強化帳密安全

守護數位安全的第一道防線

數位發展部資通安全署

Agenda

1. 威脅現況
2. 真實案例
3. 強化帳密安全
4. 帳密安全懶人包

威脅現況

為何帳密安全如此重要?

113年資安威脅類型

>37% **入侵攻擊及入侵嘗試**

試圖透過暴力破解或利用已知與未知漏洞等攻擊手法，取得系統服務資源與權限

> **暴力破解**
> 駭客經由**反覆測試不同組合來找出正確的密碼**，只要有足夠的時間和電腦運算資源，就可以不斷重複嘗試，直到找到匹配的密碼。

帳密安全

是抵禦網路威脅的

第一道防線

如同提款卡與密碼一旦落入他人手中，數位資產將毫無保障

來源：113年度國家資通安全情勢報告

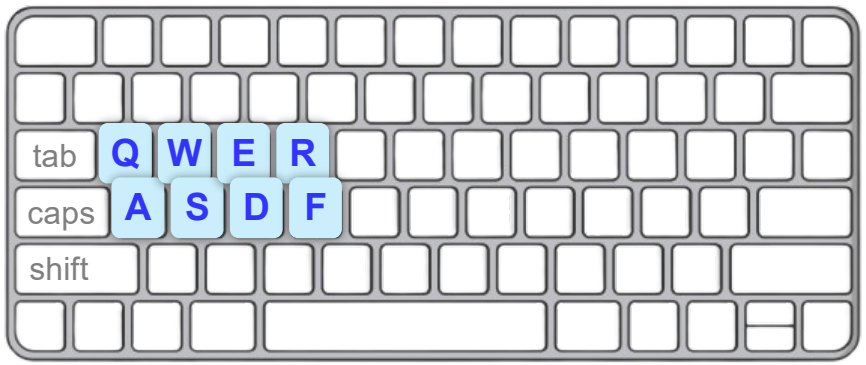
真實案例

真實案例1： 帳密安全性不足的代價

弱密碼造成
系統被入侵

弱密碼就是易於猜測的密碼

1. 使用太簡單、太短的密碼
2. 使用個人資訊，如電話、生日、身分證字號等



案例

某機關內部設備對外連線異常，原因為未檢視防火牆政策，並**以常見鍵盤排序設定密碼**，導致遭暴力破解並植入惡意程式

真實案例2：帳密安全性不足的真實代價(1/2)

撞庫攻擊

竊賊取得一串偷來的鑰匙，不破壞門鎖，而是逐戶嘗試，直到找到能直接打開的那一扇門

情境說明

真實案例2：帳密安全性不足的代價(2/2)

攻擊手法

使用者如於不同網站都使用相同的密碼，駭客便有機會以非法取得的帳號密碼，嘗試登入各項服務或網站(如銀行、郵箱、社群)，並將全數破解

案例

某公司發現部分會員帳戶遭盜用兌換，經警調單位追查，發現駭客購買大量外洩帳密後，採**撞庫攻擊**登入盜用點數兌換商品券，購買商品後變賣牟利

真實案例3：帳密安全性不足的代價

社交工程手法

案例

某機關FB遭駭客上傳不當影片，調查發現FB管理者為離職員工私人帳號，因該員工**誤點社交工程郵件**，導致管理者帳號密碼被盜用，FB私訊對話曾留存民眾報名資料，恐有個資外洩疑慮

強化帳密安全

強化帳密安全1： 使用強密碼

1 增加密碼長度及複雜度

- 至少包含15個字元(越長越好)
- 使用大小寫英文、數字或特殊符號組合

2 跨服務使用不同密碼

- 避免在不同網站使用相同的帳密
- 使用密碼管理工具產生獨特密碼

Pc29_hJ/EfuZ*3ao

3 密碼組合原則

- 不要使用生日、姓名、電話等易被猜測的資訊
- 運用4到7個無關聯的單字組成

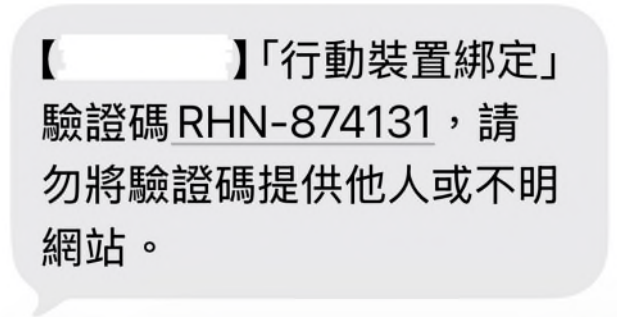
Correct-Horse-Battery-Staple

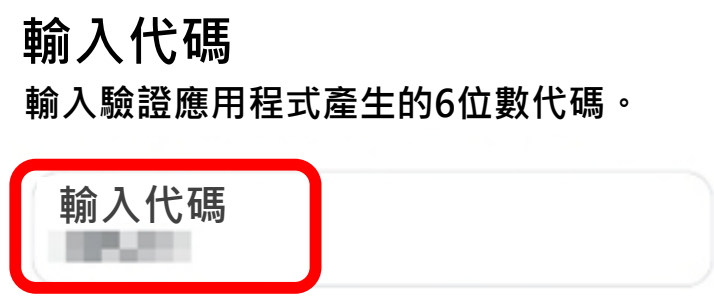
來源：美國網路安全暨基礎設施安全局 CISA

強化帳密安全2：啟用兩步驟驗證

了解兩步驟運作原理

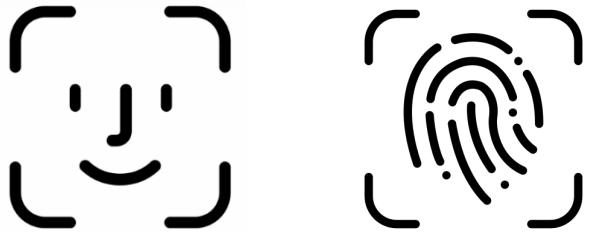
除了密碼外，額外要求**第二道驗證**
如手機簡訊、驗證代碼、生物辨識





優先啟用重要服務

建議先為Gmail、Facebook、Line
、網路銀行等**關鍵帳號**啟用兩步驟

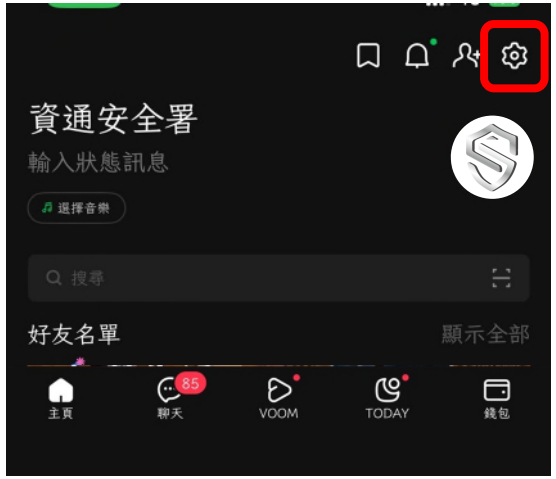


※各大服務平台（Google、Facebook、Line）皆提供詳細的兩步驟啟用步驟說明，請至官方網站「帳號安全」設定頁面查看

LINE 啟用兩步驟驗證

設定方法

1.主頁>設定



2.點擊我的帳號

3.啟用雙重認證

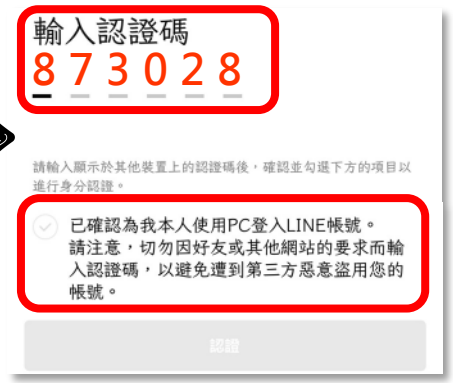
確認設定

1.非手機裝置登入

2.手機彈跳訊息

3.非手機裝置顯示驗證碼

4.手機輸入驗證碼



GOOGLE 啟用兩步驟驗證

設定方法

1.管理帳戶

2.安全性登入

3.兩步驟驗證

4.啟用驗證

確認設定

1.非手機裝置登入

2.手機確認登入資訊

強化帳密安全3：定期檢視及監控帳戶活動

定期檢視登入活動

每月至少檢查1次帳號的登入紀錄，確認是否有不明的登入行為

注意異常登入地點

如發現來自陌生國家或城市的登入紀錄，請立即變更密碼，並啟用兩步驟驗證

登入通知

異常登入（非常用裝置、地點）通知功能，第一時間掌握帳號使用狀況

4

帳密安全懶人包

懶人包

ACTION

保護個人隱私與財產

信賴資安　守護臺灣

數位發展部資通安全署
Administration for Cyber Security, moda