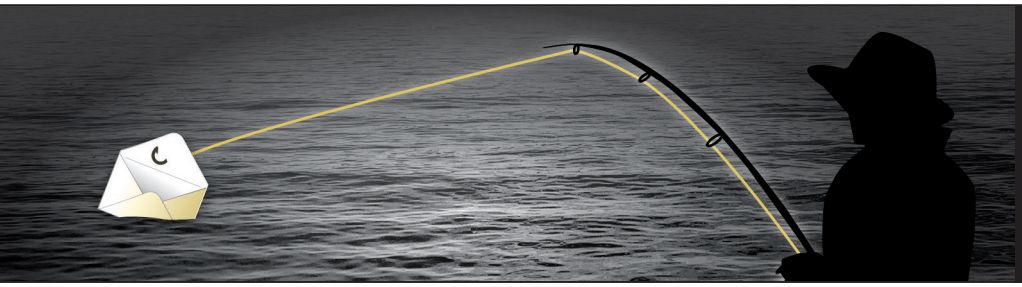
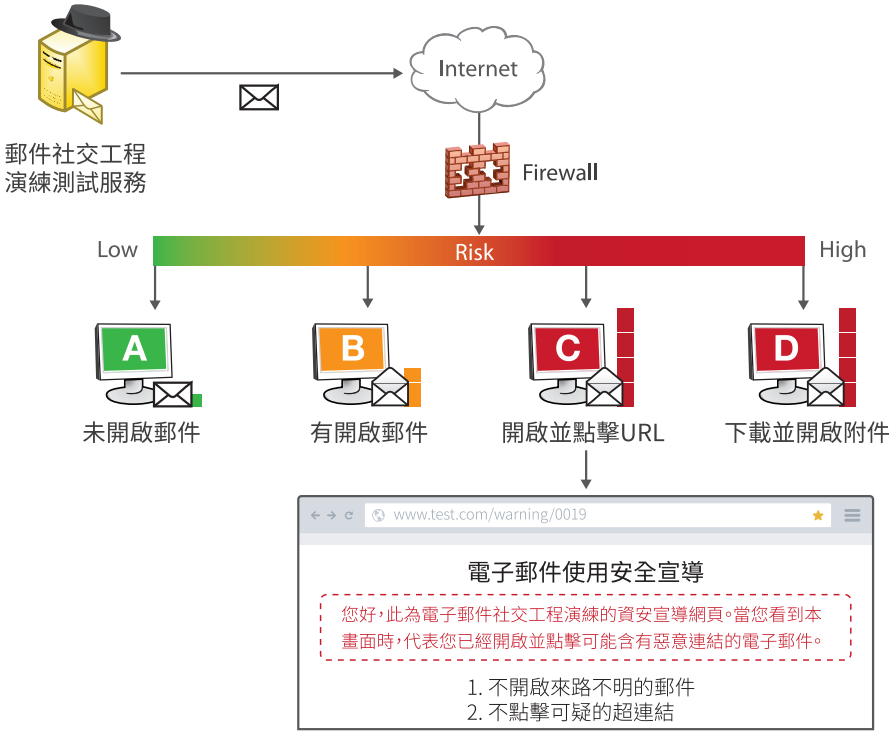


Strengthen internal security awareness. Provide top notch IT consulting services.

郵件社交工程演練服務

社交工程是一種釣魚攻擊的手法，駭客利用郵件使用者的好奇心和容易疏忽的特性，竊取個人及組織有用的資訊，近年來已成為私人企業和公家單位極需重視的資安漏洞。郵件社交工程演練服務提供員工一個安全的練習管道，從中培養謹慎的郵件使用習慣，Cellopoint 顧問團隊根據測試結果分析組織潛在的風險，並提出實際可行的改善建議，目的在補強企業資安漏洞以防微杜漸。



釣魚郵件是最常見的一種社交工程攻擊形式。IT 人員耗費大量人力和時間精心規劃出層層資安關卡，如防火牆、IPS、郵件過濾閘道，及終端安全防護等，諷刺的是人性卻是最容易突破的資安缺口。駭客只需以簡單的折價券廣告信，就能順利通過嚴密防護網，進而竊取機密資料。郵件社交工程演練服務是模擬駭客從 Internet 寄發釣魚郵件給受測員工，以郵件的寄件人、主旨、內容來誘騙收件人“開啟郵件”、“點擊連結”、“開啟附件”等，進而下載惡意程式進行 APT 滲透與竊取敏感資料，客戶可根據測試的數據統計，分析該組織弱點，並訂定企業專屬的安全指標，從而提高員工的資安意識和平日郵件使用的警覺心。

掌握個別員工的資安警覺性是有效管理的關鍵。Cellopoint 模仿駭客手法，實際發送模擬釣魚信，讓組織清楚得知員工接收社交工程演練服務的表現。測試信內容可透過討論客製化設計，而寄送時間和日期也可根據組織需求彈性決定。為了讓組織管理人員確實讀懂測試報告，Cellopoint 記錄造訪網站或下載附件的員工帳號，並將之分成不同風險級別，包含無風險、低風險，或高風險。全體員工可透過實際測試逐漸培養起良好的郵件使用習慣與警覺心，最終目標為達到釣魚郵件入侵零風險。

功能特點

- 藉由提高員工資安意識的方式，降低被駭客攻擊的可能性
- 分析內部安全弱點
- 提供專業的技術諮詢和指導方針
- 提供員工測試表現的數據資料
- 員工使用電子郵件風險評估分析

CELLOPOINT
Secure Your Email

測試流程

1. 提出服務需求

假如您曾有過收到釣魚郵件的經驗，或者單位中有遭受駭客攻擊的跡象，請聯繫我們的資安顧問團隊 CelloConsult Team，並分享貴單位目前的資安情況。這有助於了解您的企業文化，並企劃出適合貴單位的測試模式。

2. 決定測試方案

我們會與您共同擬定合適方案，包含理想的測試時間、客製化的測試信內容，還要考量到員工工作型態等，並參考實際發生過的社交工程攻擊案例，以便設計出有效的擬真攻擊信。

3. 草擬郵件範本

測試信主題可以是八卦、選舉、股票投資，或任何最新的時事新聞，然後在信件中加入文字、圖片、連結、附檔不等的陷阱。另一種類型的作法是將使用者導向到其他模擬的釣魚網站，並誘使他們提供敏感資訊， 不論是帳號或密碼。

4. 規劃測試細節

由於測試是在上班時間進行，因此確保公司郵件系統不會攔截測試信是重要的事前準備；另外也要透過雙方溝通找出恰當的寄送時間，確定員工在進行測試的當下沒有安排訓練課程或其他的活動。

5. 進行郵件發送測試

測試會在沒有預先通知任何部門的情況下，用浮動 IP 發送郵件範本。

6. 彙整測試結果

測試結束後，我們會彙整整體員工的表現結果在一份報告中，其中包含員工姓名、部門和測試表現，以及郵件開啟率、點擊率統計等詳細資料： 1. 未曾打開測試郵件的員工有高度安全意識，無資安風險 2. 打開郵件，但未做其他舉動的員工具有低度資安風險 3. 而打開郵件並點擊 URL 連結，或下載附檔的員工顯示有高度資安風險。測試報告中觸及員工識別資料的部分，不論是測試結果或員工個人資訊皆會依個資法加以保護。

7. 提供改進建議

最後您會得到詳盡的統計資料及每位測試者的表現報告。您可以清楚看出哪些部門或個人在資安意識上需要特別加強，之後可針對這些部門協助補強。而我們也會根據測試結果提供您現有資安漏洞的改進方案。

使用效益

- 降低資料外洩的風險
- 促進安全的郵件使用習慣
- 展現組織加強資訊安全的決心
- 增進內部員工對資訊安全的危機意識
- 降低 IT 人員在資安訓練項目的負擔，使其得以處理其他重要專案