

電子郵件社交工程



110教育部電子郵件社交工程演練

- 4月~11月，2次演練
- 校長、副校長、各級主管、行政人員

110教育部電子郵件社交工程演練

- 演練方式：偽冒公務、個人或公司行號發送
- 郵件主題：政治、公務、健康養生、旅遊、時事
- 郵件內容：連結網址、夾帶附檔

109年電子郵件社交工程演練結果-1

演練題目	點擊次數
公務類_108年公教人員健檢辦法	33
公務類_部務會報紀錄	12
健康類_讓熱量大降6成的密技·煮飯加一匙就行!	9
財經類_IPHONE12最速優惠	9
情色類_啦啦隊美波女神濕身走光	8
新奇類_從8個顏色中挑3種顏色 一秒看出「你的現況」	6
公務類_最新公告民國109年辦公日曆表搶先看	6
擬真類_食安展【最後150張】預約看展摸彩券	6
科技類_一口氣修補99個漏洞 Windows 10 有始以來最大更新	5
旅遊類_走進森林吸取芬多精殺菌趣! 精選八大自然系景點	4
公務類_108年公教人員健檢辦法	33

109年電子郵件社交工程演練結果-2

演練題目	開啟次數	點閱連結次數	附檔開啟次數
林奇峰 - 志願服務申請	21	9	16
【2020愛你愛你】活動報名事宜	7	0	0
MIT 國產口罩怎麼辨識？哪裡有賣？	7	2	2
桃園青埔 漫遊奇幻海洋	6	0	1
親子遊孩子為何擺臭臉？調查：九成小孩想參與規劃行程	5	1	0
2020三倍券懶人包一次看懂	4	0	0
109年公教人員健檢辦法	4	2	2
台股後勢看漲 看好四大類別	2	0	0
口罩解禁哪裡買？	2	1	1
美豬、美牛進口恐藏三大原因	2	0	0

避免社交工程攻擊

- 不開啟來路不明的電子郵件及附加檔案
- 不連結及登入未經確認的網站
- 不下載非法軟體及檔案
- 不要提供郵件密碼給任意人員或網站
- 未經確認絕不提供資料
- 請避免使用手機不小心的開啟惡意郵件

電子郵件安全維護

- 來路不明的超連結勿點選
- 嚴格把關附件開啟動作(注意副檔名[.exe])
- 關閉郵件預覽功能(outlook express)
- 不自動下載HTML電子郵件訊息或RSS項目中的圖片
- 檢視收件者清單(是否為群組發送)
- 檢視寄件者(是否業務相關?是否認識?)

WEBMAIL設定

- 個人設定->使用環境-> 郵件

一般 郵件 撰寫 POP3 收信 IMAP4 收信

讀信模式

上下分割模式 左右分割模式 整頁模式

信件自動預覽 關閉 開啟 **關閉預覽視窗**

預設讀信方式 純文字

封鎖外部圖檔 全部封鎖 **避免惡意程式碼**

內文圖片要封鎖
 已讀信件不封鎖
 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 100 封

刪信返回設定 刪信後到 信件列表

自動收取外部信件 登入時 不收取 外部信件

自動清理回收筒 登出時 不刪除 回收筒內的信件

新信通知 5分鐘

確定 取消

GMAIL關閉外部圖檔顯示

設定

[一般設定](#) [標籤](#) [收件匣](#) [帳戶和匯入](#) [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](#) [進階](#) [離線設定](#) [背景主題](#)

電話號碼

預設圖形

頁面大小上限：
每頁顯示 個會話群組

取消傳送：
取消傳送期限： 秒內

預設的回覆模式：
[瞭解詳情](#)

回覆
 回覆所有人

懸停操作：
 啟用懸停操作 - 將滑鼠游標懸停在特定項目上時，快速存取封存、刪除、標示為已讀取和延後的控制項。
 停用懸停操作

傳送並封存：
[瞭解詳情](#)

在回覆中顯示 [傳送並封存] 按鈕
 在回覆中隱藏 [傳送並封存] 按鈕

預設文字樣式：
(使用工具列上的 [移除格式] 按鈕重設預設文字樣式)

Sans Serif

這是您內文文字的外觀。

圖片：
 一律顯示不明外部圖片 - [瞭解詳情](#)
 顯示不明外部圖片時，必須先詢問我 - 這個選項也會停用動態電子郵件。

電子郵件檢查三部曲-1

(一)開啟郵件前，請確認主旨是否與本身業務相關。

郁兆錦	:新任职的经理能力差，我来帮你教
6個符號英文法	馬上上場說寫通用英文 工作需求的朋友 請看進來
六十公里網路科技	[作品欣賞] 購物車網站-藝術生活家居
陳 誼玲	三信銀行優惠貸款方案1.88%起. 三信銀行行員陳誼玲寄09334
法治世界網	【法治世界網】選舉逞口舌一時 民主開放與你到永久 2011-12-
Citytalk城市通 服務中心	【Citytalk本週活動報】熱呼呼-冬天美食三寶 / 溫暖你寒冷的心

非本人主動訂閱、與業務無關或不請自來的，別開!

Ozy1 Taiwan	來自Uni-edit的問候 研究所申請英文編修服務
志強	Publishing Practices Issue 008 NOVA
玉華	Publishing Issue 008 NOVA Editing Practices
Science and Education Foundation, Bulgaria	Conference Invitation
NOVA	【善用JCR思】_January 04_學術寫作秘技NOVA E
NOVAEDITING	NOVA學術週報 Iss29_December_12102012 如
雅芳	NOVA學術週報 立即訂閱享500字免費試編試譯

非教職、學生，怎會有編譯、國外研討會投稿的訊息？
相同類型標題，寄件人換來換去

電子郵件檢查三部曲-2

(二)不明來歷之郵件，請確認信件真實性，勿隨意開啟。

From:alice66<alice66@mail.yens.com.tw>
To:chenmei-@yuntech.edu.tw
Date: Tue, 04 Aug 2020 06:27:49
Subject: 安全通知。 有人可以访问您的文件。



盜用他人信箱發恐嚇勒索信

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。**沒有裝攝影機與麥克風，哪來被觀察？**
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。

沒有聲稱的影片

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物的话，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”）。

無須理會、匯款

我的比特币账户信息（比特币钱包）为：17WK3CtPgRxiXUWjee9K2u93LsutR6J5W4

電子郵件檢查三部曲-3

(三)不任意點閱不明郵件中之超連結、附加檔案。



KT King's Town Bank <info@ktb.com.tw>
Important!

收件者 應該不會用英文標題吧?
我們已將此郵件轉換為純文字格式。

京城銀行 變成 國王的城市!
尊敬的國王的城市銀行客戶，
我們想通知您，您的帳戶已經從一個未經授權的計算機訪問。
請訪問 <https://netbank.ktb.com.tw/MyKTBank/index.jsp>
<<http://mail.pierreberger.com/netbank.ktb.com.tw/index.php>>，並確認您的帳戶的所有者。
**掛羊頭賣狗肉，顯示京城銀行網址，
實際連到 mail.pierreberger.com**
登錄：
<https://netbank.ktb.com.tw/MyKTBank/index.jsp>
<<http://mail.pierreberger.com/netbank.ktb.com.tw/index.php>>

這詞不像本地用法吧!

110教育部電子郵件社交測試信件

此為教育部社交工程郵件演練

您已不慎點擊社交工程郵件所含之連結或開啟附加檔案，此舉隱含高度風險

- 面對可疑電子郵件，秉持3大原則：
 - **不上鉤**：不開啟可疑信件。
 - **不打開**：不隨便打開郵件所夾帶的檔案。
 - **不點擊**：不隨意點擊郵件所夾帶的網址，點選連結前，先移動滑鼠檢查真實來源。

* * 安全便利的資訊環境，需要您我共同來維持 * *

社交工程的預防

- 隨時具備危機意識，對於任何詢問重要資料的人士，都需小心求證
- 單位內對權限應加以分級控管，非屬個人分內事宜，不應掌握帳號、密碼等特殊權限，防止因不了解安全等級而不慎外流重要資料
- 安裝防毒軟體，設定個人防火牆，並定期更新病毒碼
- 針對電腦應用程式應隨時更新修補程式；設定安全密碼（6~8碼，包括英數與符號字元），避免太簡單易遭破解的密碼(優質密碼:12碼以上+英數大小寫+特殊符號)
- 重要資料檔案要加密防護(WORD、Excel)
- 謹慎使用行動裝置

社交工程-謹慎處理電子郵件

- **未經查證前最好不要轉寄予他人**

萬一這些消息是錯誤的，甚至是有心人惡意散布以打擊對手時，轉寄者也許只是出於好心想提醒親朋好友，卻可能因此須負擔法律責任。

- 依照**民法第195條**，此等行為若侵害了他人的名譽或信用，恐怕仍須負起民事損害賠償責任。

- **轉寄類似郵件時宜謹慎!**