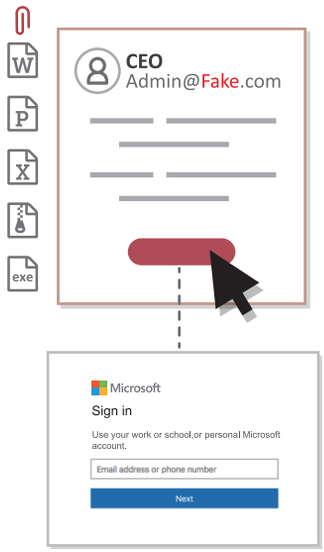
Openfind™ MailGates SEP 社交工程防護解決方案

即時全面保護針對性攻擊與魚叉式攻擊



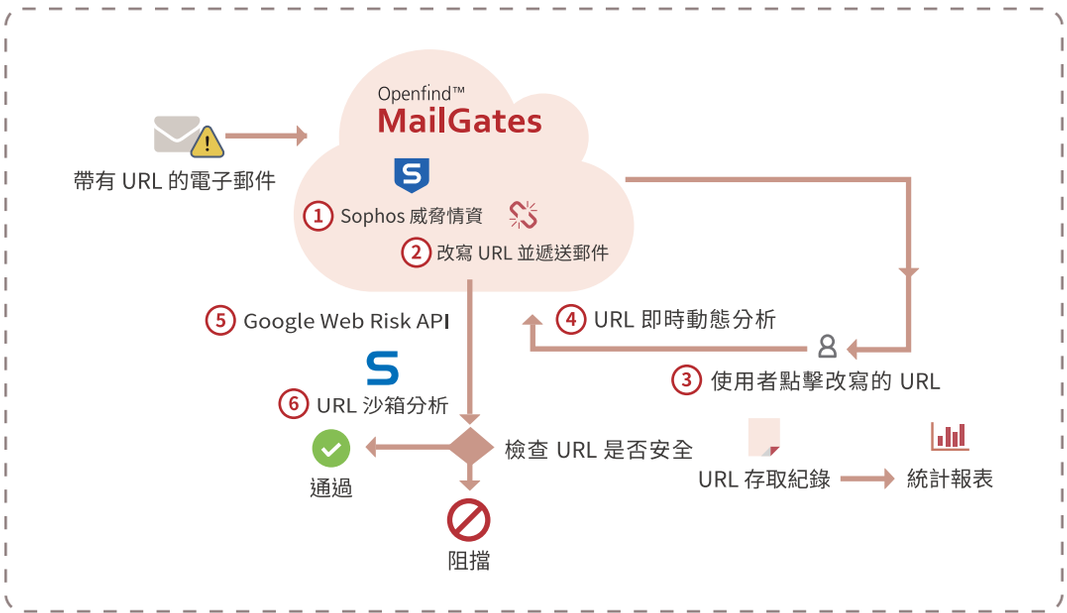
網路釣魚攻擊（Phishing Attack）正以驚人的速度不斷成長，網路犯罪分子欺騙受害者手法也更具針對性。根據統計，每天產生數以萬計新的釣魚網站，而這些網站大多僅活躍 4 到 8 個小時。

社交工程是利用人性弱點進行攻擊的手法，是最常見也最難以防範的攻擊方式，攻擊者通常使用電子郵件中的連結引導用戶連到這些極為相似的釣魚網站，進而騙取電子郵件帳號、密碼及信用卡資訊等機密個資，或將惡意程式（例如，勒索軟體）透過偷渡式下載（Drive-by Download）之攻擊手法，直接下載到用戶的電腦。

傳統的垃圾郵件過濾機制與防毒引擎，可偵測電子郵件中惡意網址，以阻擋大量散佈之釣魚信攻擊，但無法防護針對性攻擊（Targeted Attack）與魚叉式攻擊（Spear Phishing）。攻擊者先寄送帶有安全網站連結之信件，在信件被接收後將網站植入惡意程式，如此一來就可輕鬆繞過僅在接收信件期間檢查 URL 的傳統電子郵件安全系統。

MailGates 社交工程防護解決方案是進階電子郵件防禦技術，可保護組織成員免於針對性攻擊與魚叉式攻擊。社交工程防護機制會將外寄內電子郵件中所有 URL 改寫（Rewrite URL），並在使用者點擊當下即時動態分析（Time-of-Click Analysis）網址，一旦偵測到可疑網址就進行阻擋，避免攻擊者透過偷渡式下載手法誘騙收件者點擊連結，進而植入惡意程式。

MailGates 社交工程防護機制如何運作



1. 當一封郵件通過 MailGates 時，社交工程防護機制會改寫電子郵件中所有 URL，並遞送給收件者。
2. 當收件者點擊連結時，改寫的 URL 會重新導向 MailGates 主機，同步更新 Sophos 全球威脅情資及 Google Web Risk API，以確定目標網址是否為惡意網址。
3. 若 URL 內含檔案，系統會將檔案下載，用 Sophos 防毒引擎掃描或提交至雲端沙箱分析。
4. 完整記錄 URL 存取紀錄，內容包含存取時間、IP 位址、安全性、阻擋原因與動作，提供管理者詳細統計報告，以追蹤組織成員風險狀況。

社交工程攻擊關鍵指標

01 近期熱門議題，誘使收件者點擊連結。

02 偽造的電子郵件密碼過期通知信。

03 精心偽造的相似釣魚網站。

04 誘使收件者輸入電子郵件帳號、密碼或其他機敏資料。

05 偷渡式下載 (Drive-by Download) 攻擊。

MailGates 社交工程防護主要特點：

No	項目	說明
1	點擊即時分析 (Time-of-Click Analysis)	使用者每次點擊 URL 當下即時掃描，以防止潛伏在電子郵件中的未知惡意連結，在組織內部遞送所造成的安全漏洞。
2	整合全球惡意 URL 威脅情資	包含 Sophos、Google Web Risk API 及 MailCloud 等全球威脅情資。
3	URL 沙箱分析	使用者點擊時，下載 URL 中的檔案，並用 Sophos 防毒引擎掃描或提交至雲端沙箱分析。
4	彈性政策設定	管理者可設定改寫信件內文與附檔中 URL，並提供 URL 網域允許/阻擋名單。
5	URL 事後補救機制	阻擋原本為安全，但一段時間後轉變為惡意之 URL。
6	完整 URL 存取紀錄	提供完整 URL 點擊次數、點擊時間、IP 位址、URL 狀態等，以便管理者追蹤已點擊惡意 URL 之組織成員。
7	URL 威脅統計報表	提供各項 URL 統計資訊，包含已阻擋惡意網址或已改寫 URL 之監控報告。

支援郵件系統

Mail2000 | Microsoft Exchange | IBM Notes | Sendmail | Postfix

支援郵件雲端服務

Google Workspace | Microsoft 365 | Exchange Online

用戶端建議需求

Microsoft Edge | IE 11 | Firefox 最新版 | Chrome最新版

Openfind Software Engineered for Growth™

網擎資訊軟體股份有限公司　11286 台北市北投區承德路六段 120 號 7 樓
TEL : (02) 2553-2000 分機 791 潘先生　FAX : (02) 2553-0707　客服專線：(02) 2553-7272
E-mail : info@openfind.com.tw | https://www.openfind.com/