## 電子郵件社交工程 及信箱安全性設定

國立政治大學 電子計算機中心 郭紫玫技士

2023.03



- 01

 $(\boldsymbol{r})$ 

## 社交工程 Social Engineering

利用人性弱點,應用簡單的溝通和欺騙技倆,以獲取帳號、通行碼、身分證號碼 或其他機敏資料,來突破校園的資通安全防護,遂行其非法的存取、破壞行為。

### 網路釣魚 誘騙使用者登入偽裝之網站 以騙取帳號及通行碼等機敏 資料。

#### 垃圾郵件

利用電子郵件誘騙使用者開 啟檔案、圖片或連結,以植 入惡意程式、暗中收集機敏 性資料。



( > )

- 02

#### 不明的軟體

利用提供工具、檔案、圖片 為幌子,誘騙使用者下載, 如偽裝的修補程式、p2p下 載軟體、工具軟體等,乘機 植入惡意程式、暗中收集機 敏性資料。

## 垃圾郵件

### 電子郵件是最適合做社交工程攻擊的工具

- 可偽裝寄件者
- 低成本且可大量發送
- 容易使用,無技術門檻
- 可輕易利用被害者協助攻擊他人的電子郵件, ex:轉寄電子郵件給親友、同事

最喜歡利用最熱門的新聞時事發動攻擊 2020年3月,美國聯邦調查局(FBI) 發布的新聞稿: 以新冠病毒(COVID-19)為主題的詐騙攻擊正持續 地增加。網路罪犯利用新冠病毒全球大流行之事件, 對企業及政府發動社交工程攻擊。



I-032020-PSA Questions regarding this PSA should be directed to your local

Alert Number

FBI Field Office.

Local Field Office Locations: www.fbi.gov/contact-us/field



::: 骨回首頁 ♀English ▲網站導覽 承RSS

預防接種 國際旅遊與健康

#### 防詐騙!指揮中心從未發「最終通知」,接獲不明郵件勿開啟



中央流行疫情指揮中心今(4)日表示,近期接獲民眾陸續反映,收到以疾病管制署(notices@cdc.gov.tw)名義發送,主旨為「台湾疾病預防控制中心的最终 的電子郵件。在此呼籲民眾提高警戒,疾管署並不會以郵件通知進行COVID-19(武漢肺炎)相關檢測,請民眾勿開啟此類信件、點擊信件內連結或附

### **Public Service Announcement**

FEDERAL BUREAU OF INVESTIGATION

March 20, 2020

#### FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following:

Fake CDC Emails. Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.





1. 檢查寄件者名稱與信箱 3. 檢查郵件內的連結是否正確 使用密件傳送



# 如何防範電子郵件 社交工程

- 不開啟來路不明的電子郵件及附加檔案
  - 2. 以郵件主旨評估是否有必要開啟郵件 4. 檢查郵件附檔的副檔名, 是否為常見可含 有病毒的檔案名稱, ex: \*.bat、\*.pif、 \*.exe、\*.zip、\*.src、\*.cmd、\*.rar等
  - 5.轉寄郵件時刪除寄件者與收件者資料,並



## 教育部社交工程演練

### 資通安全事件通報及應變辦法 §8: 每半年辦理一次社交工程演練。

- 社交工程為駭客常用入侵管道,透過電子郵件夾帶惡意程式或連結網址等方式,輔以 吸引人之信件主旨及內容,誘使缺乏警戒心的使用者開啟後造成進一步破壞,嚴重損 害機關或個人之權益。
- 演練方式為模擬駭客寄送各種誘騙的測試信件給本校同仁,測試受測者之資安意識。
- 透過實施演練,提升教育體系人員針對社交工程攻擊之警覺性,降低社交工程風險。
- 參與演練人員為學校全體人員(具備公務電子郵件帳號者),不限於正式公務人員。
- 依據本校資訊安全推行委員會第十八次會議決議,「違反社交工程」之教職員生,將 強制選讀相關資訊安全課程。

( > )

- 05

### 教育部社交工程演練 110年演練期間:5月~11月間進行2次

 依規定提交之演練人員名單,按人員類型隨機選取100人,主管人員(組長)以上原 則佔受測人員總數35%以上。



1.不預覽信件 2. 純文字讀取 3. 封鎖圖片







 $(\boldsymbol{>})$ 

檢查副檔名

## 不能 「開啟/預覽」 郵件?

您可能覺得只要不開郵件附件 和不點擊連結,就不會中招...

- 程式。

### • 但有些惡意程式是利用ActiveX功能來 執行的,而HTML可以撰寫ActiveX。

( > )

- 07

● 若您的電子郵件是HTML格式,只要瀏 覽電子郵件,就會觸發裡面的ActiveX 執行,連結到惡意程式網站下載病毒

Q:看不見郵件內容,如何判斷是否為 社交工程郵件? A:以「純文字格式讀取」瀏覽內容取

代HTML格式







- 09

 $(\boldsymbol{\flat})$ 

## 案例1-偽造的信件及釣魚網頁

尊敬的電子郵件帳戶用戶, 您的郵箱已超出電子郵件幫助設置所設置的存儲空間限制,您必須重新驗證以接收新	• 雖已檢查寄件者
郵件。 單擊此 <u>https://taiwan3232424.cabanova.com/index.html</u>	已遭駭客登入。
注意:如果您不回复此電子郵件,我們的數據庫將禁用您的帳戶,並且您將不再接收 或發送電子郵 件。	• 應檢查連結網圠
很抱歉給您帶來不便。 版權 2021 台灣電子郵件網絡郵件服務台 版權所有	×
From:糸統管理者< <u>@nccu.edu.tw</u> > Date: Thu, 23 Sep 2021 06:50:31 Subject: 重要通知	A
From:糸統管理者< <u>@nccu.edu.tw</u> > Date: Thu, 23 Sep 2021 06:50:31 Subject: 重要通知 親愛的用戶	
From: 糸統管理者< <u>@nccu.edu.tw</u> > Date: Thu, 23 Sep 2021 06:50:31 Subject: 重要通知 親愛的用戶 我們注意到您的郵箱出現了一些未經授權的登錄嘗試。 因此,我們建議您立即驗證 您的帳戶。 請單擊下面的鏈接並使用您的評細信息宜錄,以避免您的帳戶。 感謝您幫助我們保護您。 點擊這裡 >> < <u>https://virl.ws/s/nccu-edu-tw/</u> >	
From:系統管理者< <u>@nccu.edu.tw</u> > Date: Thu, 23 Sep 2021 06:50:31 Subject: 重要通知 親愛的用戶 我們注意到您的郵箱出現了一些未經授權的登錄嘗試。 因此,我們建議您立即驗證 您的帳戶。 請單擊下面的鏈接並使用您的評細信息意意琢,以避免您的帳戶被禁用。 感謝您幫助我們保護您。 點擊這裡 >> < <u>https://virl.ws/s/nccu-edu-tw/</u> > NCCU 管理團隊 © 2021 國立政治大學。 版權所有。	

本校Email網址 https://nccu.edu.tw/indexs.html



#### **备校內信箱,但實際上該信箱**



 $(\boldsymbol{>})$ 



## 案例2一收到寄件者顯示自己信箱的恐嚇信

- 可透過mail2000信箱查看最近的IP登入紀錄 •
- 有無異常的IP登入紀錄 •



• 有: 表示確實遭駭客入侵, 應**立即更換email密碼** 



- 無: 表示對方冒用您的email名義寄出 (在電子郵件機制中, 寄件者是可以修改自己 的寄件人顯示名稱/帳號的)
- 長期對策: •
  - ・基本MailGates(郵件過濾系統)會過濾此種異常信件,**勿將自己的信箱設定為白名**單, 就不會收到學校以外的信件以自己帳號名義寄信過來了。
  - 因為MailGates系統只會過濾校外email主機寄來的郵件,透過學校信箱寄信給自己仍 是可以收到的!



資訊			$\otimes$
/06/20 09:13:03	網頁登入	140.119	
/06/17 09:36:03	網頁登入	140.119	
/05/18 09:07:55	網頁登入失敗	140.119	
/05/05 16:03:13	網頁登入失敗	140.119	
			觀看完整登入記錄

( > )







## 電子郵件信箱 安全性設定

**—** 12

 $(\boldsymbol{\flat})$ 

### 安全性設定/校園電子郵件信箱Mail2000

Þ

....

Ð

E

#### Openfind™ **MAIL2000**

使用環境 寫信 一般 郵件 撰寫 POP3 收信 信件匣 -通訊錄 雲端硬碟 信箱服務 上下分割模式 左右分割模式 個人設定 ◎開閉 ○開啟 信件自動預覽 信箱安全 ۱ 🛱 純文字 🗸 預設請信方式 2. 純文字讀取 ▼ 🌿 個人化設定 全部封鎖 封鎖外部圖檔  $\mathbf{v}$  個人資料 山内文園片要封親 快捷列 □ 已讀信件不封鎖 使用環境 □ 好友信件不封鎖 信件與附檔檢視列表 每頁顯示的信件數量 50 > 封 • 面板風格 刪信後到信件列表▼ 刑信返回設定 槽籤管理 登入時 不收取 ✔ 外部信件 自動收取外部信件 • 左側功能選單 登出時 不刪除 ✔ 回收筒内的信件 自動清理回收筒 ▶ 🔁 信件處理 5分鐘 ¥ 新信通知 ▶ 🚫 簡易廣告信過濾



(>)

### 1. 關閉信件預覽功能

### 3. 封鎖圖片/關閉自動下載圖片功能

#### $(\boldsymbol{)}$ 安全性設定/教育版Gmail信箱 G Suite (g.nccu.edu.tw) 1-50列(共列) < > 快速設定 查看所有設定

= 衬 Gmail	<b>Q</b> 搜尋郵件			•
_ 撰寫	□ - C :			
•	□ 主要	<b>20.</b> 社交網路	● 最新快訊	
□ 收件匣			•	

#### 1. 關閉信件預覽功能

一般設定 標籤	收件匣 帳戶 篩選器和封鎖的地址 轉寄和 POP/	IMAP 外掛程式 即時通訊和視訊會議
閱讀窗格:	〇 啟用閱讀窗格 - 設用這個選項可在會話 到更多郵件内又。	群組清單旁顯示閱讀窗格,這不但能讓你更
	閱讀窗格位置	

#### 2. 封鎖圖片/關閉自動下載圖片功能





14

## **安全性設定/**Microsoft Outlook信箱 (2010、2013、2016)

#### 1. 關閉信件預覽功能

e		÷						收件匣 -			
檔案	常用	傳送 /	接收	資料夾	檢視	ESET	Acrobat	♀ 告訴我您想到	要執行的動作		
<b>ら</b> 變更檢視	<b>☆</b> 檢視設定	い 重設檢視		順示為交談 交談設定、	- 記息 福管→	<sup>15</sup> 3 日期(D) Ⅰ日 大小(S)	日本	♀	<ul> <li>▲ ↓ 反向排序</li> <li>▼ ➡ 新増欄</li> <li>▼ ➡ 展開/折壘 ▼</li> </ul>	■ 資料衣 窗格	讀頭
	目前檢視			郵件	331.212		排列	方式			
▲我的:	最愛			< 4	全部未言	讀取					
收件回	E			!	0 9 0	寄件者	主旨				
寄件債	前份				日期:今	大					



### 安全性設定/Microsoft Outlook信箱



Outlook 選項	? ×
一般 郵件	協助您維護文件的安全,並讓您的電腦維持在安全和良好的狀態。
行事層	安全性和其他
人員	造訪 Office.com 以瞭解更多關於保護您的隱私權和安全性的資訊。
工作	Microsoft 高可信度電腦運算
搜尋	
語言	Microsoft Outlook 信任中心
進階	信任中心包含安全性和隱私權設定。這些設定將協 <mark>制</mark> 您 保持電腦的安全性。我們建議您不要變更這些設定 信任中心設定(D)
自訂功能區	
快速存取工具列	
増益集	
信任中心	
	確定 取消



資訊

 $(\leftarrow)$ 

開啟和匯出

另存新檔

儲存為 Adobe PDF

儲存附件

列印

Office 帳戶

選項

結束

信任中心	? ×
受信任的發行者 隱私選項 電子郵件安全性	當開啟 HTML 電子郵件訊息時,您可以控制 Outlook 是否自動下載及顯示圖 片。 封鎖電子郵件訊息中的圖片,可協助保護您的隱私。HTML 電子郵件中的圖片, 會要求 Outlook 從伺服器下載圖片。利用此種方式與外部伺服器通訊,可讓寄 供者驗證你的電子習供他也是否有效。因而可能讓你式先這項習供的目標
自動下載	✓ 不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片(D)
巨集設定 以程式設計方式存取	✓ 允許垃圾郵件師選中,[女宝的寄件者] 清単定義的寄件者所寄出, 或寄給[安全的收件者] 清單定義的收件者之電子郵件訊息的下載 (S)
	✓ 允許自這個安全性區域的網站下載(P): 信任的區域 ✓ 允許 RSS 項目中的下載(R) ✓ 公許 ShareBoint 討論原中的下載(P)
	✓ 九軒 sharePoint 討論區中的下戰(回) ✓ 當編輯、轉寄或回覆電子郵件時,在下載內容前先警告我(W)

 $(\boldsymbol{>})$ 

— 16

<b>信任中心</b>		?	×
受信任的發行者	加密的電子郵件		
電子郵件安全性	<ul> <li>♀</li> <li>□ 加密外寄郵件的內容及附件(E)</li> <li>□ 在外寄郵件加入數位簽章(D)</li> </ul>		
附件處理	✓ 當傳送簽章郵件時傳送純文字簽章郵件① ○ 為所有 \$/MIME 答章郵件表取 \$/MIME 回修(B)		
巨集設定	□ 為所为 S/WIWE 競手郵件変成 S/WIWE 国際低 預設設定	設定(S).	
以程式設計方式存取	數位 ID (憑證)		
	數位 ID 或憑證是在電子交易中供您證明身分的文件。 匯入/匯出(I) 取得數位 ID(G)		
	以純文字讀取	_	
	<ul> <li>✓ 以純文字讀取所有標準郵件(A)</li> <li>✓ 以純文字讀取所有數位簽章的郵件(M)</li> </ul>		

### 安全性設定/行動裝置郵件信箱

### iPhone郵件信箱

1. 關閉信件預覽功能 在收件匣列表中,「郵件」預設為顯示每封電子郵件的兩行文字 前往「設定」>「郵件」>「預覽」,然後選擇「無」

#### 2.不自動下載圖片

「設定」 >「郵件」> 取消選擇「載入遠端影像」

### Android郵件信箱

- 1. 關閉信件預覽功能
  - 「設定」 >「顯示」>「無」

### Gmail APP

#### 1. 不自動下載圖片

「<br/>
三」>「設定」>「數據用量」下方「圖片」>「顯示不明外部圖<br/>
片時,必須先詢問我」







**—** 18

 $(\boldsymbol{>})$ 





#### 搜尋所在信件匣







### シ 可疑信? ジ 當 MailGates 依據過濾規則無法判斷一封信為正常信或垃圾信時, 可依據使用者設定的處理原則,將信件直接刪除、做修改後繼續送至信箱, 或是將其留置在 MailGates 主機上。







( > ]

### 把可疑信加上TAG設定



( > )

雙重認證/登入 Mail2000 加強版安全機制 使用雙重驗證機制必須先在行動裝置安裝 @Mail2000 APP。 當使用帳號密碼登入後,系統會推播一組認證碼到註冊的手持裝置上,輸入該組認證碼方可 登入。

- 行動裝置
  - 1.透過 Google Play 下載並安裝 eMail2000 APP



### 2.eMail2000設定



## Web mail

<sup>Openfind™</sup> MAIL2000	
	1
寫信	
信件匣	
通訊錄	0
雲端硬碟	
信箱服務	
個人設定	
<ul> <li>▶ 由 信箱安全</li> <li>▼ 2 個人化設定</li> <li>● 個人資料</li> <li>● 快捷列</li> <li>● 使用環境</li> <li>● 使用環境</li> <li>● 面板風倍</li> <li>● 簽名檔</li> <li>● 標籤管理</li> <li>● 左側功能選單</li> </ul>	
<ul> <li>▶ ◎ 簡易廣告信過濾</li> </ul>	-

( > )

#### 「個人設定」>「使用環境」> 勾選「雙重驗證」 Ē 🔏 🌣 P **...** 搜尋所在信件匣 Q 22

#### 使用環境

信件資訊顯示模式	預設模式 ✔
登入顯示頁面	信箱資訊頁 🖌
編輯區顯示範圍	500x300 ✔ (不影響寫信編輯區)
連線失效時間	60分鐘 🗸
다 <mark>묘</mark>	(GMT+08:00) Asia/Taipei
雙重認證	〇 關閉 🧿 開啟
字型大小	標準 ✔
列表行距	標準 ✔
刘表行距	標準✔

## 平常的警覺性







— 23

 $(\boldsymbol{2})$ 

### 習慣性查看登入IP紀錄、信箱轉寄設定

1. 平常登入時看一眼登入紀錄, 留意有無異常IP的登入紀錄。(系統最多記錄登入成功及失敗 各100筆資訊)

2. 有遭駭客成功登入過的使用者,務必確認有無被設定自動轉寄信件至其他外部信箱。

Openfind™ MAIL2000	i 🖾 🖾	E E 🤜 🕈
	信箱資訊	
寫信	Image: Constraint of the second	
通訊錄	☆ 登入資訊	
雲端硬碟	2021/05/19 16:54:41	網頁登入 140.1
信箱服務	2021/05/19 16:49:44	細頁登入 140.1 細百登入失敗 140.1
個人設定	2021/05/11 08:59:36	網頁登入失敗 140.1
▶ 🖶 信箱安全 ▶ 🔧 個人化設定	信箱容量	
	● 雲端硬碟 :	0.00 MB
	● 信件使用:	428.34 MB
▶ 🛇 簡易廣音信過濾	/	9811.66 MB
	總量:	10240.00 MB





( > )









