增強式驗證如何協助阻擋網路釣魚攻擊

安全金鑰和 Zero Trust 方法可以遏止網路釣魚者

網路釣魚所造成的威脅

資料遺失、網路遭入侵、帳戶遭竊

針對性網路釣魚攻擊是組織現今面臨的最危險威脅手段之一。網路釣魚和社交工程攻擊的目標是操縱人們，使其交出敏感的資訊或存取權。登入憑證是常見的目標。

這種性質的攻擊如果成功，可能會導致以下情況：

- 帳戶盜用
- 連往更大型供應鏈攻擊的連結
- PII 和 IP 等資料滲漏
- 勒索軟體等惡意軟體攻擊

幸運的是，有一些極為有效的解決方案可以降低網路釣魚的風險。其中一種最重要的解決方案是多重要素驗證 (MFA)。

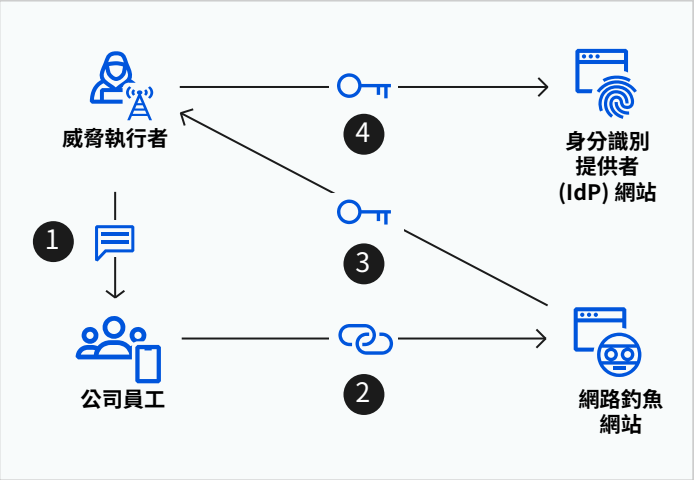


圖 1：簡訊網路釣魚攻擊的剖析。1. 傳送看似合法的簡訊。2. 連結至看似合法的網站。3. 即時轉送受害者的憑證與限時單次密碼。4. 登入真正的公司 IdP 網站。

多重要素驗證 (MFA) 如何協助阻擋網路釣魚

MFA 抵禦密碼竊取

除了在登入時輸入使用者名稱和密碼以外，MFA 還要求使用者出示金鑰。如果沒有該金鑰，使用者就無法存取其帳戶，攻擊者也一樣。

使用軟式金鑰的 MFA

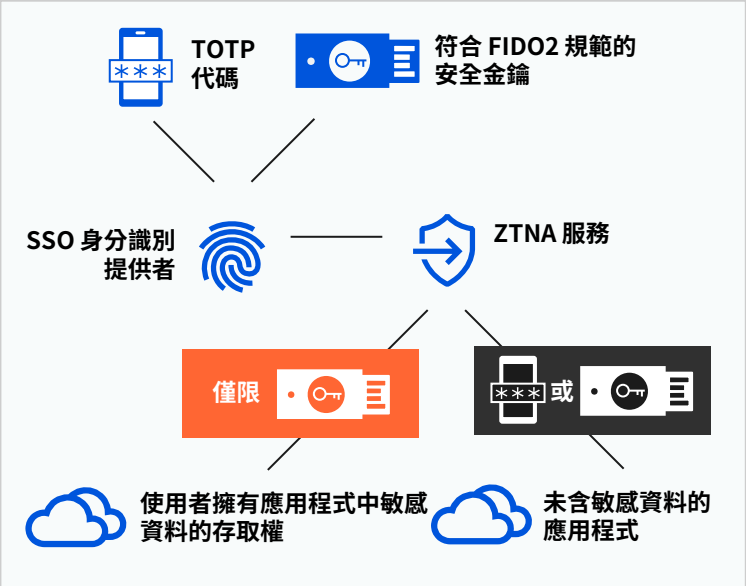
常見的 MFA 實作是使用限時單次密碼 (TOTP) 等軟式金鑰。TOTP 經常是透過簡訊、電子郵件或應用程式發出。雖然軟式金鑰比單一要素驗證更安全，但仍可能會遭到攻擊者攔截。

使用安全金鑰的 MFA

符合 FIDO2 規範的安全金鑰一旦發出，攻擊者就無法攔截，也幾乎無法在沒有實體存取的方式竊取。Google 的研究發現，使用符合 FIDO2/U2F 規範的安全金鑰阻擋了 100% 的帳戶接管嘗試。[1]

選擇性強制採用增強式驗證

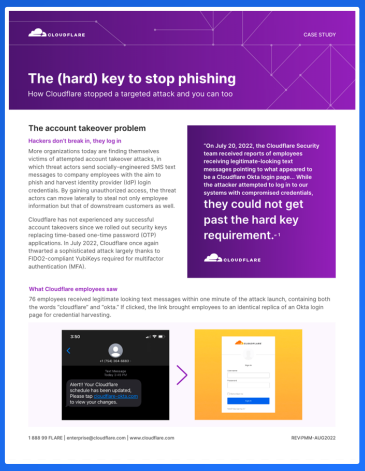
有些 IAM 解決方案可能會支援增強式驗證，但可能不允許管理員實際要求。透過 ZTNA，您可以確保要求進行 FIDO2 驗證，尤其是針對含有敏感資料的應用程式。Cloudflare 會在每次驗證時要求安全金鑰 MFA，因此大大強化了我們的安全狀態。



「在 2022 年 7 月 20 日，Cloudflare 安全性團隊接獲多次報告，說明員工收到似乎是指向 Cloudflare Okta 登入頁面且看似合法的簡訊；雖然攻擊者試圖利用外洩的憑證登入我們的系統，

但他們無法通過硬體金鑰要求。」[2]

CLOUDFLARE



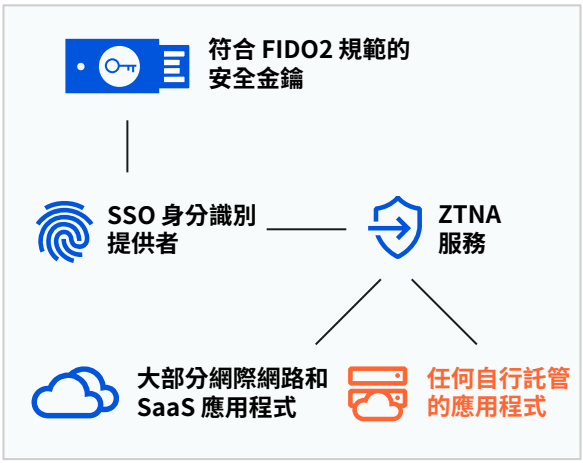
在所有地方推出增強式驗證

適用於您所有應用程式且符合 FIDO2 規範的 MFA

可透過多種傳統方式對雲端服務強制採用 MFA，在使用單一登入 (SSO) 服務時尤其如此。但是，舊式或非 Web 應用程式可能難以適用，因為其中有許多並非原生支援這種驗證。

透過 ZTNA 簡化實行

Zero Trust 網路存取 (ZTNA) 能夠在您所有的資源中擔任彙總層級，並分別為其啟用嚴格的驗證原則。SaaS、自行託管和非 Web 應用程式等都可以設置在 ZTNA 後方，以便更容易在所有應用程式間強制採用增強式驗證。



組織實作增強式驗證的關鍵要點

1

集中進行 IAM

將身分識別與存取管理 (IAM) 集中進行，以便更容易在所有應用程式間實作 MFA。

2

選擇性強制採用 MFA

依據身分識別與內容，建立選擇性強制採用 MFA 選項（TOTP 和 FIDO2，或僅限 FIDO2）。

3

支援行動裝置

針對筆記型電腦、桌上型電腦、伺服器和行動裝置等，核發 FIDO2 解決方案。

加速您的 Zero Trust 藍圖

申請架構研討會

還沒準備好進行評估嗎？

申請免費試用。

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. 2022 年 8 月 9 日 Cloudflare 部落格文章「複雜網路釣魚詐騙的機制，以及我們的阻止方式」(The mechanics of a sophisticated phishing scam and how we stopped it)：blog.cloudflare.com/2022-07-sms-phishing-attacks/