



110年臺灣學術網路 防範惡意電子郵件社交工程演練

宣導課程

110/04/01

110/04/08

演練目的

教育部為**提高教育體系各學校人員警覺性**以降低社交工程攻擊風險，特訂定本計畫，舉辦相關資安教育訓練與宣導、規劃辦理演練服務作業，以強化人員資安意識並檢驗機關宣導社交工程防制成效。

演練受測人員--機關正、副首長、各級主管及一般行政人員

- 校長、副校長、各級主管及一般行政人員
- 「具備本校郵件帳號之行政職務相關人員」即須納入受測名單，身分不侷限於正式公務人員。
- 不包含本校學生及沒有兼任行政職的老師。

演練時程

- 依「資通安全事件通報及應變辦法」第8條，每半年辦理一次演練。
- 本（110）年度自 **4月~11月**止，期間**進行2次演練**。

演練方式

- 統一由教育部集中辦理演練。
- 隨機選取受測對象100名
 - ✓ 主管(組長以上)占40%：本年度本校提報62名
 - ✓ 一般行政人員占60%：本年度本校提報**129**名
- 每人每次演練寄送10封郵件。

社交工程郵件型態

- 由教育部資訊及科技教育司以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象。
- 郵件主題分為**政治**、**公務**、**健康養生**、**旅遊**等類型。
- 郵件內容包含連結網址或word附檔。
- 當各單位收件人**開啟郵件**或**點閱郵件所附連結或檔案**時，即留下紀錄。
- 後續統計惡意郵件開啟率及惡意連結(或檔案)點擊率。

評量標準

➤ 惡意郵件開啟率：

- ✓ 開啟惡意郵件之人數 / 機關受測人數
- ✓ 信件**透過預覽或點開方式**開啟，且信件本文內**所含圖片亦完成圖片下載之動作**，始認定為測試成功。
- ✓ 無論在各種郵件系統開信(Outlook、Webmail)或**轉寄至其他信箱**(如:gmail、yahoo、hotmail等)，都會被登錄為測試成功。

➤ 惡意連結點擊或附件下載率

- ✓ 點閱惡意郵件所附連結或開啟附件之人數 / 機關受測人數
- ✓ 受測人員**點選信件內文中之連結網址**或**開啟郵件附件**，將被記錄為測試成功。

演練結果

- 惡意郵件開啟率應低於10%以下
- 惡意連結點擊或附件下載率應低於6%以下
- 由教育部資訊及科技教育司彙整演練報告，陳報行政院資通安全處，並選取成績優良單位及待改善單位。
- 演練成績不良單位，提報後續改善作為，於收到成績後2周內，提交初步改善計畫，並將持續關注下次演練績效改善。

109年「臺灣學術網路防範惡意電子郵件社交工程演練」--本校踩雷郵件清單

➤ 上半年

✓ 公務類_108年公教人員健檢辦法_tanet

✓ 公務類_最新公告民國109年辦公日曆表搶先看_tanet

「開啟信件」12人，開啟率為12.5%，「點選連結」1人，點選率為1%

➤ 下半年

「開啟信件」0人，開啟率為0%，「點選連結」0人，點選率為0%

PS.標註藍色表示該郵件內含之連結及附件有被點選或開啟

109年「臺灣學術網路防範惡意電子郵件社交工程演練」警訊

➤警訊(圖片檔)：出現於

- ✓ 以html格式瀏覽的郵件最上方(以純文字格式瀏覽的郵件不會出現)
- ✓ 點選郵件中超連結網址頁面最上方
- ✓ 開啟郵件附加檔(**WORD**檔案)的內容最上方

您好：

本郵件為教育部電子郵件社交工程演練信件，當您開啟時表示您的警覺性稍有不足。

若駭客使用此信件內容，可能已成功引誘您開啟信件並植入後門程式或病毒。

提醒您應避免開啟與您非信任往來之信件，並注意確認寄件者來源。

教育部資訊及科技教育司 敬上

109年「臺灣學術網路防範惡意電子郵件社交工程演練」郵件主題(上半年)

編號	信件類別	信件標題
Letter 1	公務類	108 年公教人員健檢辦法
Letter 2	公務類	最新公告民國 109 年辦公日曆表搶先看
Letter 3	公務類	【公文】檢送本部第 952 次（擴大）部務會報紀錄 1份，請查照辦理
Letter 4	財經類	IPHONE12 最速優惠
Letter 5	健康類	香 Q 白飯好罪惡？讓熱量大降 6 成的密技，煮飯加一匙就行！
Letter 6	新奇類	從 8 個顏色中挑 3 種顏色 一秒看出「你的現況」
Letter 7	科技類	快下載！一口氣修補 99 個漏洞 Windows 10 有始以來最大更新
Letter 8	旅遊類	走進森林吸取芬多精殺菌趣！精選八大自然系景點
Letter 9	擬真類	展覽VIP 提醒您~食安展【最後 150 張】預約看展摸彩券，請盡速索取!!
Letter 10	情色類	啦啦隊美波女神「濕身走光」影片觀看數爆衝 13 萬

109年「臺灣學術網路防範惡意電子郵件社交工程演練」郵件範本(上半年)

subject: 108年公教人員健檢辦法

attachment: 和孩子像朋友一樣玩耍.doc

您好：

本郵件為臺灣學術網路電子郵件社交工程演練信件，當您開啟時表示您的警覺性稍有不足。

若駭客使用此信件內容，可能已成功引誘您開啟信件並植入後門程式或病毒。

提醒您應避免開啟與您非信任往來之信件，並注意確認寄件者來源。

教育部資訊及科技教育司 敬上

親子遊孩子為何擺臭臉？ 調查：九成小孩想參與規劃行程



109年「臺灣學術網路防範惡意電子郵件社交工程演練」郵件範本(上半年)

from: 徐如輝(bonnysb17192@yahoo.com.tw)

subject: 最新公告民國109年辦公日曆表請先看

attachment: .doc

您好：

本郵件為臺灣學術網路電子郵件社交工程演練信件，當您開啟時表示您的警覺性稍有不足。

若駭客使用此信件內容，可能已成功引誘您開啟信件並植入後門程式或病毒。

提醒您應避免開啟與您非信任往來之信件，並注意確認寄件者來源。

教育部資訊及科技教育司 敬上

Abigail Disney and George Soros say: Tax the wealthy more

More than a dozen of the richest Americans have a message for 2020 presidential candidates: Tax us more.

In a letter sent to candidates Monday, 18 members of some of the nation's wealthiest families advocated for a wealth tax on people who amassed great personal fortunes, including themselves.

"We are writing to call on all candidates for president, whether they are Republicans or Democrats, to support a moderate wealth tax on the fortunes of the richest one-tenth of the richest 1% of Americans -- on us," said the letter, which was first published in the New York Times Monday.



109年「臺灣學術網路防範惡意電子郵件社交工程演練」郵件範本(上半年)

from: Mailall 郵件發送系統(mailallvadfag152@gmail.com)

subject: 【公文】檢送本部第952次(擴大)部務會報紀錄1份，請查照辦理

attachment: 部務會報紀錄.doc

您好：

本郵件為臺灣學術網路電子郵件社交工程演練信件，當您開啟時表示您的警覺性稍有不足。

若駭客使用此信件內容，可能已成功引誘您開啟信件並植入後門程式或病毒。

提醒您應避免開啟與您非信任往來之信件，並注意確認寄件者來源。

教育部資訊及科技教育司 敬上

蘋果提出的隱私問題，只能蘋果自己來解決

「在iPhone裡發生的，就只會留在iPhone上。」(What happens on your iPhone stays on your iPhone.) 今年在拉斯維加斯舉行的國際消費類電子產品展覽會(Consumer Electronics Show, CES)上，這條訊息以華麗的藍色白字印在大樓的一側，有14層樓高。這個位置深得蘋果公司精髓：一個大膽的場景，一個時機正好的語言遊戲，以及對Google、Amazon和所有準備在世界最大舞台上展示其最新產品的競爭對手的蓄意攻擊。但這也是一種誤導，畢竟，蘋果憑藉其強大的App Store，實際上為監控經濟奠定了基礎。

「數千萬人的數據被竊取，而他們卻毫不知情。」



OUTLOOK - 預覽功能關閉方式

預覽功能的關閉方式如下:

(1).使用「Microsoft outlook」收信的使用者，設定方式如下：

開啟「Microsoft outlook」 --> 點選「檢視」 --> 點選「變更檢視」 --> 點選「預覽」，將預覽功能的視窗關閉。



OUTLOOK - 以純文字讀取電子郵件

1. 按一下 [檔案] 索引標籤。
2. 按一下 [選項]。
3. 按一下 [信任中心]，然後按一下 [信任中心設定]。
4. 按一下 [電子郵件安全性]。
5. 在 [以純文字讀取] 底下，選取 [以純文字讀取所有標準郵件] 核取方塊。

以純文字讀取

- 以純文字讀取所有標準郵件(A)
- 以純文字讀取所有數位簽章的郵件(M)

若要併入使用數位簽章簽署的郵件，請選取 [以純文字讀取所有數位簽章的郵件] 核取方塊。

OUTLOOK - 以純文字讀取電子郵件步驟一

收件匣 - Outlook - Outlook

←

資訊

開啟和匯出

另存新檔

儲存附件

列印

Office 帳戶

選項

結束

帳戶資訊

cywang@tnua.edu.tw
POP/SMTP

+ 新增帳戶

 帳戶設定
變更此帳戶的設定或設定更多連線。

 信箱清理
清空刪除的項目和封存，以管理信箱大小。

 規則及通知
使用規則及通知可協助組織您的內送電子郵件，並在項目新增、變更或移除時收到更新。

OUTLOOK - 以純文字讀取電子郵件步驟二



The screenshot shows the Outlook Options dialog box with the Trust Center section selected. The left sidebar lists various categories, and the main area displays security-related information and a link to the Trust Center settings.

Outlook 選項

- 一般
- 郵件
- 行事曆
- 人員
- 工作
- 搜尋
- 語言
- 進階
- 自訂功能區
- 快速存取工具列
- 增益集
- 信任中心

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。

安全性和其他

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。

[Microsoft 高可信度電腦運算](#)

Microsoft Outlook 信任中心

信任中心包含安全性和隱私權設定。這些設定將協助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(I)...

OUTLOOK - 以純文字讀取電子郵件步驟三

信任中心

受信任的發行者
隱私選項
電子郵件安全性
附件處理
自動下載
巨集設定
以程式設計方式存取

加密的電子郵件

- 加密外寄郵件的內容及附件(E)
- 在外寄郵件加入數位簽章(D)
- 當傳送簽章郵件時傳送純文字簽章郵件(T)
- 為所有 S/MIME 簽章郵件索取 S/MIME 回條(R)

預設設定(F): 設定(S)...

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。

以純文字讀取

- 以純文字讀取所有標準郵件(A)
- 以純文字讀取所有數位簽章的郵件(M)

資料夾的指令碼

- 共用資料夾允許指令碼(L)
- 公用資料夾允許指令碼(F)

OUTLOOK -不自動下載圖片

信任中心

受信任的發行者

隱私選項

電子郵件安全性

附件處理

自動下載

巨集設定

以程式設計方式存取

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，可讓寄件者驗證您的電子郵件地址是否有效，因而可能讓您成為垃圾郵件的目標。

- 不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片(D)
 - 允許垃圾郵件篩選中，[安全的寄件者] 清單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)
 - 允許 SharePoint 討論區中的下載(B)
 - 當編輯、轉寄或回覆電子郵件時，在下載內容前先警告我(W)