公務機密維護宣導

社交工程手法再升級：結合雲端服務與短期憑證規避防禦

近期駭客組織持續升級社交工程與釣魚攻擊手法，此次攻擊採取進階化策略，反覆寄送偽冒的 Microsoft 系統通知，企圖製造緊迫氛圍，利用收件人對官方通知的信任與時間壓力，誘使收件人在未充分確認下點擊惡意連結提供帳號密碼，造成帳戶被未授權存取與敏感資料外洩。TWCERT/CC 提醒企業與民眾保持高度警覺，特別是在收到疑似來自官方電子郵件時，應格外謹慎，以避免成為攻擊目標，相關防護措施建議如下：

一、建議留意可疑電子郵件，注意郵件來源正確性，不點擊不明的網址或連結，進入可疑網站不輸入個資、帳號密碼及金融資訊。

二、建議定期更換符合複雜性需求之密碼，並啟用多因子認證(MFA)，以提高安全防護措施。

三、網路管理人員應參考最新受駭偵測指標，確實實施預防性阻擋措施，以攔截並過濾可疑郵件。

四、加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。

資料來源：台灣電腦網路危機處理暨協調中心全球資訊網站