108 年度下半年臺灣學術網路防範惡意電子郵件
社交工程演練結果報告

中 華 民 國 一 〇 八 年 十 一 月 二 十 八 日

目錄

壹、測試政策

依照「教育部 105-108 年度資訊安全防護作業服務需求說明書」辦理。

貳、實施方法與經過

一、 演練系統架構及實施方式

詳如「108 年度臺灣學術網路防範惡意電子郵件社交工程演練服務計畫」。

二、 測試方式

(一)、針對每位受測人員寄發 10 封測試測試信件進行統計分析作業，統計受引誘而預覽信件、連結點選或開啟附檔之數量及比率。

(二)、若過多教育部機構未點選 10 封測試測試信件，則可能已被郵件伺服器進行關鍵字阻擋，此時增加測試一封圖片郵件進行測試。

(三)、測試作業不會植入後門程式及讀取個人電腦資料，不會影響正常公務執行。

(四)、本項測試作業之測試信件寄件人名稱，均為偽造，用來測試受測人對寄件人名稱是否合理的辨識能力。

三、 時間及範圍

表1　測試範圍

機關	開始日期	結束日期	測試信件數目	總人數	總信件數
教育部機構 A 級單位	2019/10/01	2019/10/31	10	300	3000
教育部機構 B 級單位	2019/10/01	2019/10/31	10	14612	146120
部屬機關(構)	2019/10/01	2019/10/31	10	1313	13130
縣市教育網路中心	2019/10/01	2019/10/31	10	283	2830

四、信件內容

本次測試信件共分成十封主題內容不同的信件。

表2　測試信件摘要表

編號	信件類別	信件標題
Letter 1	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 2	擬真類	108 年下半年資訊安全教育訓練,請尚未參訓之同仁盡速報名
Letter 3	公務類	公文 e 系統維護公告，具時效之公文請提前處理
Letter 4	公務類	最新公告民國 109 年辦公日曆表搶先看
Letter 5	擬真類	轉知：「2019 資通訊網路安全實務強化研討會」意見回饋抽獎活動
Letter 6	公務類	108 年公教人員健檢辦法
Letter 7	生活類	洗牙通知
Letter 8	擬真類	電信費用入賬通知
Letter 9	學術類	民國 108 年環境教育與交流活動
Letter 10	公務類	檢送 108 年度第 6 次處務會議紀錄乙份，請依會議裁示事項辦理

圖 1：測試信件內容

from: 華中電信(hcctebill62fy23@msa.hinet.net)

subject: 電信費用入賬通知

attachment: 被撤回投資陸企名單.doc

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

貿戰延燒！美議員籲政府退休基金、撤回投資陸企決定

Photo credit:Visualhunt

中美貿易戰戰火蔓延至金融市場，美國參議員要求大型政府退休基金推翻先前決定，不要投資部份陸企，以免傷害美國國家安全。

---

from: 萬芳牙科部(wanfangdentist@outlook.com)

subject: 洗牙通知

attachment: 北中南高鐵站美食攻略.doc

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

高鐵乘客少的站該廢除？　行家曝「母湯設計」：想搭也難

日前有一名網友於 PTT 八卦版上發文，表示自己剛好正在某個南部的高鐵站，但站內的乘客數量真的相當稀少，這讓他相當疑惑，高鐵每年乘客數量那麼多，怎麼還會有這樣的現象呢？認為是不是應該要廢掉這些較少人搭的高鐵站呢？

---

from: 全國人事服務處(Healthcheck71r541@gmail.com)

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

親子遊孩子為何擺臭臉？　調查：九成小孩想參與規劃行程

---

from: Una from好康彩頭(acgoodkangcaltou_una@yahoo.com.tw)

subject: 轉知：「2019資通訊網路安全實務強化研討會」意見回饋抽獎活動

attachment: 歷年空服員薪資大拚比.doc

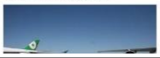
您好：
本郵件為教育部電子郵件社交工程演練信件，當您開啟時表示您的警覺性稍有不足。
若駭客使用此信件內容，可能已成功引誘您開啟信件並植入後門程式或病毒。
提醒您應避免開啟與您非信任往來之信件，並注意確認寄件者來源。

教育部資訊及科技教育司　敬上

航空罷工誰賠旅客？品保協會喊旅行社無違約責任 籲修法

中華民國旅行業品質保障協會表示，長榮航空空服員發動罷工，造成旅客行程受阻，被迫取消或變更行程，甚至留滯國外衍生額外費用。

有消保團體主張旅行社應旅客負違約金的賠償，但這不是旅行社的過失，也絕無違約責任，建議主管機關在相關法規及旅遊契約中，明定罷工事件所產生問題的責任歸屬。



---

from: 徐如婷(bonnysb17192@yahoo.com.tw)

subject: 最新公告民國109年辦公日曆表搶先看

attachment: 最新公告民國109年辦公日曆表搶先看.doc

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

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.

---

from: 公文系統管理組(edittitung@hotmail.com)

subject: 公文e系統維護公告，具時效之公文請提前處理

attachment: 修補程式.doc

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

微軟被黑客攻擊，致部份Outlook.com郵件用戶帳號資訊外泄！

有駭客取得微軟支援人員帳密，導致outlook.com部分用戶Email帳號資訊曝光長達3個月微軟上周以電子郵件通知Outlook.com用戶。

微軟客服人員遭駭客入侵，導致年初「數量有限」的網頁郵件用戶的電子郵件及主旨等內容曝光長達3個月，可能導致用戶遭網釣或垃圾郵件攻擊。

---

from: 資安會談(securytrainiing461@outlook.com)

subject: 108年下半年資訊安全教育訓練，請尚未參訓之同仁盡速報名

attachment: 來測測你可以答對幾題.doc

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

網友熱議！「123456789 x 72」國小數學考倒成年人

這題國小數學居然考倒成年人！一名女網友分享兩題國小數學題目，原本對國小程度的題目自信滿滿，沒想到看完後，讓不少人直呼「可以拿計算機嗎？」貼文一PO出後，立刻引來熱心網友幫忙解題。

---

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

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，這條訊息以簡單的黑底白字印刷在大樓的一側，有14層樓高，這個宣言深得蘋果公司精髓：一個大膽的場面，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，事實，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。」

參、名詞定義

一、 測試成功定義

（一）開啟信件：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。以教育部員工使用郵件系統，其預設之安全設定不會自動下載圖片，即使預覽功能設定為開啟，或是直接打開測試信件，因無下載圖片之動作，不會造成安全漏洞，將不會記錄為測試成功。

（二）點選連結：受測人員點選信件內文中之連結網址，將被記錄為測試成功。

（三）開啟附檔：受測人員開啟信件內文中之附檔，將被記錄為測試成功。

二、 測試統計方式說明

（一）測試成功人數

以駭客的角度而言，發送眾多測試信件，只要有一封測試成功，即達到目的。因此本次演練參演人員只要曾經開啟或預覽過測試信件中之任一封，即視為測試成功。

演練統計資料以受測信箱數量計算，同一受測信箱即使曾開啟/預覽多封不同內容之測試信件，但在統計資料中會紀錄為 1 人。

連結點選的測試成功人數計算方式與開啟/預覽信件測試成功人數計算方式相同。

（二）測試成功率

以單位演練參演人員受測信箱總數為分母，測試成功人數為分子，計算所得之百分比，即為受測單位本測試的整體測試成功率。將分別統計「信件開啟率」、「連結點選率」及「信件開啟或連結點選率」。

肆、測試結果

各單位之惡意郵件開啟率應低於 10%以下；惡意連結(或檔案)點擊率應低於 6%以下。

部分單位點選連結人數高於開啟信件人數，原因是使用者在純文字模式下開啟信件將不會觸發信件連結，同樣可達到防止惡意信件的目的，但卻又自行將信件內文中的連結網址複製到瀏覽器中開啟。演練結果如下：

全部測試結果統計

108 年度教育機構社交工程演練成果							
單位名稱	總人數	開啟信件(人數)	開啟信件(%)	點選連結(人數)	點選連結(%)	開啟或點選(人數)	開啟或點選(%)
A 級(附設醫院)	300	0	0.00%	0	0.00%	0	0.00%
B 級(大學院校)	14612	52	0.36%	1	0.01%	52	0.36%
部屬機關(構)	1313	0	0.00%	0	0.00%	0	0.00%
縣市教育網路中心	283	0	0.00%	0	0.00%	0	0.00%

伍、統計報表

參演單位測試結果請洽教育部資訊及科技教育司李紀緯先生。電話：（02）7712-9090；Email：moe_infosec@mail.moe.gov.tw。

陸、成績說明

未達標準單位：

演練結果「開啟信件」比率大於 10%或「點選連結」比率大於 6%之單位，請擬定改善計畫並針對開啟信件或點選連結人員加強訓練宣導。

（1）A 級單位

無未達標準單位

（2）B 級單位

代號	參演人數	開啟信件(人數)	開啟信件(%)	點選連結(人數)	點選連結(%)	開啟或點選(人數)	開啟或點選(%)
5	100	46	46.00%	0	0.00%	46	46.00%

（3）部屬機關(構)

無未達標準單位

（4）縣(市)教育網路中心

無未達標準單位