達和環保服務股份有限公司

社交工程演練測試服務

報告書

建議單位

SYSTEX | uniXecure

2023 年 02 月

資訊等級 ☐機密　☐密　☐普通　☐內部使用
閱讀對象 ☐一般主管　☐一般員工　☐資安人員　☐資訊人員

保密條款

本文件標示為「機密文件」，內容包含貴單位內部網路架構、系統配置、應用系統現況與本公司業務營運技術等之機密資訊。本公司依規定，視同為機密文件並採取必要之保密措施維持其機密性，雙方並同意，不得洩漏、告知、交付、移轉或以任何方式提供第三人或自行以非合約目的方式，加以使用或利用。

目 錄

1. 電子郵件 資安意識人因社交工程演練分析報告

1.1. 演練基本資料

1.1.1. 專案緣由

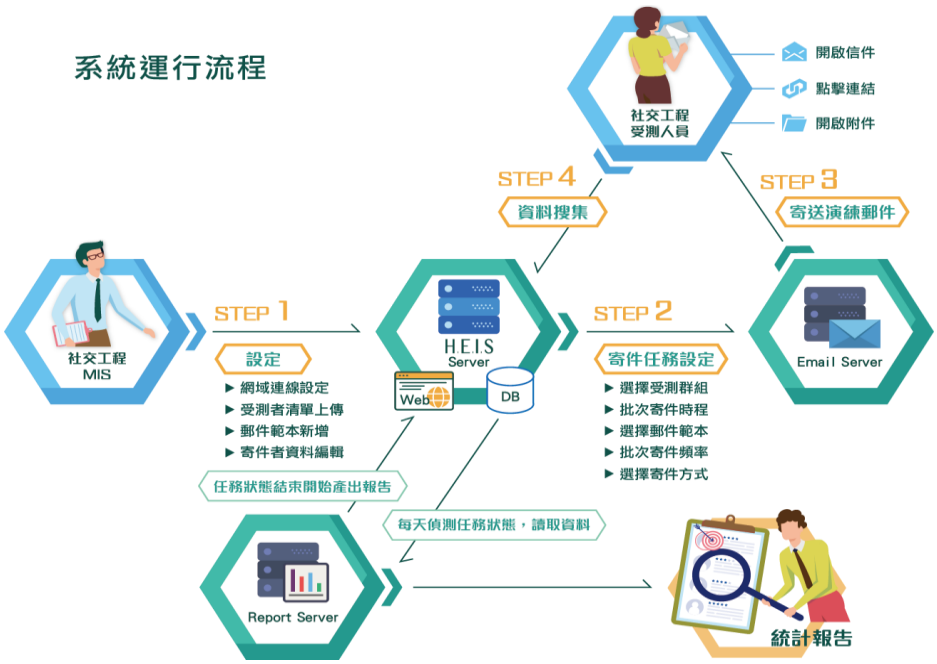
透過「 資安意識人因社交工程郵件測試服務」之執行成果，使受測單位瞭解 資安意識人因社交工程的存在，並提高警覺;同時受測單位可以根據測試結果瞭解可能發生的安全缺口，藉以實施其內部教育訓練來補強，並作為資訊安全的管理依據。

1.1.2. 採用技術

本次社交演練任務採用[UNIXECURE-資安意識人因分析系統 HEIS]來模擬駭客思維設計釣魚郵件，透過本 資安意識人因社交工程演練以提升員工資安意識與資安警覺性，防止員工一個輕忽的行為而引發重大的資安危機，造成無法彌補的後果。HEIS 透過直覺化導引式介面，使得 IT 人員能夠更快速的依照系統介面指示設定任務排程、設計郵件範本、並產出演練報告，此外，HEIS 還能藉由互動式動態數據模板提供即時專案進度及警示訊息，使單位主管在有限的時間內，即時掌握單位員工的資安意識狀態以及風險分佈，並培育單位員工在各種駭客攻擊中更具警覺性與資安意識，進而有效降低單位資安風險。

1.1.3. 演練流程說明

圖表 HEIS 演練流程圖



1.1.4. 執行任務總覽

本次演練任務採 2 封釣魚郵件於 2023/02/15 ~ 2023/02/22 執行投放，詳細演練主旨與類別請參閱以下圖表：

圖表 演練任務基礎資訊表

主旨	期間	類別
人工智慧參賽還幫你寫論文？AI 可以取代人類工作嗎？	2023/02/15 ~ 2023/02/22	科技
會議主持人正等待您加入會議!	2023/02/15 ~ 2023/02/22	生活

1.1.5. 資料搜集期間

- 2023/02/15 ~ 2023/02/22

1.1.6. 執行項目

- HEIS 社交工程演練測試服務

1.1.7. 演練帳號數

受測單位提供的受測者郵件帳號，共計 255 筆
總發信量：合計 510 封

1.1.8. 演練範本

演練期間每位受測帳號都會收到 2 封信件，樣本數共計 2 種，測試項目詳見圖表所示：

圖表 演練信件主旨

項目	郵件類別	信件主旨	測試項目	測試人數
1	科技	人工智慧參賽還幫你寫論文？AI 可以取代人類工作嗎？	開啟信件 連結觸發	255
2	生活	會議主持人正等待您加入會議!	開啟信件 連結觸發	255

1.1.9. 測試方式

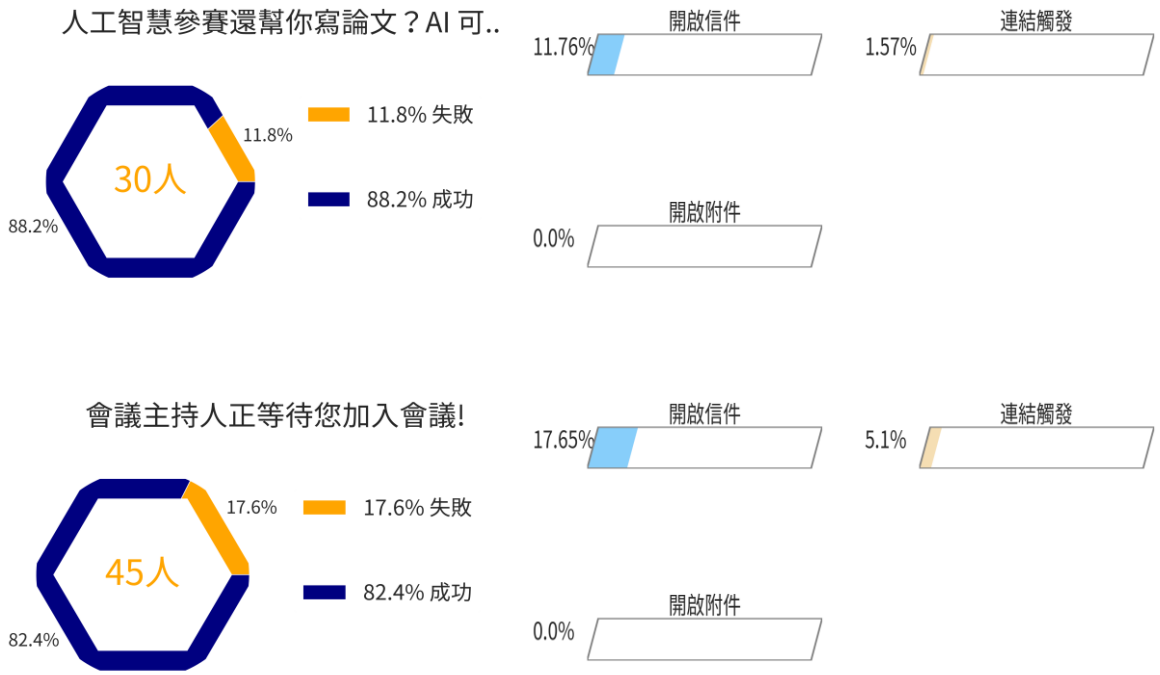
本次演練任務提供範圍內電子郵件帳號的測試服務，各帳號進行 2 封 HEIS 社交工程演練郵件測試，2 封固定寄送，共計 510 封 HEIS 社交工程演練測試郵件。內容除以

HTML 格式呈現外，若帶有附檔須為 Office(如 Word)、RAR 等檔案格式，並以打開附檔或點選連結當作被入侵成功之統計。

2. 演練結果統計

本次演練任務總帳號數有 255 個，總演練郵件數為 510 筆，開啟信件總數有 54 個帳號，開啟信件比率為 21.18 %；連結觸發總數有 17 個帳號，連結觸發比率為 6.67 %；本次演練沒有進行開啟附件測試，每個類型郵件演練數據詳見圖表。

圖表 演練任務結果統計圖



2.1. 依部門統計

2.1.1. 依部門觸發行為統計

針對部門測試結果統計，發現開啟信件最多次的部門是「總公司」，開啟信件比率最高的部門是「永康廠」;連結觸發最多次的部門是「總公司」，連結觸發比率最高的部門是「上水 北辦」;本次演練沒有進行開啟附件項目測試;

本次演練任務信件開啟比率愈高，代表受測人員對電子郵件 對於社交工程防護的認知不足，針對點閱演練信件的人員應透過資安意識培訓程以提升人員的安全認知。

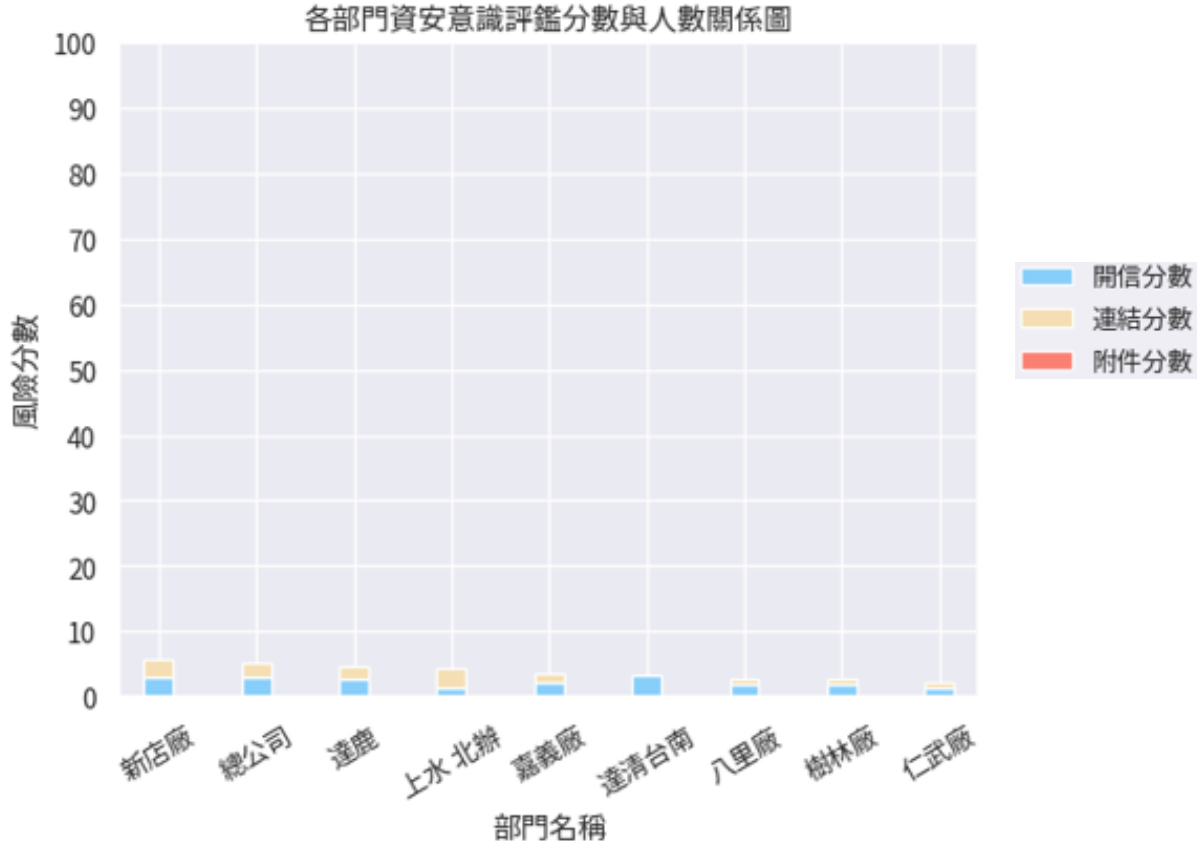
※此計算為統計測試項目的帳號數，已排除重覆資料

※若需詳細部門觸發行為資料請至**受測人員觸發行為統計表.xlsx** 查閱

2.1.2. 依部門演練範圍統計

根據 HEIS 社交工程演練部門範圍長條圖，單位總人數與(點擊信件 10%、點擊連結 20%、開啟附件 40%)計算其對應「資安意識評鑑分數」並取得個別單位之長條圖，此統計僅針對資安意識評鑑分數「前十高分」部門進行呈現，長條圖越長者代表社交工程防護與資安意識最差，該單位需要進一步提出改善計畫。

圖表 各部門資安意識評鑑分數與人數關係

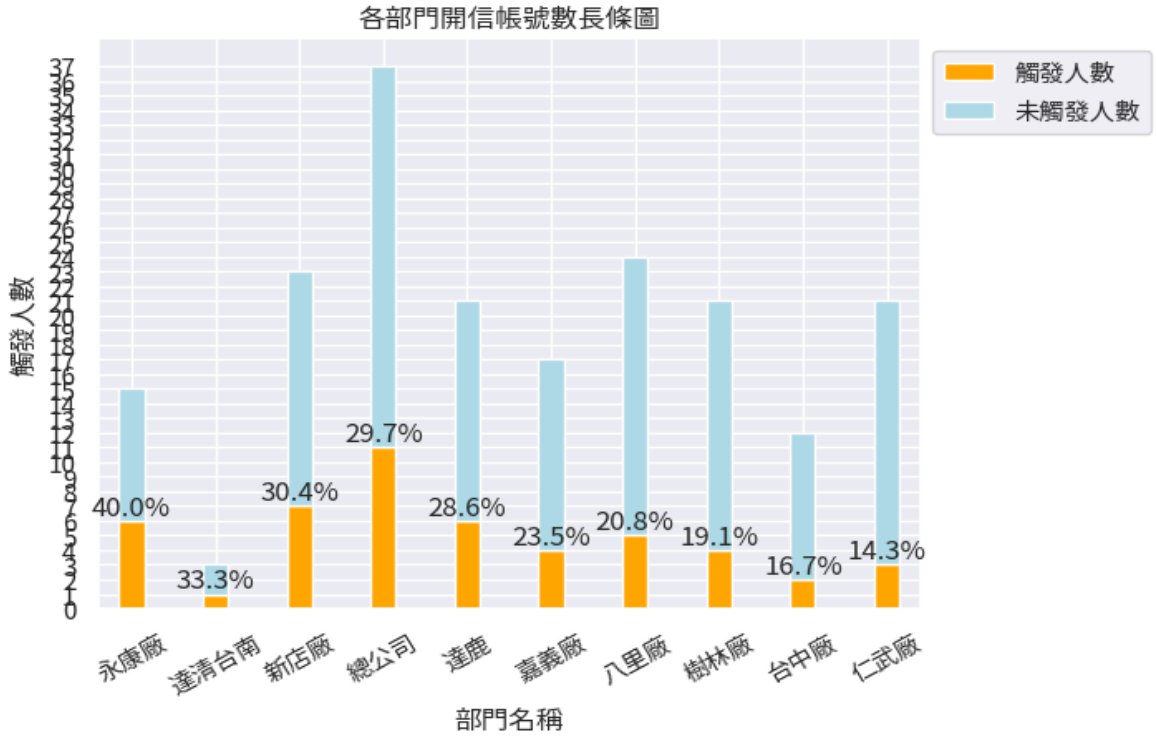


2.2. 依受測行為統計

2.2.1. 各部門開起信件比率

本次演練任務總開信帳號數為 54 個，各部門開信帳號數之資訊，呈現如下方圖表。
根據本次演練任務數據之統計分析，取得「開起信件比率」**前十大**的部門。「開信帳號數」之定義以帳號數計算，亦即單一帳號開信超過一次，以一次計算。透過圖表，本次演練任務可以得知以 HEIS 開信帳號數最多之部門，建議針對此部門持續強化資安意識培訓。

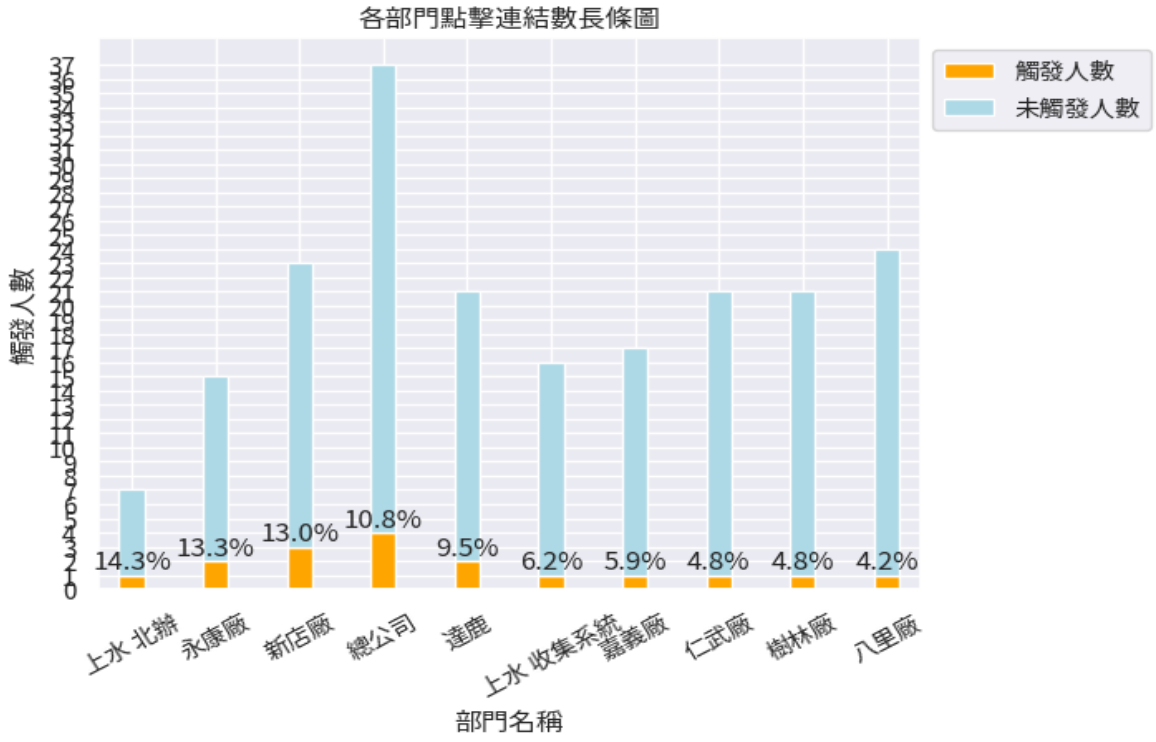
圖表 各部門開信帳號數長條圖



2.2.2. 各部門連結觸發比率

本次演練任務總點擊連結帳號數為 17 個，各部門點擊連結數之資訊，呈現如下方圖表。
根據本次演練任務數據之統計分析，取得「連結觸發比率」**前十大**的部門。「點擊連結數」之定義以帳號數計算，亦即單一帳號點擊連結超過一次，以一次計算。透過圖表，本次演練任務可得知以 HEIS 點擊連結數最多之部門，建議針對此部門持續強化資安意識培訓。

圖表 各部門點擊連結數長條圖



2.2.3. 各部門開啟附件比率

本次演練沒有進行開啟附件測試或開啟附件數為零

2.3. 依個人統計

本次演練任務統計受測者之行為，包括開信、點擊連結、開啟附件，並依照員工各行為之次數進行排序，取得最具社交工程風險之前十名受測者。建議企業與組織針對此些具高度風險之受測者進行後續資安意識培訓，以避免成為駭客攻擊口。詳見圖表所示。

※備註 1：開信次數、點擊連結次數、開啟附件次數皆為該受測者於演練期間觸發該行為次數加總

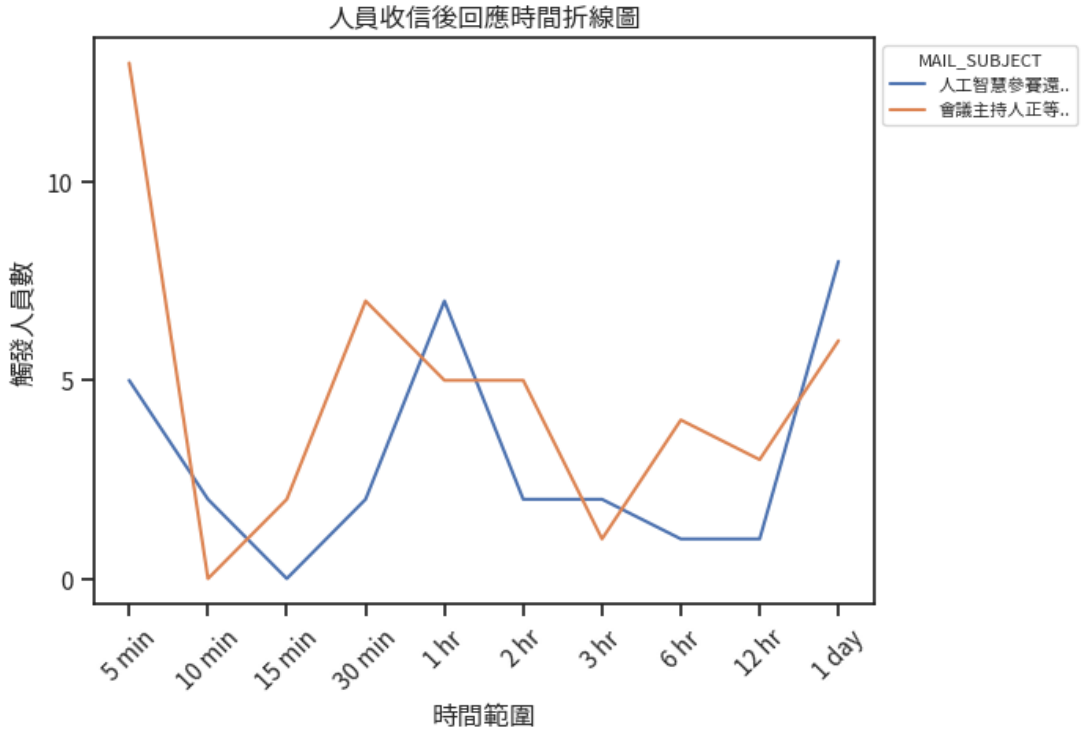
圖表 受測人員觸發行為統計表

姓名	電子郵件	部門	開信次數	點擊連結次數	開啟附件次數
洪博彥	quinn.hung@tahoho.com.tw	新店廠	10	2	0
謝伊庭	yiting.hsieh@tahoho.com.tw	新店廠	11	0	0
張哲訓	chehsun.chang@tahoho.com.tw	樹林廠	7	0	0
楊芳哲	david.yang@tahoho.com.tw	永康廠	4	1	0
林冠君	janie.lin@tahoho.com.tw	達鹿	3	1	0
陳丁全	chendingchuan@tahoho.com.tw	八里廠	3	1	0
黃信行	hsinhsing.hwang@tahoho.com.tw	新店廠	4	0	0
林家妤	amy.lin@tahoho.com.tw	達鹿	4	0	0
陳君華	coleman.chen@tahoho.com.tw	永康廠	2	2	0
林言滄	yiengtsang.lin@tahoho.com.tw	永康廠	3	0	0

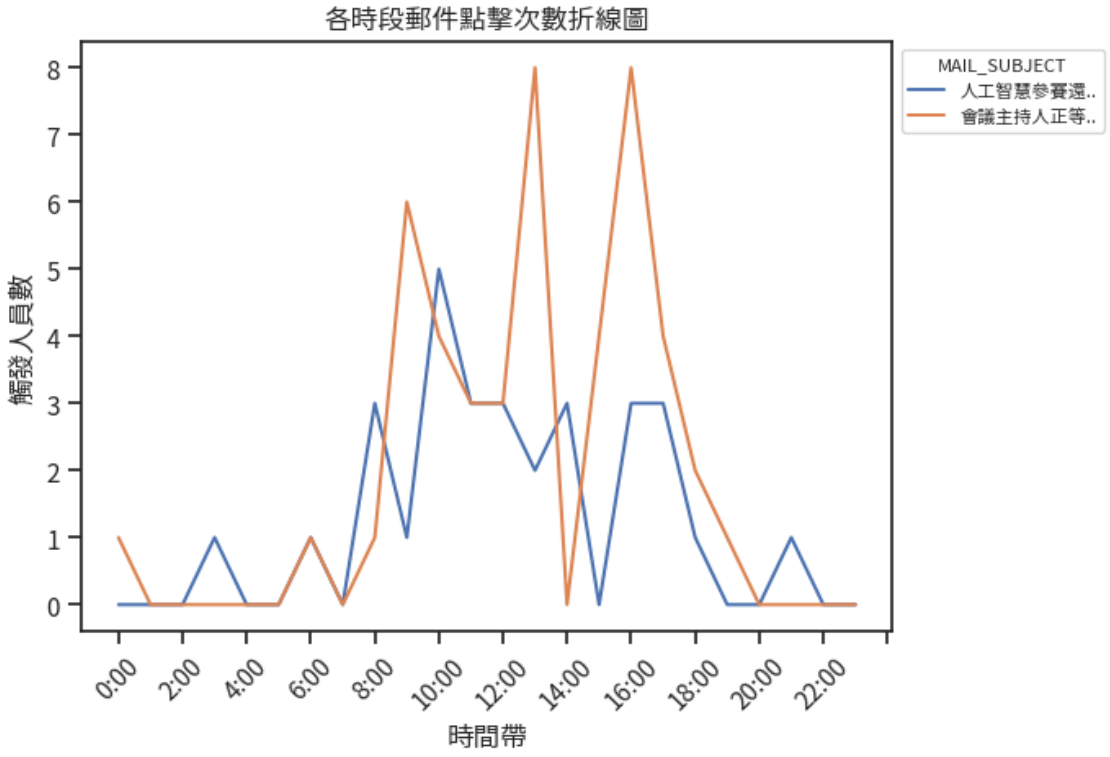
2.4. 依照用戶行為時間統計

本次演練任務統計受測者平均反應時間，亦即受測者收到演練信件後，相隔多少時間才會將信件打開，比例最高的反應時間詳見圖表所示。

圖表 人員收信後回應時間折線圖



圖表 各時段郵件點擊次數折線圖



3. 結論

3.1. 資安意識人因社交工程演練測試服務結論

3.1.1. 資安意識人因社交工程演練之執行結果

針對演練信件統計，發現員工對「會議主持人正等待您加入會議!」信件較感興趣，詳見圖表所示：

圖表 依信件主旨觸發行為統計表

信件主旨	演練帳號數	開啟信件		點擊連結		開啟附件	
		帳號數	比率	帳號數	比率	帳號數	比率
人工智慧參賽還幫你寫論文？AI 可以取代人類工作嗎？	255	30	11.76%	4	1.57%	0	0.0%
會議主持人正等待您加入會議!	255	45	17.65%	13	5.1%	0	0.0%

※此計算為統計測試項目的帳號數，已排除重覆資料

大部份受測者對社交郵件已有所警覺，少部份受測者易受郵件內容吸引而有開啟或點擊連結之行為。單位需了解網路釣魚，駭客會使用的釣魚手法與攻擊方式，進一步嘗試觀察信件的一些可疑指標。

3.1.2. 資安意識人因社交工程演練之統計分析

本次演練任務時間為 2023/02/15 ~ 2023/02/22，共計 8 天。

根據演練結果所示，資安意識人因社交工程郵件演練開信率為 21.18%

最高的部門為永康廠單位，該單位總人數為 15 人，開啟信件的人數則為 6 人，佔了該部門的 40.0%。該部門本次演練的部門人數排名中算是單位內第 10.0 大的單位，觸發人數單位占比較高為中段班，未來若中駭客攻擊，需注意橫向感染的可能性。

由於該部門平均點擊信件的時間大多落在 8 點前後，可間接反應工作效率最高時間為下午時段，且平均回應信件的時間為 11 小時 47 分，本次演練的信件樣本感興趣程度普通。

由於現今的電子郵件系統，都有具備點擊預覽以及手機預開信等功能，因此開信率的正確性僅視為企業在考察資安意識人因社交工程演練總體成果的參考指標。由於現今的電子郵件系統，都有具備點擊預覽以及手機預開信等功能，因此開信率的高低僅能代表受測人員對於該郵件類型的興趣程度，單位需進一步觀察其郵件連結點擊率以及附件開啟率來進行多方研判。

資安意識人因社交工程郵件演練連結開啟率為 6.67%

根據排名最高的部門為上水 北辦單位，該單位總人數為 7 人，開啟郵件連結的人數則為 1 人，佔了該部門的 14.29%，而該部門本次演練的部門人數排名中算是單位內第 14.0 大的關鍵單位，觸發人數單位占比較低，管理者需注重該部門與其他部門的業務連結性，避免惡意攻擊跨部門影響。

由於該部門平均點擊連結的時間大多落在 10 點前後，可間接反應工作效率最高時間為下午時段，且平均回應信件的時間為 1 小時 28 分，本次演練的信件樣本感興趣程度偏高。

對於有點擊不明連結的人員，需視情況強化資安意識宣導，電子郵件為許多企業對外進行業務的主流管道，駭客也會藉此安插惡意連結，對於該單位的狀況，建議安排指導正確的資安觀念，並再次進行演練。

本次演練沒有進行開啟附件測試或開啟附件數為零