# 「國際間鼓勵非公務機關採用雙因子驗證機制Two-Factor Authentication (2FA)趨勢」專案報告

# 一、背景

近年新聞媒體頻繁揭露因駭客攻擊導致發生個資外洩事件，而外洩之個資如遭有心人惡意利用，將伴隨詐騙及勒索等犯罪行為，對國人財產造成嚴重損失。近期本籌備處彙整列管之個資外洩事件根因調查結果，發覺以駭客偽冒使用者身分，侵入系統竊取使用者個資之樣態為最大宗，且常見手法為「撞庫攻擊」。

「撞庫攻擊」係網路駭客自其他系統平臺，或由現實生活中取得當事人的帳號密碼組合，利用民眾使用共通密碼的習慣，嘗試登入不同的網站或服務，只要當事人剛好使用相同帳號密碼組合，則駭客就可輕易登入，並進而取得當事人在網站或服務中所留存之個資。

# 二、撞庫攻擊案例

- **全統運動之報名網：112年3月底接獲民眾反應疑似有個資外流情形，全統運動公司檢查報名主機、資料庫登入狀況無異常，但監控網站流量有多組境外IP嘗試暴力攻擊均被防火牆阻擋。**

- **台灣之星(現併入台灣大哥大)會員網：112年10月下旬，有3個IP曾嘗試以大量門號（含非台灣之星門號）登入原台灣之星官網（總次數逾293萬次)，且有同一門號多次以不同IP、密碼或不同時間嘗試進行登入，而當登入成功後即開始測試下一組帳號密碼，持續此異常的使用行為。**

- **台灣高速鐵路會員系統：113年9月發現有心人士透過於其他平臺或管道非法取得民眾個資(取得個資之來源不明)，並於利用個資成功登入高鐵會員系統後，進行點數兌換商品券牟利。**

# 三、防範撞庫攻擊之常見作法

| 防範作法 | 提高系統密碼設置之複雜度 | 採取雙因子驗證方式驗證登入身分 | 限定特定 IP 對系統進行存取 |
|---|---|---|---|
| 優點 | Ø 不用額外花費成本<br>Ø 可適用於會員/用戶數較多之系統 | Ø 較未造成會員/用戶過多負擔<br>Ø 可適用於會員/用戶數較多之系統 | Ø 不用額外花費成本<br>Ø 較未造成會員/用戶過多負擔 |
| 缺點 | 造成會員/　用戶記憶密碼難度 | 需花費驗證成本[註] | 無法適用於會員/用戶數較多之系統 |

**評估上述作法，在考量不過度造成用戶困擾且適用性廣泛之前提下，「採取雙因子驗證方式驗證登入身分」之作法較適合推廣！**

註：
- 成本需視機關規模及使用技術如APP、簡訊、OTP、FIDO等，另如Google、微軟亦有提出相關的驗證方案。
- 例如：採電子郵件OTP認證，可整併於網站改版或維護時加入該機制，或併於程式開發節省成本。

# 四、雙因子驗證(2FA)概述

驗證是存取控制的重要關鍵，用於確認某人是其所聲稱的身分；驗證因子則是不同類別的身分驗證方法，目前主要的身份驗證因子種類有：

| | |
|---|---|
| 知識因素(Something you know) | ，如使用者名稱、密碼 |
| 持有因素(Something you have) | ，如獨立的裝置、身分證、提款卡 |
| 生物因素(Something you are) | ，如臉部辨識、指紋、聲紋 |

## 雙因子驗證 (Two-Factor Authentication, 2FA)

- 要求使用者透過**2種認證因子**確認存取身分的認證機制，通過才會被授予存取權限，為多因子驗證 (Multi-Factor Authentication, MFA) 概念的一種。
- 請注意，使用單一類型因子進行兩次認證的機制(例如輸入使用者名稱和密碼這2項知識資訊)並不構成雙因子驗證。

# 五、國際間推動趨勢及非公務機關應用情形(1/3)

| | |
|---|---|
| 美國國家標準暨技術研究院(NIST) | • MFA是重要的安全增強功能 |
| 歐盟網路安全局(ENISA) | • 應優先使用2FA存取處理個人資料的系統 |
| 英國國家網路安全中心(NCSC) | • 鼓勵企業為線上服務提供MFA |
| 新加坡個人資料保護委員會(PDPC) | • 鼓勵使用2FA保護敏感個人資料帳戶的存取 |

# 五、國際間推動趨勢及非公務機關應用情形(2/3)

| | |
|---|---|
| 紐西蘭電腦網路危機處理小組(CERT) | • Two Steps, Too Easy |
| 紐西蘭官方隱私專員辦公室(OPC) | • 「對於以數位方式持有或分享個人資訊的小型企業或組織來說，雙因子驗證是期望的最低要求。如被發現存在與網路相關的隱私洩露行為，且沒有至少兩個因素的身份驗證，那麼可能會被發現違反了《隱私法》。」 |

# 五、國際間推動趨勢及非公務機關應用情形(3/3)

**雙因子驗證(2FA)或多因子驗證(MFA)在各行業中扮演著越來越重要的保護角色：**

- 科技產業
  - Google：2025年起將強制Google Cloud用戶採用MFA
  - 微軟：2024年7月起強制Azure用戶啟用MFA
  - Meta：針對具敏感身分的臉書用戶帳號，強制啟用2FA
  - Apple： 2FA能為「Apple 帳號」提供多一層安全保護
  - LINE：於2024年9月3日更新LINE Business ID的登入方式，初始設定中將2FA由預設關閉變更為預設開啟。
- 金融電信業：「環球銀行金融電信協會」(SWIFT) 推動MFA機制以強化帳號密碼管理，減少詐騙行為的發生。
- PayPal：全球最大線上支付平台之一，提供多種2FA方式，包括手機簡訊。
- 線上訂房平台Booking.com ：鼓勵使用者開啓帳戶的2FA，為帳戶安全增添保護。
- 全球知名的程式碼共享與版本協作平臺GitHub：要求使用者必須啟用2FA。

# 六、結語

雙因子驗證(2FA)已經成為國際上推動資訊安全的重要作法之一，其優勢包括：

- 提升系統安全性
- 符合法規的安全要求
- 提升用戶信任
- 降低風險成本

從相關研究、案例和產業經驗來看，2FA是一種重要的個資安全維護措施，除增加駭客入侵的難度，也有助降低資料外洩風險，保護用戶的敏感資訊。因此，推廣非公務機關積極採用2FA措施，以保障資訊及個人資料安全。