gamania
CloudForce
雲力橘子

新竹縣教育研究發展暨網路中心電子郵件社交工程演練統計報告

2026 年 01 月 13 日

gamania CloudForce

目錄

1. 測試概述 4
1-1. 測試目的 4
1-2. 名詞定義 5
1-3. 測試範圍 6
1-4. 測試說明 6
1-5. 信件範本 7
2. 演練結果說明 8
2-1. 各信件誘騙成功統計表 8
2-2. 各信件各單位誘騙成功人數統計表 9
2-3. 各單位誘騙成功人數統計表 9
3. 改善措施建議與方法 16

Confidential

表目錄

表 1　測試範圍 6

表 2　信件範本 7

表 3　各信件誘騙成功統計表 8

表 4　各單位誘騙成功人數統計表 9

Confidential

1.測試概述

1-1. 測試目的

釣魚郵件屢禁不絕，無疑是當今企業或網路使用者面臨的最大安全威脅之一，駭客們不再隨機發送數以千計的垃圾郵件希望能引誘人點擊，而是有針對性地發送特別製作的釣魚郵件。雖然這些郵件需要駭客花費更多的時間和精力來製作，但回報絕對是值得的。駭客們現在都已了解到，人們能一眼區分出垃圾郵件和有用的郵件，但要識別釣魚郵件則困難許多。現今的世界生活節奏很快，人們被四面八方的資訊包圍著，注意週期越來越短，點選連結習以為常。打開一封郵件，你只有幾秒鐘的時間判斷它是否重要或有意義，如果有用，你會點選連結閱讀彈出的網頁，然後檢查下一個資訊。這幾乎成了一種下意識的反應。釣魚郵件設計就是觸發你的這種自動點擊反應。但是您這個自動點擊的反應，可能對您的自身或甚至您所在的公司，造成不可估計的損失。

現階段的資安防護除了仰賴各種資安設備及產品的偵測防禦功能外，使用者具備良好的使用習慣或足夠的資安意識，也將扮演非常重要角色。本次測試即模擬駭客攻擊手法，寄送各種誘騙信件給同仁點選。透過各類型誘騙信件讓同仁體驗實際的攻擊情景，並依受誆騙統計狀況來瞭解同仁資安意識的落實狀況與企業對社交工程、網路釣魚等行為的防護能力。

Confidential

1-2. 名詞定義

- 開啟信件

  必須完成兩項行為始認定為誘騙成功：1.透過預覽或直接點選的方式開啟信件 2.郵件內的圖片成功顯示出來。若是**已點開信件但圖片並未顯示出來**則不計入誘騙成功的統計資料內。

- 點擊連結

  受測人員**有點選信件內文中之超連結**即被記錄為誘騙成功。

- 點擊附件

  受測人員**有開啟信件所包含之附件檔案**即被記錄為誘騙成功

- 開啟釣魚網站輸入資料

  受測人員**開啟釣魚網站後輸入資料**即被記錄為誘騙成功。

- 誘騙成功人數

  以駭客角度來看，眾多信件中只要有 1 封誘騙成功，即達成目的。因此在每位受測者收到的 3 封信件中，只要有 1 封信件有開啟郵件、點選連結、點擊附件及開啟釣魚網站輸入資料 4 個行為之中任一行為，即核算該位受測者被誘騙成功，統計人數為 1 人。

Confidential

- **誘騙成功率**

  以本次受測單位提供之全體受測人員 E-mail 總數為分母，前項敘述定義之誘騙成功人數為分子，計算出百分比即為此次社交工程演練之誘騙成功率。

1-3. 測試範圍

表 1　測試範圍

開始統計日期	結束統計日期	每人測試信件數	總人數	總信件數
2025/12/09	2025/12/18	3	1484	4452

1-4. 測試說明

1. 測試作業不會植入任何惡意後門程式，也不會帶走受測者電腦內任何資料，不會影響日常公務執行。
2. 測試作業寄發信件使用的寄件人名稱及寄件人 E-mail 皆為**偽造**，用來檢驗受測人員對釣魚信件是否有足夠的判斷及辨識能力。
3. 測試作業於 2025-12-9、2025-12-10、2025-12-12 各寄發一封信件，最終所有受測者都會收到相同的 3 封信件。

Confidential

1-5. 信件範本

本次測試所使用的信件範本如下表所示：

表 2　信件範本

編號	郵件標題	寄件者名稱/E-mail	寄件時間
1	您的貨到付款訂單#250704Q1VP6JN7 已被確認	info@dgcsec.online	2025-12-09
2	【點數到期提醒】您有點數 304 點將於 2025/12/31 到期，多元兌點服務盡享美好。	高鐵會員 TGO < TGO@dgcsec.live>	2025-12-10
3	【11/14 盛大開展】台北國際酒展盛大登場！邀您品飲世界美酒！	展詔電子信 <chanchao@dgcsec.online>	2025-12-12

Confidential

2.演練結果說明

2-1. 各信件誘騙成功統計表

本次演練測試中，發現有 125 位員工資安意識不足，且有 68 人填寫連結導向的表單。

表 3　各信件誘騙成功統計表

編號	郵件標題	寄件者名稱/E-mail	演練類型	誘騙成功數	誘騙成功率
1	您的貨到付款訂單 #250704Q1VP6JN7 已被確認	info@dgcsec.online	圖片	2	0.13%
			連結	9	0.61%
			附件	1	0.07%
			輸入資料	2	0.13%
2	【點數到期提醒】您有點數 304 點將於 2025/12/31 到期，多元兌點服務盡享美好。	高鐵會員 TGO < TGO@dgcsec.live>	圖片	15	1.01%
			連結	107	7.21%
			附件	3	0.20%
			輸入資料	66	4.45%
3	【11/14 盛大開展】台北國際酒展盛大登場！邀您品飲世界美酒！	展詔電子信 <chanchao@dgcsec.online>	圖片	0	0.00%
			連結	4	0.27%
			附件	0	0.00%
			輸入資料	0	0.00%

Confidential

2-2. 各信件各單位誘騙成功人數統計表

本次測試共對 1484 個信箱寄送 4452 封測試信件，每封信件皆包含 4 種誘騙手法(開啟信件、點擊連結、點擊附件及釣魚網站)，總誘騙機會為 17808 個機會，總共被誘騙成功機會次數為 209 次，其中開啟信件 17 次，點擊連結 120 次，點擊附件 4 次，開啟釣魚網站輸入資料 68 次。

詳請參考附件：新竹縣教育研究發展暨網路中心電子郵件社交工程演練統計資料.xlsx

2-3. 各單位誘騙成功人數統計表

以駭客角度而言，不論每封信件有幾個誘騙機會，只要成功一個即算任務達成；本次演練每位員工收到 3 封信件，每封信有 4 個誘騙機會(圖片、連結、附件及釣魚網站)，共有 12 個誘騙機會，只要其中任 1 個誘騙成功即算任務達成，該位員工將可能被駭客入侵。因此只要有出現在原始統計資料內的員工皆會列入被誘騙成功之人數，同一位員工在 12 個誘騙機會裡只要成功 1 個以上，不論成功多少個，皆以 1 人計算。

表 4　各單位誘騙成功人數統計表

代碼	人數	誘騙成功人數	占部門比
m06	18	1	5.56%
p81	18	1	5.56%
m22	7	2	28.57%
p83	19	4	21.05%

Confidential

p06	8	0	0.00%
p45	20	0	0.00%
p60	8	2	25.00%
m08	20	1	5.00%
p43	20	0	0.00%
p39	21	0	0.00%
h09	16	0	0.00%
p18	6	0	0.00%
m29	18	4	22.22%
m15	19	0	0.00%
p58	6	0	0.00%
n00	32	1	3.13%
m31	24	2	8.33%
m02	25	6	24.00%
m30	23	3	13.04%
p05	16	0	0.00%
p71	8	0	0.00%
m33	21	5	23.81%
p20	9	0	0.00%
m26	8	0	0.00%
p31	6	0	0.00%

Confidential

m25	12	0	0.00%
p50	10	1	10.00%
p78	24	3	12.50%
p37	24	0	0.00%
p10	21	3	14.29%
p48	6	1	16.67%
p52	15	1	6.67%
m27	15	0	0.00%
p00	19	1	5.26%
p79	19	3	15.79%
p57	10	2	20.00%
p46	6	0	0.00%
h05	17	12	70.59%
p38	6	1	16.67%
p41	21	1	4.76%
m05	21	2	9.52%
p42	8	0	0.00%
p59	12	0	0.00%
m10	6	1	16.67%
p35	6	0	0.00%
m24	10	0	0.00%

Confidential

p84	19	0	0.00%
p04	19	1	5.26%
m14	20	0	0.00%
m04	23	4	17.39%
m34	16	2	12.50%
m20	16	1	6.25%
m11	19	5	26.32%
p12	25	1	4.00%
p03	21	0	0.00%
p14	19	5	26.32%
p17	8	0	0.00%
p19	20	0	0.00%
p30	5	0	0.00%
m16	16	0	0.00%
p54	16	3	18.75%
p86	6	0	0.00%
m09	15	2	13.33%
p01	23	1	4.35%
p16	20	5	25.00%
p77	10	0	0.00%
p72	6	0	0.00%

Confidential

p67	8	0	0.00%
m19	21	2	9.52%
p56	6	0	0.00%
m07	12	0	0.00%
p80	20	2	10.00%
p65	6	2	33.33%
p08	5	0	0.00%
p09	7	0	0.00%
p02	23	1	4.35%
p33	5	1	20.00%
p70	7	0	0.00%
p40	14	0	0.00%
p24	10	1	10.00%
p62	9	0	0.00%
p47	9	0	0.00%
p82	23	0	0.00%
p69	7	0	0.00%
p26	6	1	16.67%
p51	7	0	0.00%
p36	6	0	0.00%
p27	13	0	0.00%

Confidential

p55	5	0	0.00%
p07	5	2	40.00%
p21	6	0	0.00%
m13	15	0	0.00%
p74	5	0	0.00%
p22	6	0	0.00%
m12	6	2	33.33%
p61	7	1	14.29%
p85	6	0	0.00%
m17	8	1	12.50%
m18	8	0	0.00%
m28	8	1	12.50%
p28	16	2	12.50%
p23	7	0	0.00%
p11	11	3	27.27%
p34	6	1	16.67%
k01	2	0	0.00%
p64	6	0	0.00%
p63	6	1	16.67%
p32	6	1	16.67%
p73	7	0	0.00%

Confidential

p25	5	0	0.00%
m23	8	2	25.00%
p66	7	0	0.00%
m03	13	1	7.69%
p68	7	0	0.00%
p15	6	0	0.00%
p44	7	1	14.29%
p76	6	1	16.67%
p13	5	0	0.00%
p49	5	1	20.00%
p29	5	0	0.00%
p75	8	0	0.00%
總計	1484	125	8.42%

Confidential

3.改善措施建議與方法

本次演練遭誘騙人數比例約為整體之 8.42%。為了有效避免社交工程所導致的相關資安事件發生，建議於貴公司於各單位宣導防騙停看聽的資安概念，針對開啟信件行為之改善建議可針對信件自動下載圖片功能、及取消信件預覽功能做宣導。針對附加檔案開啟之行為，須請同仁特別注意檔案之格式是否與實際圖示相符，因為只要有一位同仁開啟信件附加檔案，就可造成公司內部網路架構遭駭。

停	確實更新防毒軟體病毒碼 關閉信件自動下載圖片及其他內容 以純文字模式開啟信件 取消信件預覽功能
看	信件是否來自與貴公司有往來之單位 標題或內容是否與本身業務相關 其餘信件應視為垃圾郵件
聽	透過電話或其他聯絡方式確認信件真偽

Confidential

另一方面，建議貴公司在同仁防範社交工程宣導或教育訓練過程中，持續增強同仁使用電子郵件應有的以下警覺性觀念：

1.我為何會收到這封郵件? 寄件者是誰？我認識他嗎？須注意『寄件者名稱』和『寄件者地址』也是可以假造的。

2.我是不是應該收到這封郵件? 這封信是不是跟我有關聯? 內容是否合理?有沒有威脅利誘的字眼?有沒有詐騙的可能?

3.我是不是有必要開啟附件或點選連結?

社交工程是一種利用人性弱點的詐騙技術，它避開了企業內嚴密的資通安全技術防護，是一種非常難以防範的攻擊模式，只有倚靠貴公司同仁具備高度的危機意識及警覺心，才能減少社交工程攻擊的傷害。

Confidential