

RSA/Outseer FraudAction Service

外部偽冒事件偵測關閉服務



RSA/Outseer FraudAction Service 特色

1. 釣魚詐騙及偽冒行動軟體關閉下架：

RSA/OUTSEER 的關閉下架執行文件是發停止並終止信函(Cease and Desist Letter)，要求終止一項行為(cease)，並且再也不從事(desist)，否則將面臨法律訴訟，非一般的申訴文件或程序。

若發現並確認釣魚詐騙(Phishing Scam)或品牌侵犯(Brand Abuse)威脅，RSA/OUTSEER 會發停止並終止信函(C&D Letter)給 ISP/註冊機構/託管業者，請其協助立即執行強制關閉。

若發現偽冒行動軟體(Rogue App)，RSA/OUTSEER 會發停止並終止信函(C&D Letter)給行動軟體平台管理業者，請平台管理業者協助立即執行強制關閉下架。

經委託客戶與 RSA/OUTSEER 共同確認有 Phishing Scam(網路詐欺)或 Brand Abuse(品牌冒用侵犯)時，委託客戶確認要執行關閉時，RSA/OUTSEER 會代位執行關閉釣魚詐騙威脅的相關鏈接、網頁或網站。如有需要，執行層級會上升至事件當地的 CERT 主管機關或 Cyber Police 網路警察。

2. 法律事證資訊：

企業與其客戶或網站業者萬一發生釣魚詐騙(Phishing Scam)及偽冒行動軟體(Rogue App)相關訴訟，RSA/OUTSEER 服務所保存的監測記錄及資料具備法律事證效力，可以提供企業作為呈堂供證資訊。

3. 海外分支機構金檢提供協助：

金融企業使用反釣魚詐騙及偽冒行動軟體偵測關閉服務，海外分支機構的外部偽冒相關資安全檢，較容易過關。

4. 形成聯防機制：

RSA/OUTSEER 與全球各大入口網站、ISP/註冊機構/託管業者、官方和不斷增長的第三方行動軟體平台及主要資安業者合作超過 17 年，已形成覆蓋全球 365x24x7 運作的網際網路反詐欺聯防網。萬一發現釣魚詐騙威脅，RSA/OUTSEER 可立即通知反詐欺聯防網絡成員，在最快的時間內啟動針對該釣魚詐騙相關鏈接網頁或網站的阻斷機制。

選購暗網情資提供：

- (一) Indicators of Compromised (IP 黑名單、Email 黑名單)
- (二) 國際洗錢帳戶情資
- (三) 實體地址黑名單情資
- (四) 被駭國際信用卡/金融卡(Credit/Debit)卡號情資
- (五) 暗網客戶外洩機敏情資

台灣金融業客戶：

臺灣金控、第一金控、中國信託金控、國泰人壽、國泰世華銀行、富邦金控等 30 家金融機構。