jamf

Security 360：

年度趨勢報告

行動裝置

前言

在各行各業與不同應用場景中，從零售工作流程到醫療作業，企業領導者透過行動技術創新，改變人們的工作方式，以達成最佳化的組織成果。對許多產業的員工而言，行動裝置（例如智慧型手機與平板電腦）是他們在工作中唯一使用的裝置。現代職場的重點在於賦能員工，讓他們能夠隨時隨地、使用任何他們想用的 裝置連線工作。

行動工作的其中一個關鍵驅動力，是將行動性納入企業 IT 服務的一環。 行動裝置不再只是輔助設備，它們正逐漸成為主要的工作入口。雖然行動性早已進入職場，但它如今更深入地整合至各項核心工作流程中。 現今的職場不僅要求卓越的數位體驗，更需具備**安全性**，以在任何地點都能發揮員工的最大生產力。

— Josh Stein，
產品管理副總裁

介紹

Jamf 的 Security 360 報告根據真實客戶事件、威脅研究與過去一年的產業趨勢分析所整理而成。本報告聚焦於行動威脅情勢，揭示組織面臨的風險與挑戰。

我們評估了各種常見攻擊手法，這些手法主要目的是欺騙使用者、入侵行動裝置，甚至滲透整個組織。這些攻擊不僅限於裝置漏洞，因此我們的分析也涵蓋了高風險應用程式、網路威脅等多種面向。

除了趨勢分析外，報告也納入 Jamf 資安長的觀點，提供保護終端使用者、裝置、應用程式與網路層級的實務洞見。

研究方法

為了解並量化這些資安趨勢的實際影響，我們分析了 140 萬台由 Jamf 保護的裝置樣本。分析於 2025 年第一季進行，涵蓋前 12 個月的資料，橫跨全球 90 個國家與多個平台，主要包括 iOS、iPadOS 與 Android 裝置。

為保障隱私與維持高標準，我們所分析的 資料來自匿名彙總的日誌紀錄，不包含任何個人或 組織識別資訊。

研究目的

我們希望透過此分析，幫助組織與使用者了解現有的資安趨勢，並學習如何降低風險。內容同時也介紹了 Jamf Threat Labs 最具影響力的研究成果，包括他們所發現的威脅與漏洞。我們希望透過這份資訊，破除錯誤迷思，協助您了解該如何部署防護措施，以保護使用者與資料安全。組織可實施的一些常見資安最佳實務，包括：

- 作業系統持續與即時更新
- 使用者教育與訓練
- 應用程式審查與控管
- 多重要素驗證（Multi-Factor Authentication）
- 零信任安全架構
- 建立並管理合規性基準
- 為企業 資料制定合理的使用政策

我們將本報告的分析內容分為四大類別，我們發現這些類別全球組織最關注的資安優先事項：

I. 行動釣魚攻擊

II. 漏洞管理

III. 應用程式風險

IV. 惡意軟體與間諜程式

本報告的統計數據 涵蓋 **Apple** 與 **Android** 裝置。

報告中的多數分析來自 Jamf 威脅情報，由原始研究、真實數據、新聞分析與資料來源彙整而成。Jamf 威脅情報由 Jamf Threat Labs 與資料科學團隊主導，針對裝置、應用與網路流量持續監控風險、威脅與零時差漏洞。

我們 也針對**Mac 裝置**推出了《Security 360》報告 ，您可在**這裡**查閱：

行動裝置的主要趨勢

I. 行動釣魚一直是企業面臨的挑戰

釣魚攻擊仍是攻擊者常用的手法，在當今資安威脅版圖中依然活躍。2024 年 9 月，**Apple 發布了一篇 部落格文章**，向使用者提供指引，幫助他們「避免詐騙並了解收到可疑郵件、電話或其他訊息時該怎麼做」。無論平台或作業系統多安全，社交工程的設計就是從裝置中最不安全的部分入手，也就是使用者本身，以滲透企業資料。

II. 單一漏洞就可能造成全系統淪陷

軟體中存在漏洞是事實，不論是作業系統還是應用程式，我們每天使用的工具都可能潛藏風險。根據 **NIST 特別出版品 800-124r2**，「一般軟體平均每 1000 行程式碼中，約會出現 25 個錯誤或漏洞。」 美國國家漏洞資料庫（NVD）所公布的「常見漏洞與曝險」（CVE）資料，有助於大眾了解目前已知的安全漏洞。這些更新十分重要，但只有在實際部署修補程式後，對組織才真正有幫助。 59

Apple 和 Google 在發現漏洞時，會提供相關資訊與對應的系統更新內容，說明哪些版本已修補漏洞。舉例來說，Apple 今年稍早針對 **CVE-2025-24201** 釋出 iOS 18.3.2，該漏洞可能讓經特殊設計的網頁內容突破 Web Content 沙盒的限制。**Google 則發布 Android 安全公告，** 說明已修補 43 個漏洞，其中包含兩個嚴重的零時差漏洞（Zero-Day Vulnerabilities）。

III. 即使平台安全，應用程式仍可能帶來風險

自 Apple App Store 與 Google Play 上線以來，這些平台就致力於保護使用者與企業的安全。Apple 使用者從 App Store 下載應用程式時，會受到多重保障，因為 Apple 會「**針對每個應用程式進行惡意軟體與其他可能影響使用者安全、隱私的檢查**」。Android 使用者則可透過 Google Play Protect 獲得保護。但這些防護仍無法完全阻止惡意攻擊者。 **過去五年內，Apple 已 阻止超過 90 億美元的潛在詐騙交易。 歐盟《數位市場法案》（DMA）** 允許建立替代的應用程式市集，並要求平台開放其「圍牆花園」。透過替代市集分發的應用程式，未必遵循 Apple App Store 的審核標準，因此可能對使用者的安全、隱私與整體風險帶來威脅。各種風險，包括社交工程（如釣魚）、勒索軟體、間諜軟體等，都可能透過下載應用程式或使用非官方支付系統的過程滲透到裝置中。

今年稍早，**Google 警告有一款新型的木馬病毒**，已針對超過 750 款合法的銀行與購物應用發動攻擊。目前，歐盟已強制這兩大應用程式平台允許使用者側載（sideload）應用程式，也因此擴大了攻擊面。

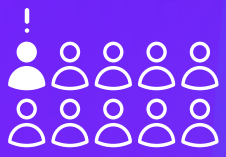
IV. 有針對性的攻擊使行動裝置面臨風險

行動裝置的彈性讓我們能夠在任何需要的地點工作；許多高階使用者經常透過行動裝置處理全球業務。但也因為這些裝置儲存大量敏感資料（如智慧財產、財務資料等），**高階使用者往往成為攻擊者的主要目標**。對於駭客來說，鎖定這些人是最有價值的勒索對象。

在過去 12 個月中，我們發現：

25%

的組織曾遭社交工程攻擊



1 in 10

使用者點擊了惡意釣魚連結。

I. 行動釣魚攻擊

釣魚攻擊（Phishing）是社交工程的一種，是目前對組織構成威脅最普遍且破壞性最強的方式之一。根據美國「資安與基礎建設安全局」（CISA）指出：「超過 90% 的成功網路攻擊都 **是從 釣魚電子郵件開始。**」

行動裝置上的釣魚攻擊來自多種管道。攻擊手法不再僅限於電子郵件，還包括 簡訊（稱為 smishing）、社群媒體或連結到偽裝網站。

但為什麼釣魚攻擊在行動裝置上更容易得逞呢？

首先，全球超過 **62% 的網頁瀏覽**都是透過行動裝置進行。這代表行動裝置已成為網路流量的主力，也讓攻擊者有更多潛在的目標與漏洞加以利用。

另一方面，行動裝置螢幕較小、介面簡潔，是其普及的原因之一，讓使用者更容易忽略攻擊跡象。這種裝置便於攜帶，也讓企業能夠將它納入各種流程，例如：

- 零售產業（POS 系統或庫存管理）
- 醫療產業（護理巡房或病床旁作業）
- 製造產業（設備操作或機械指令）
- 航空產業（例如電子飛行包或地勤使用的裝置）

但也正因為行動裝置帶來這些便利，使用者在面對惡意釣魚攻擊時更容易分心、掉以輕心。多數人仍認為行動裝置本身很安全，但正如我們在報告中說明的，只要點進一個連結，就足以讓整台裝置被入侵。

釣魚攻擊中最常被濫用的前 20 大品牌

行動裝置讓企業能導入新的工作流程、簡化與顧客的互動方式，並提升整體使用者體驗。 現在很多人都靠行動裝置工作——無論是當作輔助工具，還是處理公務的主要入口。行動裝置連結著我們的生活——無論是在職場還是在家中。攻擊者也深知這一點，並以此作為攻擊的切入點。

我們的研究發現，有些知名品牌經常被拿來當作社交工程攻擊的誘餌，用來騙取終端使用者在行動裝置上的信任。我們將這些品牌分為 **四大類**，這些類別是最常被拿來利用終端使用者 信任的手法。

使用行動裝置的原因很多，例如收工作信、網購生活用品、處理個人銀行業務，攻擊者正是針對這些常見且必要的使用情境，來設法取得資料存取權限。下方表格列出了在這四大類別中，最常被用來社交工程攻擊的前 20 大品牌。

1.	2.	3.	4.
娛樂	**商務**	**公用事務**	**個人用途**
Netflix	Outlook	美國郵政服務 (USPS)	Amazon.com Inc
Bet365	Office365	俄羅斯天然氣工業公司 (Gazprom)	Telegram
Steam	Allegro	AT&T Inc	Facebook, Inc
	InterActive Corp	Orange S.A.	Chase
	騰訊	DHL	WhatsApp
		BT Group	Yahoo, Inc.

由於這些品牌本身就非常知名、具公信力，對企業與個人都具影響力，因此經常被攻擊者拿來冒名使用。品牌的信任形象讓使用者更容易誤信那些看似安全、其實卻是惡意的內容。

這份清單僅列出的是過去一年最常被濫用的 20 個品牌，但實際上遠不止於此。攻擊者手法不停進化，仿冒的品牌也隨時可能改變。最終來說，這代表攻擊者可以如何利用品牌多年建立的信任來欺騙並剝削使用者。

在現代世界中，我們的個人資訊時刻處於風險之中。隨著行動裝置同時用於公私用途，攻擊者的滲透範圍也持續擴大。他們運用更進階的策略，利用逼真的介面、流暢的使用體驗與仿真的溝通語氣，來誘騙毫無戒心的受害者上鉤。但企業仍有辦法防範（例如持續對員工進行資安訓練、使用威脅防護工具），來保護使用者與資料的安全。

Jamf 在**一年內**共偵測到約 **1,000 萬次釣魚攻擊**，影響了我們樣本群中的 **140 萬台裝置**。

我們也發現其中約 **1.5–2%** 的攻擊會被歸類為**零時差攻擊（Zero Day）**，代表 攻擊者使用全新的、從未被發現過的釣魚網站來誘騙使用者點擊惡意連結。

辨識並驗證零日釣魚攻擊，有助於組織保護使用者免受全新且未被偵測的釣魚網站侵害。

資安長的觀點

- **導入完善的訓練計畫：**
  這是我們成功的關鍵之一。我們執行進階的釣魚模擬攻擊、進行遊戲化訓練、針對提出需求的使用者提供單次訓練，並全年無間斷地允許使用者回報釣魚郵件，並即時獲得確認與回饋。這對我們來說不只是每年一次的「做完就好」訓練。
- **掌握最新趨勢與攻擊手法：**
  這或許看似顯而易見，但攻擊者總會利用任何機會，往往包括新聞中出現的新事件、突破性技術或爭議性話題。你需要調整訓練內容與封鎖策略來因應這些情況。這可能會讓某些使用者感到不安，但透明度是關鍵。這項訓練的目的是讓學員做好準備，因為真正的攻擊者不會顧及你的感受，甚至會故意激起情緒反應，藉此讓受害者混亂、難以判斷。
- **採取多層防禦策略：**
  沒有單一方法或工具可以讓你完全避免成為針對性釣魚攻擊的受害者。你需要從多個角度來進行防護。 封鎖惡意網域。確保已實施多重驗證（MFA）。 採行零信任架構。啟用「不可能速度」這類異常登入偵測規則。採取一兩項防護措施可能還不夠，得透過多層安全防線，才是避免成為釣魚受害者的最有效方式。

II. 漏洞管理

所謂漏洞，指的是系統、應用程式或通訊協定中存在的弱點，可能會被攻擊者利用，進而影響其安全性、完整性或可用性。**Apple** 與 **Google** 都會公布影響其作業系統的已知漏洞清單。換句話說，這些漏洞在 Apple 或 Google 推出更新與安全修補之前，早就已經「流傳在外」。從 2024 年 1 月 1 日到 2025 年 4 月 1 日，Apple 共針對 iOS 各版本釋出 **29 次含 CVE 編號的安全更新**。同一期間，Android 系統也記錄了 **39 項系統漏洞**，並在 Android Security Bulletin 中標示 CVE 編號。

Apple（透過 **Rapid Security Responses**）與 Google（透過 **Android Security Patches**）會在主要版本更新之外另行發布獨立的安全修補。為什麼這些修補更新很重要？因為這些都是即時更新，組織可以直接套用，不必等到整個版本更新才獲得保護。

現代**資安威脅** 既多變又複雜，不論是一般使用者還是企業都必須提高警覺、及時更新裝置。不 只是單純更新裝置而已，更要確認該**更新** 是**真實有效的**。

Jamf Threat Labs 最近深入研究 了攻擊者如何維持對系統的持續存取權限這項手法。 他們的研究指出，「攻擊者可能會利用 iOS 的設定介面，篡改系統更新設定，甚至製造出更新提示與 通知，讓使用者以為有可用的 iOS 更新。」

我們接下來將深入看看 Apple 最近幾個版本中記錄的重要漏洞（本報告撰寫於 2025 年 4 月）。

Apple CVE 修補內容	日期	漏洞評分	衝擊
iOS 18.4.1 與 iPadOS 18.4.1	2025 年 4 月	CVSS 評分：7.5｜嚴重程度：高度（High）	CoreAudio
iOS 18.4 與 iPadOS 18.4	2025 年 4 月	CVE-2025-30430 CVSS 分數：9.8｜嚴重程度：危急（Critical）	Authentication Services
iOS 18.3 與 iPadOS 18.3	2025 年 1 月	CVE-2025-24085 CVSS – 分數：7.8｜嚴重性：高	CoreMedia
iOS 18.3 與 iPadOS 18.3	2025 年 1 月	CVE-2025-24154 CVSS 分數：9.1｜嚴重程度：危急（Critical）	WebContentFilter

更新的 AOSP* 版本	日期	漏洞評分	衝擊
13, 14, 15	2025 年 4 月	CVE-2025-26416 嚴重程度：危急（Critical）	權限提升（Escalation of Privileges）
15 間	2025 年 3 月	CVE-2025-22403 嚴重程度：危急（Critical）	遠端程式碼執行（Remote Code Execution）
15 間	2025 年 2 月	CVE-2025-0096 嚴重程度：高度（High）	權限提升（Escalation of Privileges）
12, 12L, 13, 14, 15	2025 年 1 月	CVE-2024-43771 嚴重程度：危急（Critical）	遠端程式碼執行（Remote Code Execution）

*Android Open Source Project（Android 開放原始碼計畫）

這些漏洞——全部都可在 Apple 與 Android 官方網站查詢——說明了開發軟體時難免會出現漏洞。對資安專業人員來說， 重點在於 能夠辨識並立即處理這些漏洞，才能保護資料安全。

其中最有效的方式之一，就是確保作業系統保持在最新狀態， 並 使用正確的工具來 推送更新。

透過最新作業系統維持良好的安全狀態

企業最佳的漏洞防範方法以及維持合規性的方式，就是持續更新其裝置的作業系統。如前頁所示，Apple 與 Android 都會定期釋出作業系統的漏洞修補更新。

組織最常透過行動裝置管理（MDM）方案來更新作業系統及員工日常使用的商業應用程式。 MDM 也能提供每台受管裝置的作業系統版本詳細清單。不過實際上，組織中經常有多種用途的裝置，運行著不同應用程式、提供給不同的使用者使用。讓整個裝置環境都同步在最新版本作業系統上並不容易（例如，還要先測試應用程式才能部署），也往往不太實際。

在過去十二個月內：

32%

的組織至少有一台裝置存在重大漏洞。

55.1%[6]

的工作用行動裝置
執行的是有漏洞的作業系統

有些組織使用的行動裝置並未安裝最新安全修補。我們的資料顯示，有 **4.8%** 的 Android 裝置存在漏洞，卻仍被用來存取公司資源。

行動辦公讓我們可以用自己習慣的方式工作從開車接電話到強化第一線與客戶互動員工的工作流程，行動裝置為工作帶來更多可能。但如同所有電腦裝置，這些系統也會成為攻擊者的目標。組織可以透過合適的工具，在不犧牲使用體驗的情況下平衡安全性，並結合員工訓練與對現今常見威脅的理解，來降低整體裝置的風險 。

資安長的觀點

- **確保你能掌握整個組織的漏洞狀況：**
  盡可能瞭解終端使用者裝置或基礎架構中存在的漏洞，是一個絕佳的起點。你可以從這些資料出發，分析特定應用程式的影響範圍、潛在風險等。這是以資料導向方式為漏洞設定優先處理順序的好方法。
- **導入完善的修補計畫：**
  回到前述的 MDM 重點，擁有一套能協助維持軟體或作業系統在最新或支援的 N-X 版本的工具，對於維持穩定安全的環境是十分重要的。若能在幾乎不影響終端使用者的情況下做到這點，也能更順利地支援業務運作。
- **導入風險為本的存取機制：**
  若有不符規範的裝置嘗試存取公司資源，應限制其存取，直到終端使用者修正問題，讓裝置盡可能輕鬆地恢復合規狀態。

III. App 風險

2024 年 11 月底，資安機構發布 了 **2023 年最常被利用的漏洞報告**。（這是這份報告的最新版本。）本報告深入探討前 15 個漏洞，包括攻擊者可藉此造成的傷害之相關細節。這些漏洞存在於多種運算平台的作業系統與應用程式中，是組織員工與學生日常使用的工具。如報告指出：「2023 年，惡意網路攻擊者利用的零日漏洞數量高於 2022 年，讓他們得以入侵企業網路並攻擊高價值目標。」該資安機構也進一步提供開發人員與終端使用者組織可採取的漏洞緩解措施。對於終端使用者組織，本報告建議：

- 及時更新軟體、作業系統、應用程式與韌體
- 定期執行自動資產盤點
- 實施健全的修補管理流程
- 建立並記錄安全基準設定
- 定期進行系統備份，確保安全
- 維護最新的資安事件應變 計畫

什麼樣的 App 被認定為「高風險」？ 高風險 App 的幾項常見特徵包括：

- 異常行為特徵
- 惡意程式碼與可疑行為
- 危險的權限要求
- 具有風險的動態行為
- 可疑的開發者資料

掌握應用程式版本、是否有資料外洩風險等資訊，有助於組織搶在風險發生前調查並即時處理。

企業了解自身應用程式的整體安全狀況是非常重要的。以下是組織在辨識與處理高風險應用程式時應關注的幾個關鍵資料點：

- 安裝了過時版本應用程式的使用者數量
- 使用特定應用程式版本的使用者數量
- 使用已知加密機制有漏洞的應用程式清單，這些漏洞可能導致敏感資料在未受保護的網路中外洩
- 申請某些權限以存取裝置中其他部分資料的應用程式

深入解析一個真實漏洞：繞過 Transparency, Consent and Control（TCC）機制

在 Apple 各作業系統中，TCC 是一套關鍵的安全機制，用來要求使用者同意或拒絕應用程式存取如照片、聯絡人、位置等敏感資料的請求。繞過 TCC 的漏洞指的是這些控制機制失效，導致應用程式可以在未經使用者同意的情況下存取私密資料。這表示攻擊者可以在不通知使用者的情況下，取得檔案、資料夾、健康資料、 麥克風與鏡頭等資訊的未授權存取權限。

Jamf Threat Labs 發現了 CVE-2024-44131，一項影響 Mac 裝置中 File Provider 的 TCC 繞過漏洞。Apple 在 iOS 18.0 中迅速修補了這項漏洞。CVE（如 CVE-2024-44131）提醒我們：也要說明了保持組織裝置隨時更新相當重要。

App Store 的保護機制與詐騙防範

正如前文所述，在過去五年內，Apple 阻止了超過 90 億美元的詐騙交易。僅在 2024 年，Apple 就攔截了超過 20 億美元的詐騙交易。再進一步來說，Apple 在 2024 年：

- 終止了超過 14.6 萬個涉入詐騙問題的開發者帳號
- 拒絕了另外 13.9 萬個開發者註冊申請
- 駁回了超過 4.3 萬個含有隱藏或未說明功能的應用程式提交
- 拒絕了超過 32 萬個重複他人應用、垃圾內容，或可能誤導使用者的應用程式提交
- 偵測並封鎖了超過 1 萬個在盜版應用平台上流通的非法應用程式

App Store 一直被視為下載應用程式最安全、最符合使用者隱私且使用體驗最佳的管道。iOS 的 App Store 採用沙箱機制、使用者授權請求，並僅允許經簽署的程式碼在裝置上執行。但如數據資料所示，惡意攻擊與詐騙仍層出不窮。自 2008 年起，Apple 一直致力於打造一個安全、值得信賴的 App Store 環境，保護使用者與開發者。 然而，「側載應用程式」（來自第三方 App Store，如 AltStore）就無法享有這些保護。

資安長的觀點

有效的行動裝置安全需要層層防護策略。即便使用最新硬體與作業系統，仍不足以完全防禦針對組織與敏感資料的攻擊。良好的資安實踐應涵蓋整個技術堆疊，包括應用程式在內。

- **針對關鍵行動應用導入審核機制：**
  從最關鍵的應用程式開始，定期確認組織中是否皆使用最新、安全版本。隨著規模擴大，擴充審核範圍至所有進入企業 App Store 的應用程式。
- **建立政策，當裝置安裝不被允許的應用程式時，標記為「不符規範」**，並限制其存取 SaaS 應用、資料中心或遠端工作負載，直到這些應用被更新或移除。
- **將行動應用程式安全納入教育訓練，** 讓使用者能主動在日常工作使用的裝置上執行必要更新，成為資安防線的一部分。
- **若組織沒有使用替代的 App Marketplaces 的需求**，應制定政策，防止員工裝置連線至這些平台。同時，也應防堵側載應用，確保裝置只使用官方來源的應用程式。

Jamf Threat Labs 團隊展示了一個側載的社群媒體應用程式如何 監控照片並上傳至攻擊者伺服器的案例。這款應用程式「已被修改，但功能完全正常」。該團隊也提出了一些明確的安全建議，包括：

- 啟用並定期檢視 App 隱私報告
- 慎選應用程式權限
- 避免在裝置中儲存敏感資訊

僅從可信來源（例如 App Store）下載應用程式

原生應用程式與雲端託管的網頁應用程式都存在風險。
雲端應用因為攻擊面更大，風險也更高。但只要具備正確的能見度、控制力與應變能力，組織仍可有效降低應用程式風險。

IV. 鎖定攻擊與進階間諜軟體威脅

自 2021 年起，**Apple 已向**超過 150 個國家的使用者發出威脅通知。這些通知用來警示高風險對象，如記者、政治人物、外交人員等，遭受僱傭間諜軟體攻擊的風險。 2025 年 4 月下旬，Apple 表示「本週已向多名疑似遭政府間諜軟體鎖定的使用者發出通知」。但這類攻擊並不只針對 Apple。這些攻擊會鎖定各種作業系統與應用程式。**根據The Citizen Lab，**「這些間諜軟體會被植入 WhatsApp 和其他 Android 裝置上的應用程式中。」

Apple 發送威脅通知所揭露的惡意程式與間諜軟體，是目前組織與個人所面臨的最嚴重威脅之一。不過，仍有方法能保護組織內各層級的使用者免於這些威脅。

Apple 提供了使用者防範惡意軟體的建議，其中有大部分已在本報告中說明。具體來說，Apple 建議使用者：

- 更新裝置至最新版本，取得最新的安全修補
- 為裝置設定密碼
- 啟用雙重驗證並為 Apple ID 設置高強度密碼
- 僅從 App Store 安裝應用程式
- 在線上使用高強度的密碼
- 不要點擊來自不明發件人的連結或附件

Jamf Threat Labs： 裝置在使用者毫不知情的情況下被入侵

Jamf Threat Labs 展示 了一台未安裝防護軟體的裝置如何被悄悄入侵。這個展示顯示攻擊者能夠取得電子郵件、公司通訊、雙重驗證與其他個人資料。團隊接著說明組織可如何保護企業與個人資料：

1. 強制執行安全設定，確保公司裝置與自攜裝置符合合規要求
2. 啟用威脅預防與偵測，並採取行動，同時維護終端使用者隱私
3. 對所有受管裝置強制啟用裝置加密

資安長的觀點

與其他主要運算裝置相比，惡意軟體在行動裝置上的普及率較低。
但一旦出現，通常都採用高度進階的技術，並 會針對特定個人發動攻擊。

- **千萬不要掉以輕心，** 以為行動惡意軟體不會影響你的組織。僅去年，Apple 就向約 100 個國家的使用者發出間諜軟體入侵通知。
- **最起碼，應任命一位行動資安負責人**，定期彙報組織行動部署的整體狀況。統整手機遺失、目標型釣魚、效能下降與其他可疑異常的事件紀錄。理想狀況下，應該將裝置管理與安全工具的遙測資料串接起來，並整合進你的安全營運中心。把行動裝置視為與其他端點同等重要的資安對象。
- **在可行的情況下，收集行動系統資料，尋找零日攻擊的跡象。**這需要具備專業知識，不論是內部或委外皆可。若是大型企業具備專職資安分析師，建議培養團隊具備行動鑑識專長。

總結

行動釣魚 是攻擊者取得敏感資料最常見的手法之一。能夠導入訓練計畫、掌握趨勢與手法（包含隨時調整訓練內容），並實施多層資安防護的組織，能從各個面向提升防禦力。

各種類型的軟體都有可能出現漏洞。 建立良好的資安習慣，有助於降低漏洞所帶來的風險。定期更新作業系統與停用不必要的控制項（例如：第三方應用程式商店），可協助組織符合內部基準與外部標準框架。

應用程式管理不當或使用不當都會帶來風險。問題不一定出在應用程式本身，也可能是應用程式與惡意網路的連線行為。建立企業級應用程式商店並持續審查應用程式（尤其是私有或自訂應用程式），可讓組織更有效地監控、修復並修補存在漏洞的應用程式。

進階持續性威脅（APT）與間諜軟體攻擊變得越來越普遍。這些威脅（通常來自國家級或特殊組織）影響全球的組織，常常鎖定擁有敏感資料的重要人士。透過落實深層防禦策略，並將行動裝置視為其他裝置一樣重要，組織才能全面保護行動生態系與所連接的資料資源。

建立並維護企業擁有裝置的可接受使用政策，要求符合使用規範，並確保其存取公司資源或遵守組織政策。對於自攜裝置（BYOD），則需施加額外的隱私控制，例如 **Apple 裝置所提供的隱私保護機制**。

jamf

歡迎聯絡我們，深入了解行動威脅環境。