

# OUCH!

## 本期話題

- 密碼
- 什麼是雙因子認證
- 雙因子認證如何運作

## 鎖定登入

### 概述

證明身份的驗證程序，是保護個人網路資料的主要關鍵，如電子郵件、社群媒體或網路銀行帳號。大家或許沒有意識到，有三種不同方式可以證明您是誰：已知的資訊（如密碼）；已擁有的東西（如駕照）；及身體的某些特徵（如指紋）。每一種方法都有各自的優

缺點。目前最普遍的驗證方式是利用您已知的資訊——密碼。不幸的是，僅使用密碼已被證實越來越不安全。

在本期文章中，將教您如何保護自己，並使用相較於僅以密碼登入更好的方式來鎖定登入，也就是所謂的雙因子認證。

### 客座編輯

Tiffany Schoenike在國家網路安全聯盟中 (@staysafeonline) 擔任倡議活動的主管。2016年，Schoenike與白宮、政府及企業一起合作，在STOP.THINK.CONNECT.™推廣活動中提出有關雙因子認證的「鎖定登入」機制。

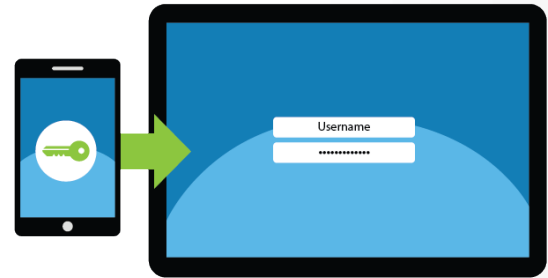
### 密碼已經不夠看

密碼認證是依據您所知道的資訊來證明自己的身份，不過，假如有人能猜到或獲取您的密碼，那麼他們就能偽裝成您且存取帳號裡所有資料。強度不足的密碼是帳號被駭客入侵的主要原因之一，因此會建議使用不容易被他人猜測出來的密碼短語，另外每個帳號請使用不同的密碼，而且絕不告知其他人。雖然以上方法仍建議採行，但僅靠密碼事實上已不足以保護帳號安全。幸運的是，有一種簡單且快速的方法讓您能管控並使個人資料更安全，即是所謂的雙因子認證。

## 鎖定登入

## 什麼是雙因子認證？

雙因子認證（也稱為兩階段驗證，多因子認證，或 2FA）遠比只使用密碼來得安全。它利用兩種不同的方法來證明身份。金融卡是一個很好的例子：當您在自動提款機（ATM）提款時，實際上就是在使用雙因子認證。您需要金融卡（已擁有的東西）和金融卡密碼（已知的資訊）這兩樣東西才能提領現金。即使金融卡不慎遺失或被竊取了，在不知道金融卡密碼的情況下，其他人仍然無法提領現金。小偷必須同時擁有您的金融卡及金融卡密碼才能提款。這就是雙因子認證的概念。



無論何時盡可能地使用雙因子認證來鎖定登入，這是您可以採取的最強網路安全自保方法之一。

## 雙因子認證如何運作

大型銀行、電子郵件、社群網路及許多網站已廣泛使用雙因子認證。這些網站大多數都會提供如何啟用雙因子認證的簡易步驟說明（如需更多訊息，請參閱文末的參考資料部分）。一旦啟用了雙因子認證，通常使用方式如下：首先像平常一樣使用用戶名稱和密碼登入帳號。這是兩因子中的第一個部分——利用已知的資訊；接著會收到一組一次性的驗證碼，通常是以簡訊寄送到您的智慧型手機，輸入驗證碼後即可登入頁面。這是兩因子的第二個部分——您必須擁有手機才能接收驗證碼。現在帳號已受到完整的保護了。即便網路犯罪份子竊取您的密碼也無法存取帳號，除非他們同時擁有您的手機。

您可以在智慧型手機上安裝一個驗證器APP來取代透過簡訊接收驗證碼。每次要登入時，這個行動APP都會產生一個獨特的驗證碼。使用此行動APP有更為安全的優點，因為這組驗證碼是透過 APP 產生，而不是藉由

## 鎖定登入

簡訊傳送；此外，它非常的方便，您不需要透過電話連線服務取得驗證碼，因為該APP會持續產生可以用來登入帳號的新驗證碼。

雖然雙因子認證一開始看似很繁瑣，不過卻能使個人資料安全性大幅提升。千萬不要讓駭客有機會入侵，請現在就為您的重要帳號（如電子郵件，銀行或社群媒體）啟用雙因子認證，並享受更佳網路安全環境帶來的安心感受。

## 進一步了解

歡迎訂閱OUCH! 全民資訊安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS資訊安全意識方案，請瀏覽我們的網站 [securingthehuman.sans.org/ouch/archives](http://securingthehuman.sans.org/ouch/archives)。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站 <http://www.tsc-tech.com> 或臉書@tsctech了解更多訊息。

## 參考資料

- 密碼短語: <https://securingthehuman.sans.org/ouch/2017#april2017>
- 支援雙因子認證的網站: <https://twofactorauth.org>
- Stop|Think|Connect: <https://www.lockdownyourlogin.org>
- Google兩階段驗證: <http://www.google.com/landing/2step/>

OUCH!由SANS Securing The Human發行刊登，遵從[Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)(創意公用授權條款4.0版)。在不更改本刊物內容的前提下，您能夠自由分享此月刊或使用於您的安全認知計劃。有關翻譯或其他資訊，請聯絡[ouch@securingthehuman.org](mailto:ouch@securingthehuman.org)。

編輯委員會: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley  
翻譯群: 邱俊傑、黃意雯、宋亞倫、孫權劭、王澤薇、葉力維、陳月娥



[securingthehuman.sans.org/blog](http://securingthehuman.sans.org/blog)



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://plus.google.com/securethehuman.sans.org)