Proofpoint Security Awareness and Training 內容

改變使用者行為以減少風險

重要功能

內容資料庫
根據威脅、使用者、地區和格式尋找內容

基礎課程
資安長/中小企業導向學習路徑，可快速追蹤實作並讓新使用者上手

使用者評估
了解使用者、群組和部門的優缺點

訓練單元
涵蓋安全性、隱私權及使用者偏好設定的多種主題和格式

自訂和提供內容
確保使用者可獲得個人化學習體驗，想要的話也可透過學習管理系統 (LMS) 提供內容。

安全性意識資料
現成資料可促成有效且有效率的提升意識活動和及時的威脅警示和報告

翻譯
基礎課程有 40 種語言版本，所有內容至少 6 種語言版本

模擬
完整模擬威脅資料庫可評估使用者辨識社交工程攻擊的程度

Proofpoint Security Awareness Training (PSAT) 提供您員工經證實的內容，以產生可測量的行為改變。我們的解決方案可讓您在適當時間為適當人員提供適當訓練。這可確保正確回應安全性和隱私權的威脅和需求。使用我們的解決方案，您可享有下列優勢：

- 評估和訓練使用者
- 獲得適用於安全性意識活動的實用資料
- 自動化報告
- 修正可疑電子郵件

Proofpoint Security Awareness Training 內容包括多種訓練和其他資源。

基礎課程、學習路徑和翻譯

以資安長/中小企業導向課程和學習路徑，加快行為改變。基礎課程提供使用者重要知識，協助使用者從基本進步至進階能力。組織還可搭配角色專屬學習路徑，運用專家指導，快速追蹤使用者學習和訓練管理情況。

所有基礎課程翻譯為超過 40 種語言，其他課程和提升意識資料則有超過 6 種語言版本。

評估內容：了解使用者需求

談到安全性和隱私權做法時，務必了解員工知識落差。我們協助您提供個人化安全性意識訓練，並為組織識別更多安全性風險。

我們的ThreatSim模擬攻擊協助您評估員工對實際威脅的懷疑程度。這些模擬攻擊包括網路釣魚和USB攻擊。您可以使用CyberStrength知識評估，判斷員工對多個重要安全性主題的知識。

THREATSIM 模擬網路釣魚和 USB 攻擊

模擬攻擊範本

您可以針對多種威脅評估使用者。這些威脅包括惡意附件、內嵌連結、USB 攻擊及索取個人資料。您可在超過 36 種語言版本的數千個範本中選擇。

範本類別：

- 雲端
- 商業廣告
- 消費者
- 公司
- Proofpoint 威脅情報
- 週期性產品
- USB
- 產業

教學時刻登陸頁面

您可以運用「及時教學」，也就是員工與假造網路釣魚電子郵件互動的時刻。這些登陸頁面會說明發生的情況。同時列出與實際攻擊相關的危險。此外，也提供避免日後攻擊的建議。

教學時刻類型：

- 自訂
- 內嵌
- 錯誤訊息
- 互動式
- 影片

CYBERSTRENGTH 知識評估

自訂和預先定義的知識評估

您可以針對除了模擬攻擊外的多種主題評估使用者。您可在超過 400 種內建問題中選擇，或自行新增問題。此外，您可以在多種不同類別的 17 種預先定義知識評估中選擇。

預先定義知識評估：

- 55 題、33 題和 22 題概略評估
- GDPR
- 內部威脅
- 線上安全
- 密碼保護
- 支付卡產業
- 網路釣魚
- 個人識別資訊 (PII)
- 防範入侵
- 受保護的健康資訊 (PHI)
- 保護個人資料
- 進階保護電子郵件
- 基礎保護電子郵件
- 安全性保全
- 行動安全性

Proofpoint 訓練單元

我們獲獎肯定的靈活訓練單元能以遊戲、互動式和影片形式使用。這些訓練單元是根據學習科學原則製作，目的在於推動行為改變。我們的單元源自 Proofpoint 威脅情報，根據不斷變化的威脅情況確保關聯性。

關於單元

- 課程簡短且聚焦。單元平均只需 5 到 15 分鐘即可完成。這可讓使用者在整個訓練過程中專心，更可能學到並記住內容。
- 可自訂內容，確保為使用者量身打造。自助 Customization Center 可讓您編輯文字、畫面、影像、問題、答案，甚至重新排列內容。
- 可在評估中為使用者自動報名訓練單元。這可確保使用者在適當時間接受適當訓練。
- 訓練單元可在行動裝置上使用，且為無障礙設計，並符合美國第 508 節標準和 Web 內容無障礙指南 (WCAG) 2.0 AA 標準。

訓練單元主題

- Application Security (應用程式安全性)
- Anti-Fraud and Bribery (防詐騙和賄賂)
- Anti-Money Laundering (防洗錢)
- Avoiding Dangerous Attachments (防範危險附件)
- Avoiding Dangerous Links (防範危險連結)
- Business Email Compromise (企業電子郵件詐騙)
- Compromised Devices (裝置遭入侵)
- Data Protection and Destruction (資料保護和銷毀)
- Email Security (電子郵件安全性)
- Email Security on Mobile Devices (行動裝置電子郵件安全性)
- FERPA (家庭教育權利及隱私法)
- GDPR (一般資料保護規則)
- Healthcare (醫療照護)
- Insider Threats (內部威脅)
- Phishing (網路釣魚)
- Malware (惡意軟體)
- Mobile Security (行動安全性)
- Passwords (密碼)
- PCI (支付卡產業)
- Physical Security (實體安全性)
- PII and Personal Data Protection (個人識別資訊和個人資料保護)
- Privileged Access Awareness (特殊權限存取意識)
- Ransomware (勒索軟體)
- Role-based modules for customer service, finance and management (適用於客戶服務、財務和管理部門的角色型單元)
- Safe Social Networking (安全社交網路)
- Safe Web Browsing (安全 Web 瀏覽)
- Secure Printing (安全列印)
- Security Beyond the Office (辦公室外的安全性)
- Security Essentials (安全性要點)
- Travel Security (旅遊安全性)
- URL Training (URL 訓練)
- USB Device Safety (USB 裝置安全)
- Working From Home (在家上班)
- Workplace Security in Action (實作工作環境安全性)
- Video: Workplace Security in Action (影片：實作工作環境安全性)

TeachPrivacy 訓練單元

我們與 TeachPrivacy 合作，拓展提供的內容種類和訓練類型。所有內容均經我們的學習和發展團隊審查，確保為您使用者提供一致的指導。

TeachPrivacy 專精於隱私權法規和要求。我們透過其豐富隱私權內容，為您的專屬挑戰和文化量身打造隱私權和法規遵循訓練。

TeachPrivacy 主題

- 加州健康隱私權
- 加州消費者隱私保護法
- 家庭教育權利及隱私法
- 聯邦貿易委員會紅旗規則
- 一般資料保護規則
- 金融服務法現代化法
- 健康保險可攜性及責任法
- 惡意軟體和隱私權
- 支付卡產業
- 聯邦政府承包商的隱私權
- 德州健康隱私權
- 勒索軟體

自訂和提供內容

您可以使用自助 Customization Center，為您的使用者改善內容關聯性。運用與您使用者相關的文章、影像和問題，輕鬆量身訂做訓練。快速複製並修改單元、課程和頁面，即時進行必要變更。甚至可透過一個開關，從訓練單元 (含問題) 切換為提升意識單元。

為了維持效度，學習科學評估人員會提供意見回饋，讓您設計有效的學習體驗。舉例來說，如果挑戰的時間長度、螢幕上的內容量或問題數量不正常，我們會告訴您。

若為有自己的學習管理系統 (LMS) 且使用 SCORM 檔案的組織，管理員可輕鬆自訂訓練單元並匯出至其 LMS。也可將多個單元合併為一個，甚至排定使用者可上課的優先順序。

安全性意識資料

我們提供多種提升意識單元、影片、海報、影像、電子報、文章、資訊圖等，加強您的訓練計劃。這些資料專為讓您與使用者持續討論網路安全性。注意安全性可減少您組織的風險。

- 您可以使用組織的標誌，自訂大部分提升意識資料。可在「安全性意識資料」入口網站存取原始檔案。
- 許多提升意識資料提供 20 種語言版本。

Attack Spotlight 和威脅警示

我們運用市面領先的威脅情報，協助您了解遭攻擊的對象和方式，並確保他們接受適當訓練。而我們的持續威脅情報讓您能掌握新興威脅，以便訓練和提升意識單元可立即讓使用者準備好辨識和防範新威脅。

Attack Spotlight：告訴使用者最新威脅。這份每月發行的及時內容來自 Proofpoint 威脅情報看到的實際網路釣魚攻擊、技術和騙術。

- COVID-19 (新型冠狀病毒)
- DocuSign Phishing (網路釣魚)
- Domain Fraud (網域詐騙)
- Dridex
- Fake Browser Updates (偽造瀏覽器更新)
- Fake OneDrive Emails Steal Logins (偽造 OneDrive 電子郵件偷竊登入資料)
- Fraudulent Shipping Notifications (偽造貨運通知)
- 外觀相似的網站欺騙使用者
- Microsoft Office 365 Credential Phishing (Microsoft Office 365 認證網路釣魚)
- OneDrive Phishing Campaign (OneDrive 網路釣魚活動)
- Phishing Campaign Delivers Dangerous Trojan (網路釣魚活動傳送危險特洛伊木馬程式)
- Scammers Mimic Real Banking Emails (騙徒模仿實際銀行電子郵件)
- Malicious Cloud Applications (惡意雲端應用程式)

威脅警示：快速警示使用者 Proofpoint 威脅情報看到的特定流行攻擊。

- COVID-19 Credential Phishing (U.S. Retailers) (COVID-19 認證網路釣魚 (美國零售商))
- COVID-19 Phish Spreading Malware (U.S. Infrastructure) (COVID-19 網路釣魚散播惡意軟體 (美國基礎架構))
- WebEx Credential Phishing Lures (WebEx 認證網路釣魚騙術)
- Zoom Credential Phishing Lures (Zoom 認證網路釣魚騙術)
- Zoom Phishing Attacks Spread Malware (Zoom 網路釣魚攻擊散播惡意軟體)
- 每週還有更多攻擊

提升意識影片：透過吸引人且有趣的影片，讓您的員工認識安全性意識的重要。下列挑選超過 50 部影片：

- 安全意識影片：點按前多想一下 (搶救資安大行動)
- 安全意識影片：雲端安全嗎？
- 安全意識影片：使用公用 Wi-Fi 時請小心
- The Defence Works Video: (The Defence Works 影片：) Not Particularly High Tech (並不特別使用高科技)
- The Defence Works Video: (The Defence Works 影片：) Oh… My Password! (噢… …我的密碼！)
- The Defence Works Video: (The Defence Works 影片：) Swiped Right Into Trouble (向右滑就糟了)
- 60 Seconds to Better Security: (60 秒改善安全性) What is Smishing? (什麼是簡訊釣魚？)
- 60 Seconds to Better Security: (60 秒改善安全性) What is Phishing? (什麼是網路釣魚？)
- 60 Seconds to Better Security: (60 秒改善安全性) What is BEC? (什麼是企業電子郵件詐騙？)
- 還有更多內容

資訊圖：運用下列精選內容，加強安全運算的基礎知識：

- Business Email Compromise Attacks (商業電子郵件詐騙攻擊)
- Internet of Things (物聯網)
- Phishing Decision Tree (網路釣魚決策樹狀圖)
- Phishing: A Scammer's Sinister Scheme (Regular and Expanded) (網路釣魚：騙徒的邪惡陰謀 [一般和擴充版本])
- Tax-Related Schemes (稅務相關詐騙)
- Understanding Ransomware (瞭解勒索軟體)
- 還有更多內容

電子報和文章

- 安全性電子報和文章說明許多不同主題：返校、危險連結和附件、假期購物、內部威脅、密碼、網路釣魚、實體安全性、旅遊秘訣等。

海報：彰顯訊息並加強學習。

- Avoiding Malicious Attachments (避免惡意附件)
- Be Smart About Mobile Security (聰明處理行動安全性)
- Destination Unknown URL Security (目的地不明 URL 安全性)
- Dangerous USB Devices (危險 USB 裝置)
- Is Physical Security on the Menu? (是否具實際安全性？)
- Not All Offers Are as Sweet as They Seem (某些優惠實際上圖謀不軌。)
- 還有更多內容

其他內容

- 插圖和創作其他內容的方向
- 「Cybersecurity Consequences」(網路安全性後果) 遊戲
- 「Lock Before You Walk」(離開前加以鎖定) 便利貼
- 迷因
- 明信片
- 尋字遊戲
- 還有更多內容

方案資料

要讓方案成功，每個參與的人都必須了解參與的原因及對他們的期望。這就是我們安全性意識方案內容包括給管理員的專家指導原因，這可讓他們了解最有效執行方案的方式。我們也提供鎖定對象的通訊內容給重要相關人員和使用者。我們的方案資料分為四類：

- 最佳做法
- 成功關鍵
- 活動

這些資訊有助於方案管理員建立信任，並加強安全性意識文化。

最佳做法：最佳做法文件協助方案管理員推動最有效的行為改變。方案是否為全新或已執行一段時間並不重要。這份內容提供時程、最佳做法和執行方案的建議計劃資訊。

活動：活動可簡化管理，並協助創造精心安排的使用者體驗。這包括所有內部通訊資源，以及在組織中推行多管道安全性意識計劃所需的內容。

成功關鍵：這些播客、網路研討會、研究和其他內容都是為了管理員製作。有助於管理員向重要對象說明安全性意識訓練的價值、讓人同意接受更多訓練、帶領後果模型討論等。同時提供照稿的預先錄製簡報，涵蓋網路釣魚、身分竊取和社交工程等多個主題。管理員可在實體或線上訓練課程運用這些內容。

深入了解

試用訓練單元示範版本，並檢視安全性意識資料：
https://www.proofpoint.com/us/resources/try-security-awareness-training