全民資訊安全意識月刊

OUCH!

本期話題

- **密碼短語**
- **安全地使用密碼短語**
- **參考資料**

密碼短語

議題緣由

密碼是大家幾乎每天都會使用到的東西, 舉凡存取電子郵件、利用信用卡在線上購物或使用智慧型手機都需要使用密碼。然而, 密碼也是大部份人的防護弱點之一; 假如有人得知或猜到您的密碼, 他們就可以存取您的帳戶, 將錢轉走、讀取電子郵件或竊取身分資料。這就是為什麼設定高強度密碼對於保護自己至關重要。但是密碼設定通常很令人傷腦筋, 因為不太容易牢記也不好輸入。在本期文章中, 將可學習如何建立好記又容易輸入的高強度密碼—密碼短語。

客座編輯
My-Ngoc Nguyen（發音為Me-Nop Wynn）是SANS認證講師, 也是資訊科技安全解決方案公司（Secured IT Solutions）的執行長及首席顧問。她擁有高級專業認證, 並且於各種產業有超過14年開發、執行及管理網路安全計畫的經驗。可以搜尋Twitter帳號@MenopN 或LinkedIn帳號My-Ngoc"Menop"Nguyen與她聯絡。

密碼短語

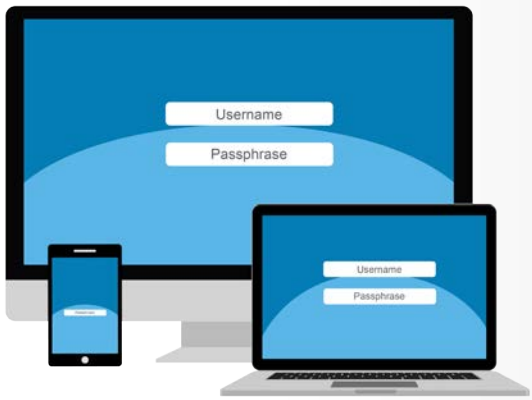
現今我們所面臨的挑戰是駭客已開發出先進且有效的方法暴力破解（自動猜測）密碼。若設定的密碼強度太弱或很容易被猜中, 壞人可很輕易地取得您的密碼。保護自己的一大重點是使用高強度密碼。這通常需要建立複雜的密碼, 但問題是這些密碼可能很難被牢記、容易弄混且不易輸入。我們建議改用由一連串隨機字詞或一個句子構成的密碼短語。因為有越多的字元, 密碼強度就越大。優點是讓駭客難以入侵, 同時更容易記憶和輸入。這裡有兩個不同的範例提供給您參考:

Sustain-Easily-Imprison （持續—輕鬆地—囚禁）
Time for tea at 1:23 （下午茶時間在1: 23）

使這些密碼短語如此強大的原因不僅是字元長度夠長, 還有交叉使用了大寫字母和特殊符號（提醒: 空格和標

密碼短語

點符號都是特殊符號的一種），同時比較容易被牢記和輸入。若想要讓您的密碼短語強度更強，可以使用數字或特殊符號取代字母，例如用符號 '@' 取代字母 'a'，或用數字0取代字母 'o'。另外，如果網站或程式限制密碼使用字元數量，請使用允許的最大字元數。



密碼短語是一個建立並牢記高強度密碼的簡單方法。

安全地使用密碼短語

除了設定密碼短語外，也請務必小心地使用。如果壞人可能很容易地竊取或複製，那麼任何高強度的密碼短語也無法發揮作用。以下為一些建議做法：

1. 每個帳戶或設備請使用不同的密碼短語。例如，工作或銀行的帳戶切記不要使用與私人帳戶，如Facebook、YouTube或Twitter相同的密碼短語。這樣可以確保當某個帳戶遭到入侵，其他帳戶仍是安全的。如果您需要記住太多組密碼短語（這非常普遍），請考慮使用密碼管理器。這是一種特殊的程式，可以安全地儲存所有的密碼短語，如此一來，只要牢記電腦或設備，以及密碼管理器的密碼短語就可以了。
2. 切勿與任何人（包括同事或主管）分享密碼短語或其建立的方式。請記住，這是每個人的秘密，如果被任何人得知就不再是安全的。一旦密碼短語不小心被其他人知道了，或覺得可能已被盜用，請立即變更。假如想讓最信任的家庭成員知道重要密碼短語，以供緊急情況時使用，建議的做法是將密碼短語（請確保它們與工作無關）記下並儲存在安全的位置後，告知深受信任的家庭成員。如此一來，如果您發生了事情需要幫助時，您親愛的家人就可以存取這個重要帳戶。
3. 請不要使用公共電腦登入您的帳號，比如飯店或網咖的電腦。因為任何人都可以使用這些電腦，它們可能已被入侵並側錄所有的鍵盤打字紀錄。建議只在可信任的電腦或行動裝置上登入您的帳號。
4. 請小心那些要求您回答個人問題的網站。這些問題通常在您忘記密碼短語，需要重新設定的時候使用。麻煩的是這些問題的答案往往可以在網路上，甚至在您的Facebook頁面上被找到，因此務必使用非公開或

密碼短語

虛構的資訊來回答個人問題。要記住這些安全性問題的所有答案有困難嗎? 可以選擇一個主題, 比如電影角色, 並以該角色的立場回答問題。或是使用密碼管理器, 它們大多能安全地儲存此附加訊息。

5. 可使用雙因子驗證, 又稱為二階段驗證。許多網路帳戶提供所謂的雙因子驗證, 驗證機制為登入帳號時, 除了密碼短語之外, 還需要輸入另一個傳送到您智慧型手機的驗證碼, 二者必須同時存在才能登入該帳號。這個方式又比僅使用密碼短語更加安全。因此盡可能使用這些更強的驗證方法。
6. 設定行動裝置PIN碼。行動裝置通常需要PIN碼來保護對其本身的存取。PIN碼也是一個密碼。提醒您, PIN碼長度越長, 就越安全。現今許多行動裝置甚至允許將PIN碼更改為密碼短語或生物識別, 如指紋。
7. 最後, 如果您不再使用某個帳戶, 請務必將其關閉、刪除或停用。

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.

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

密碼管理器: https://securingthehuman.sans.org/ouch/2015#october2015
二階段驗證: https://securingthehuman.sans.org/ouch/2015#september2015
鎖定您的登入: https://lockdownyourlogin.com
SANS SEC301 - 網路安全基礎的五天課程: https://sans.org/sec301

編輯委員會：Bill Wyman, 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