NICE · ACTIMIZE

以詐騙控制應對行動通訊時代

目錄

行動銀行使用率增加 3

金融機構現今面臨的挑戰 3

管理不斷擴大的資料數據 3

不斷演變的詐騙形式 4

行動通訊業的快速發展 4

廣泛使用行動通訊設備 4

行動化的詐騙減緩 5

使用 Actimize 詐騙解決方案，識別並打擊行動通訊詐騙 6

Actimize 行動銀行詐騙防護的主要特點 6

由於行動銀行的使用迅速增加，詐騙人士也隨之快速增長。媒體上充斥行動電話詐騙和入侵的消息，從利用行動瀏覽器盜取信用卡資料、繼而入侵帳戶；以至使用先進的行動惡意軟體，自動執行未經授權的交易等等。另一方面，銀行業務方面正引進更多的行動和瀏覽器功能，滿足消費者的需求。詐騙和風險策略小組有責任實行所需措施，促進企業業務發展，同時防範詐騙的威脅。

行動銀行使用率增加

金融機構現今面臨的挑戰

儘管手機詐騙的環境不斷變化、不斷演進，金融機構面臨的挑戰是顯而易見的。

管理不斷擴大的資料數據

全球使用行動電話的趨勢，帶來了全新的數據使用工具。這些數據必須加以收集和管理，擴大對顧客的瞭解，並保護業務及其顧客免受詐騙活動影響。要有效使用這些數據絕不容易，大致原因如下：

- 據估計，行動設備可取得多達 300 個不同的原始屬性；而行動保安點解決方案，則可產生額外 100 個已運算或人工的屬性。這樣的資料量帶來多種存儲、通訊和資料延遲的問題。
- 行動設備和操作系統各有不同，這種差異令格式化數據的過程更為複雜。
- 法律規定絕對是考量之一，因為一些可用的資料（如地理位置和設備上的個人資料）可能觸及隱私問題，不同國家的法律對此有不同規定。
- 透過追查交易及活動紀錄，現在企業能更準確找出目標客戶，並向他們推廣更合適的金融服務和產品。

不斷演變的詐騙形式

詐騙人士不斷開發精密的方法來突破銀行現有的風險控制。一旦業界開始打擊一種類型的攻擊，騙子就迅速演進他們的攻擊方式，為詐騙團隊建立持續「急起直追」的步調。除了簡單的網路釣魚詐騙行為，最先進的惡意軟體攻擊現在會將惡意代碼注入網路銀行的應用程式中。由於採用能驗證設備使其免受詐騙的設備技術，使用應用程式攻擊的騙子已大幅的演進。騙子還開發了行動帳戶接管的攻擊，他們可以識別客戶的最新交易以通過該機構客服中心的共同驗證流程。

行動通訊業的快速發展

金融業已習慣資訊技術供應商提供定期更新的服務，以因應不斷變化的市場需求，例如微軟的 Windows 過去每三年一次發布的桌面操作系統。這些定期發布的週期允許機構和供應商採用適當的 Y 型計劃資源，確保自己系統和流程的兼容性。現今，隨著行動供應商的激增（設備和操作系統），變更週期變得更快速且結構更小，因此金融機構很難跟上變化。金融機構需要具有清楚路線圖的合適系統來預測這些變化，以及「自成一型」的能力，以擷取新資料並建立無線網路點對點傳輸規則和客戶資料來解決眼前的問題。

廣泛使用行動通訊設備

行動設備和相關應用程式的公眾採用率成長迅速，且消費者已經習慣立即使用的便利性。金融機構、零售商和其他商 家已將行動管道視為重要的商機，增加隨身硬碟產品、服務和客戶選擇。這個企業良機，對詐騙資訊技術團隊和系統來說，卻可能是個挑戰。交易量和資料點規模需要健全、可擴展的架構，以及一群經驗豐富、能有效部署和管理適當詐騙解決方案的技術團隊。

行動化的詐騙減緩

最近的艾特分析報告「行動通訊時代：引發詐騙革命」中概述行動詐騙的概況，並詳細指出，當採取了合適的安全監控時，行動通訊環境其實可以比網路環境更為安全。此報告詳述了從 2013 年 10 月至 2014 年 4 月，與超過 60 家供應商、金融機構防詐騙主管，以及商家防詐騙主管訪談的結果。

擴展艾特報告中涵蓋的概念，以下列出幾種金融機構能夠落實以防範行動化的詐騙控制方式，利用提升的詐騙分析和網路詐騙減緩策略，以多種策略體現手機的獨特性。

1. 掌握有效的行動資料收集

透過有效的資料處理，金融機構必須了解隱藏在行動資料中的機會和威脅。他們應該識別所有可能的屬性， 提供豐富的資料來源，使設備能進行辨識和設備風險分析。

2. 跨管道的檔案和分析

由於惡意活動往往利用漏洞，從一個管道攻擊至另一管道，因此防範行動威脅時，應考量所有可用的銀行管道。金融機構可以透過利用跨管道的檔案，識別這些漏洞，以保護整個金融環境。

3. 使用分析結果來管理漏洞

機構應在所有管道識別設備，並評估其在銀行活動背景的漏洞，確保為客戶來好良好體驗，防止不必要的干擾。被惡意軟體入侵，或遭多個使用者使用的設備，即使已偵察出漏洞，仍可以用來在已知客戶和受益人之間，進行合法的交易。

4. 時刻僅記保持收益

機構的重點不應該僅僅放在設備上，也須顧及收集資料並分析其客戶金錢行為的需要，同時確保設備和管道分析能提供風險的全面觀點。

5. 與時俱進的詐騙防禦

當威脅環境持續發展和變化，金融機構必須確保行動銀行的防禦具有靈活性的發展，有效保護企業及其客戶免受當前和未來的威脅。

使用 Actimize 詐騙解決方案，識別並打擊行動通訊詐騙

Actimize 的銀行詐騙解決方案，提供真實、端對端的能力，支援詐騙管理過程中各個環節：從初步偵測，以至警報整合、檢視、 調查、解決方案和監督等等。

Nice Actimize 於全球頂尖金融機構中，在遠端銀行詐騙活動的所有層面，都擁有獲認證的相關經驗，可讓企業填補現有遠端管道安全程序的漏洞，或提供完整的詐騙風險管理程序。

Actimize 行動銀行詐騙防護的主要特點

Actimize 的銀行詐騙解決方案，提供真實、端對端的能力，支援詐騙管理過程中各個環節：從初步偵測，以至警報整合、檢視、 調查、解決方案和監督等等

統一的行動資料模型

高效擷取金融機構使用的格式化行動設備資料，包括第三方行動工具解決方案。

全面的漏洞辨識

準確識別任何設備的漏洞，當中包括金錢交易和客戶活動，讓企業瞭解真正風險。

高效的跨管道檔案與分析

執行客戶多管道資料分析，確保能識別每一個金錢和非金錢的交易，並分析當事人在所有管道上的活動。

可擴展、靈活的平台功能

你可獲取不同來源的資料，包括 Actimize 市場領先解決方案、由企業改良或建立的系統、或由第三方供應商提供的系統。這樣你便可詳盡及深入瞭解金融犯罪的風險。

整合的警報和個案管理

以能自動彙整所有機構內金融犯罪環境的警報來提高調查效率和準確度，提供風險的單一觀點，並允許分析人員在此背景中檢視客戶活動。企業可從整個企業提升的報告獲益，進而改善詐騙風險管理和策略規劃。

關於 NICE Actimize

NICE Actimize 為地區和全球金融機構以及政府監管機構提供金融犯罪、風險與合規解決方案，是業內最大和最廣泛的供應商。一直以來在業界領先群雄，NICE Actimize 的專家運用創新技術保護機構，並透過識別金融犯罪、防範詐騙和提供守規規條，守護消費者和投資者的資產。本公司提供即時、跨管道詐騙防範、防制洗錢偵測和交易監控方案，以解決付款詐騙、網路犯罪、制裁監測、市場濫用，客戶盡職調查和內線交易等相關問題。

info@niceactimize.com | www.niceactimize.com | www.niceactimize.com/blog | @nice_actimize | linkedin.com/company/actimize | facebook.com/niceactimize

NICE · ACTIMIZE