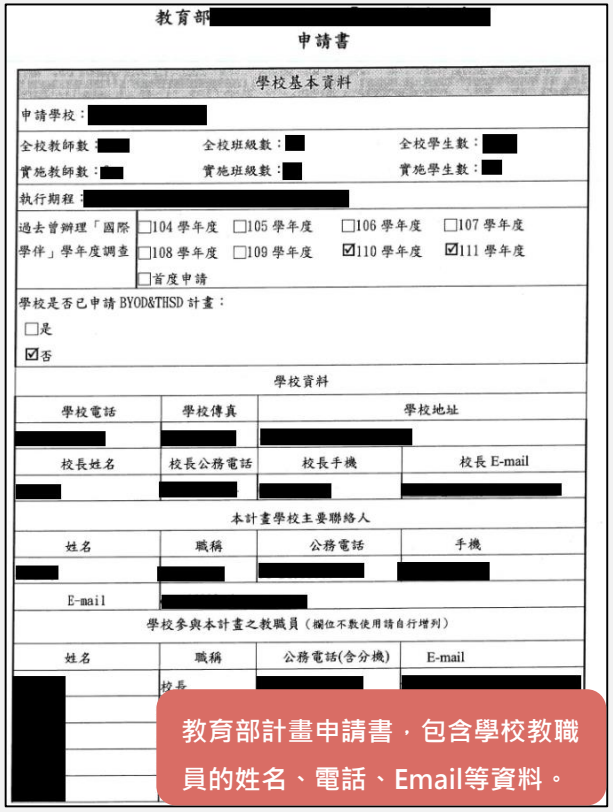
申請單位：[redacted]　計畫名稱：教育部 [redacted]

計畫期程： 112 年 1 月 1 日至 113 年 12 月 31 日

經費項目	計畫經費明細			
	單價(元)	數量	總價(元)	說明(請勿刪除說明內容，計算明細請加於後)
(1) 資訊耗材費				[redacted]
(2) 帶班費	[redacted]	10 時/1 學期	[redacted]	[redacted]
(3) 全民健康保險補充保費				[redacted]
(4)材料費	[redacted]	1 式/1 學期	[redacted]	課程所需之教材費用，核實支付。
(5)雜支	[redacted]	1 式/1 學期	[redacted]	凡前項費用未列之辦公事務費用屬之，如文具用品、紙張、郵資及維繫計畫所需之項目等。
小計			[redacted]	每班每年可申請額度以 2 萬元為原則。

承辦單位　主(會)計單位　機關學校首長或團體負責人

教育部計畫經費申請表



教育部 [redacted]

申請書

學校基本資料

申請學校：[redacted]

全校教師數：[redacted]　全校班級數：[redacted]　全校學生數：[redacted]

實施教師數：[redacted]　實施班級數：[redacted]　實施學生數：[redacted]

執行期程：[redacted]

過去曾辦理「國際學伴」學年度調查：☐104 學年度 ☐105 學年度 ☐106 學年度 ☐107 學年度 ☐108 學年度 ☐109 學年度 ☑110 學年度 ☑111 學年度 ☐首度申請

學校是否已申請 BYOD&THSD 計畫：

☐是

☑否

學校資料

學校電話	學校傳真	學校地址
[redacted]	[redacted]	[redacted]

校長姓名	校長公務電話	校長手機	校長 E-mail
[redacted]	[redacted]	[redacted]	[redacted]

本計畫學校主要聯絡人

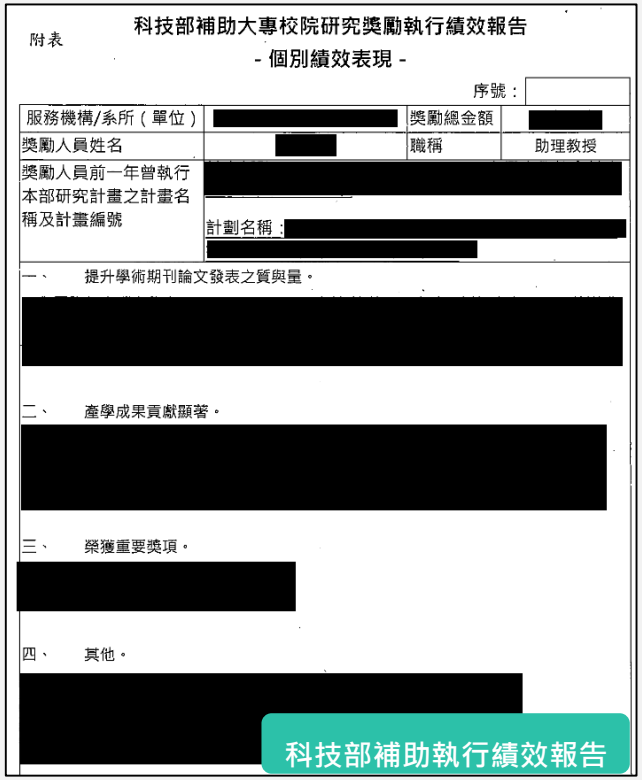
姓名	職稱	公務電話	手機
[redacted]	[redacted]	[redacted]	[redacted]

E-mail [redacted]

學校參與本計畫之教職員（欄位不敷使用請自行增列）

姓名	職稱	公務電話(含分機)	E-mail
[redacted]	校長	[redacted]	[redacted]

教育部計畫申請書，包含學校教職員的姓名、電話、Email等資料。



附表　科技部補助大專校院研究獎勵執行績效報告

- 個別績效表現 -

序號：

服務機構/系所（單位）	[redacted]	獎勵總金額	[redacted]
獎勵人員姓名	[redacted]	職稱	助理教授
獎勵人員前一年曾執行本部研究計畫之計畫名稱及計畫編號	[redacted]	計劃名稱：[redacted]	

一、 提升學術期刊論文發表之質與量。

[redacted]

二、 產學成果貢獻顯著。

[redacted]

三、 榮獲重要獎項。

[redacted]

四、 其他。

[redacted]

科技部補助執行績效報告

建議措施

- 建議將設備放置於內部網路，若有外部網路存取需求，請限定連線IP(ACL)。
- 關閉預設帳號與匿名登入服務，並使用強度較高的密碼。
- 若有放置機敏性資料的需求，請進行加密或作適當的遮罩，並於使用完畢後移除以降低風險。
- 依據檔案的重要性與機密性建立權限控管機制。
- 定期檢視系統稽核紀錄降低資安風險。

Q & A