您無法想像，只因一名員工點擊了一封釣魚郵件，可能為您的公司帶來的損失！

SOS 釣魚郵件模擬服務

保護您的業務，將員工從潛在的安全弱點轉化為您最強大的防線!

在現今的數碼時代，釣魚攻擊已成為中小企業面臨的最嚴峻的網絡安全威脅之一。只需一封看似無害的釣魚郵件，便可能導致敏感數據洩漏、財務損失，甚至是企業聲譽的永久損害。

釣魚攻擊的威脅有多大?

34億

每日有超過 34億封 釣魚郵件在全球範圍內發送。

1/4,200

平均每 4,200封郵件 中，就有一封是釣魚郵件。

470萬

2022年，已有超過 470萬宗 釣魚攻擊案件被正式舉報。

常見的釣魚攻擊的運作方式

釣魚攻擊是一種利用社會工程學手法的網絡犯罪，攻擊者精心設計看似真實的通訊內容，誘騙受害者洩露敏感資訊或安裝惡意軟體。這種攻擊手法之所以如此成功，正是因為它不是針對電腦系統的弱點，而是專門利用人類心理弱點所設計。

假冒發件人

攻擊者會偽裝成可信任的組織或個人，如銀行、電子商務平台、政府機構或甚至是受害者的主管或同事。他們使用與正規機構相似的郵件地址、標誌和通訊格式，讓受害者難以識別真偽。這種偽裝通常非常精緻，即使是資訊安全專業人員有時也難以立即辨識。

緊急信息

釣魚郵件常常創造出一種虛假的緊急感，迫使受害者迅速行動而不經思考。例如「您的帳戶即將被鎖定」、「立即確認您的付款資訊」或「您的個人資料已遭到入侵」等緊急信息，意圖讓受害者驚慌失措並做出不理性的決定。這種緊迫感是釣魚攻擊成功的關鍵因素之一。

惡意內容

一旦受害者被誘導點擊郵件中的鏈接或下載附件，攻擊者就能夠執行各種惡意行為。這些行為可能包括引導受害者進入偽造的網站輸入個人資料，或者在受害者的設備上安裝惡意軟體、勒索軟體或遠端控制程式。有些釣魚攻擊甚至不需要任何下載，僅通過點擊惡意鏈接就能夠實現攻擊目的。

數據洩露

釣魚攻擊最終目的通常是竊取敏感資訊，如登入憑證、財務資訊、客戶資料或商業機密。攻擊者獲取這些資料後，可能會直接用於犯罪活動，或在暗網上出售給其他犯罪分子。對企業而言，這種資料洩露不僅可能導致直接的財務損失，還可能引發監管處罰、商業信譽受損，以及長期的客戶信任危機。

> 警惕統計：每日全球範圍內發送超過34億封釣魚郵件，平均每4,200封郵件中就有一封是釣魚郵件。2022年，已有超過470萬宗釣魚攻擊案件被正式舉報。

這些數據凸顯了釣魚攻擊的普遍性和嚴重性。特別是對中小企業而言，由於通常缺乏大型企業的資源和專業資訊安全團隊，更容易成為攻擊者的首選目標。一旦企業成為釣魚攻擊的受害者，不僅面臨直接的經濟損失，還可能遭受聲譽損害、客戶流失、法律訴訟和合規問題等連鎖反應。

為什麼選擇 SOS 的釣魚郵件模擬服務？

面對日益複雜的釣魚郵件威脅，企業需要一種先發制人的防禦策略。SOS 的釣魚郵件模擬服務正是基於「最佳防禦就是先發制人」的理念設計，幫助企業在真實攻擊發生前識別並解決安全漏洞。我們的服務採用 Microsoft® Defender for Office 365 技術，提供全面的測試、培訓和報告功能，從而提升您的員工網絡安全意 識，將潛在的弱點轉化為強大的防線。

設計與定制模擬

- 根據您的行業特性和當前網絡威脅趨勢，量身定制釣魚郵件模擬場景
- 模擬真實攻擊場景，包括最新的釣魚技術和社會工程學策略
- 確保模擬過程中企業數據安全，避免任何實際風險
- 針對不同部門和職位層級設計不同難度的釣魚測試

部署與分析

- 無縫整合至您現有的 Microsoft 365 環境，無需額外硬件或複雜安裝
- 根據預設計劃或特定時間點發送模擬釣魚郵件
- 實時監控和記錄用戶對模擬釣魚郵件的反應和行為
- 深入分析用戶互動數據，識別組織中的安全弱點和風險區域

培訓與改進

- 為「中招」的員工提供即時且針對性的安全培訓
- 通過互動式學習模塊提升員工識別和應對釣魚攻擊的能力
- 定期進行後續測試，評估培訓效果和安全意識提升情況
- 針對反覆「中招」的員工提供強化培訓和個人輔導

詳細報告

- 提供全面的數據分析和視覺化報告，展示測試結果和趨勢
- 識別組織內的高風險用戶、部門或行為模式
- 追蹤安全意識改進情況和投資回報率
- 為管理層提供清晰的安全狀況評估和改進建議

SOS 釣魚郵件模擬服務的獨特優勢在於它不僅僅是一次性的安全測試，而是一個持續的安全意識培養過程。我們認為，真正有效的網絡安全防禦必須將技術解決方案與人為因素相結合。通過我們的服務，您的員工將從組織安全的潛在弱點，轉變為主動識別和抵禦釣魚攻擊的第一道防線

客戶受益分析

採用 SOS 釣魚郵件模擬服務為您的企業帶來全方位的安全提升和商業價值。我們的服務不僅能夠幫助企業降低網絡安全風險，還能夠提升整體組織的安全文化，為企業的長期發展提供堅實的安全基礎。以下是您的企業將獲得的主要受益：

降低釣魚攻擊風險

通過模擬真實的釣魚攻擊場景，我們幫助企業提前發現並補救安全弱點，顯著減少釣魚攻擊成功的可能性。研究表明，經過有效的釣魚郵件模擬訓練的組織，其遭受成功釣魚攻擊的風險可降低高達90%。這意味著您的企業可以避免潛在的數據洩露、財務損失以及聲譽損害，保護企業的核心資產和競爭力。

專業安全意識培訓

我們的服務不僅能夠識別安全風險，還提供針對性的專業培訓，幫助員工提高安全意識和威脅識別能力。通過互動式學習模塊和實時反饋，員工能夠掌握識別釣魚郵件的關鍵技能，學會如何正確應對可疑通訊，從而將組織的人為安全弱點轉化為強大的防禦力量。這種「學中做、做中學」的方法比傳統的安全培訓更加有效，能夠顯著提高員工的安全意識持久性。

全面安全狀況報告

我們提供詳盡的數據分析和視覺化報告，幫助您準確了解公司的安全現狀和潛在風險區域。這些報告包括各部門和職位的風險評估、員工反應統計、安全意識改進趨勢以及具體的風險緩解建議。基於這些數據，管理層可以做出更明智的安全投資決策，制定更有針對性的安全策略，優化資源分配，最大化安全投資回報。

無縫整合與便捷管理

我們的服務完全整合於 Microsoft 365 平台，無需額外的硬件設備或複雜的配置過程。這種無縫整合確保了服務的快速部署和便捷管理，最小化對日常業務運營的干擾。此外，我們提供直觀的管理界面和自動化報告功能，減輕IT團隊的工作負擔，使安全管理更加高效。即使是資源有限的中小企業，也能夠輕鬆實施和維護這一重要的安全措施。

服務效益	SOS 釣魚郵件模擬服務	傳統安全培訓
釣魚攻擊防禦成功率	提升 85-90%	提升 30-40%
員工安全意識持久性	6-12 個月	1-2 個月
安全投資回報率 (ROI)	平均 300%	平均 50%
實施與維護複雜度	低 (無縫整合)	中至高
可量化安全改進指標	詳細數據報告	有限或無

優惠試用方案

為了幫助更多中小企業提升網絡安全防護能力，SOS 現推出限時特別優惠方案，讓您以極具競爭力的價格獲得專業級的釣魚郵件模擬服務。這是保護您企業數位資產的最佳時機，不要錯過這個提升安全防線的寶貴機會。

優惠方案內容

只需 **HK$1,200**，即可享受試用我們的釣魚郵件模擬服務套餐，為您的企業構建堅實的第一道防線。相較於市場上同類服務動輒數萬港元的價格，此方案為您節省安全投資成本，同時提供同等專業水準的防護能力。

此特別優惠套餐包含：

- 1 次全面的釣魚郵件模擬活動 (最多可測試 300 名員工)
- 根據您行業特性定制的釣魚郵件模板
- 即時安全意識培訓材料 (支援中英文)
- 詳細的結果分析報告和改進建議
- 專家諮詢服務 (1 小時)

優惠條件與限制

限量名額:此特別優惠僅適用於首 **50** 位客戶，先到先得，額滿即止。我們之所以設置此限制，是為了確保每位客戶都能獲得最高質量的服務和最專業的支援。

優惠有效期： 此優惠方案有效期至 **2025 年 6 月 30 日**。即使您現在可能沒有即時需求，也可以提前購買並保留使用權，在未來一年內任何時候啟用服 務。

技術要求： 客戶需擁有 Microsoft Defender 授權才能享受此優惠。這是因為我們的服務基於 Microsoft Defender for Office 365 平台開發，需要相應的授權支援。如果您尚未擁有此授權，我們的顧問可以為您提供獲取建議。

85%

成本節省 相較市場同類服務

90%

風險降低 經測試後釣魚攻擊成功率下降

100+

企業受益 已成功服務的香港中小企業數量

30分鐘 快速部署

服務啟用所需時間

立即行動，搶佔限量名額，為您的業務構建更堅固的安全防線!

官方網站

訪問我們的官方網站，了解更多關於 SOS 安全服務的詳細信息、客戶案例和技術資源。

網址: www.soshk.com

電子郵件

通過電子郵件聯繫我們的客戶服務團隊，獲取個性化方案建議或技術支援。

郵箱: enquiry @soshk.com

電話諮詢

直接與我們的安全專家通話，立即解答您的疑問，獲取即時支援。

熱線: +852-3525 1828