【Zero Trust X 身分驗證】

整合 OTP 與生物辨識的郵件安全新戰略

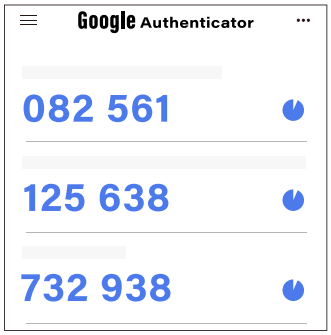
當企業資訊安全面對日益複雜的威脅環境，「Zero Trust」（零信任）成為核心防線的設計原則。若郵件系統只仰賴傳統的帳號密碼登入機制，遠遠不足以保障企業郵件溝通的完整性與保密性，根本防不了釣魚信、假冒信與帳號盜用。因此，ShareTech 推出結合雙重驗證的解決方案，讓企業郵件系統落實真正的 Zero Trust 登入安全，並進一步取消管理者預設帳號（admin）登入，避免成為低防護缺口。

問題：帳密外洩頻傳，信任機制不再安全

電子郵件是企業內外溝通的核心，同時也是駭客最愛入侵的管道。無論是內部員工重複使用弱密碼、或是使用者誤點釣魚信件導致帳密外洩，一旦郵件帳號被盜取，可能造成商業機密洩露、業務誤發指令，甚至導致金錢損失。這類風險無法僅靠使用者教育解決，企業需要從技術層面加強身份驗證，建立「零信任」的郵件存取機制。

解決方案：雙重驗證機制導入 Zero Trust

ShareTech 提出結合雙重驗證（2FA）的郵件強化方案，透過兩種機制，讓使用者的身份多一層確認，阻擋帳號被盜風險：



- Google Authenticator — OTP 驗證

  在 Zero Trust 架構下，且 AI 工具持續進步的時空下，僅憑帳號與密碼的驗證方式非常危險。為此，ShareTech 支援整合 Google Authenticator 作為 OTP（一次性密碼）驗證機制，提供使用者與管理者雙層保障。

台中總公司 04-2705-0888
台中市西屯區西屯路二段 256 巷 6 號 3F-6

台北分公司 02-2501-1185
台北市中山區松江路 129 號 6F-2

高雄分公司 07-229-8788
高雄市新興區民權一路 251 號 7F-5

免付費專線 0800-666-188

官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

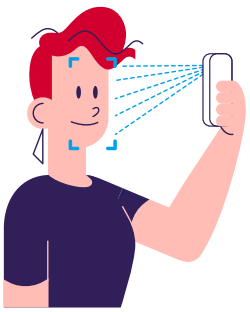
【Zero Trust X 身分驗證】整合 OTP 與生物辨識的郵件安全新戰略

不論是一般使用者登入 Webmail 信箱，或是系統管理者登入郵件管理後台介面，皆可搭配 Google Authenticator 啟用二階段驗證，於登入時提供一組即時變動的六位數 OTP 驗證碼。使用者僅需透過手機上的 Google Authenticator App 掃描 QR Code 綁定帳號，即可在後續登入時產生一次性的專屬驗證碼。

這樣的設計不僅降低帳號被暴力破解或社交工程入侵的風險，也進一步防止內部權限被濫用。對管理者而言，更能透過後台設定強制啟用 OTP，全面落實企業郵件帳號的身分驗證控管。

- ShareTech Authenticator — 生物辨識驗證

為進一步強化身份驗證安全與使用者體驗，ShareTech 提供自家研發的生物辨識登入，目前已應用於信箱登入場景。使用者可選擇以指紋辨識或臉部辨識作為驗證方式，有效避免帳號遭冒用或密碼洩漏所造成的風險。



當使用者透過 ShareTech Authenticator 完成裝置綁定後，僅需輸入帳號（無需密碼），即可直接透過指紋或臉部進行身分驗證，快速且安全地登入個人信箱。不僅提升使用便利性，更實現「人機一體」的身分安全防線。此功能特別適用於對資訊安全要求較高的角色，如主管、財務、法務等人員，甚至可推廣至全體員工，打造無縫的信箱保護機制。

未來 ShareTech 也將持續擴展生物辨識技術的應用，推進至郵件管理介面，實踐更全面的 Zero Trust 登入控管。

總結：從「帳號密碼」邁向「身分信任」

Zero Trust 並非一種技術，而是一種策略思維。在郵件系統上落實 Zero Trust，第一步就是確保「驗證每一次登入的身分」，而非預設信任。透過導入 Google Authenticator 的 OTP 驗證，搭配 ShareTech 的生物辨識登入機制，並淘汰容易被鎖定的預設管理者帳號，企業不僅能提升郵件的安全性，更能讓身分驗證流程更加順暢與智慧。從帳密管理進化到動態、多元的驗證模式，企業才能真正邁向高防護、低風險的郵件環境。

ShareTech 將持續陪伴企業打造更可信、更安全的郵件通訊未來。欲了解更多資訊，歡迎聯繫我們：

sales@sharetech.com.tw

www.sharetech.com.tw