電腦用戶安全意識月刊

OUCH!

本期話題

- **密碼短語**
- **安全地使用密碼短語**
- **資源**

密碼短語

背景

密碼是您幾乎每天都使用的東西, 從網絡訪問您的電子郵件,網絡銀行來購買商品或訪問您的智能手機。不過密碼也是您的薄弱環節之一, 如果有人知道了您的密碼, 他們可以竊取您的身份, 轉移您的錢, 或訪問您的個人信息。強密碼是保護自己必不可少的。本月刊, 您將學習如何通過使用一種叫密碼短語的密碼創建易記的強密碼。

編輯嘉賓

Guy Bruneau是IPSS公司的高級安全顧問,以及是SANS講師和ISC處理。Guy持有SANS GSE並完成了SANS網絡守護程序。您可以在Twitter上**@GuyBruneau**和**handlers.sans.org/gbruneau**找到他。

密碼短語

我們面臨的挑戰是, 網絡攻擊者已經開發成熟的方法來猜測或“蠻力”破解密碼, 而且不斷進步。這意味著他們可能會危及您的密碼, 如果他們是虛弱或容易被猜到。一個重要的步驟來保護自己是使用強密碼。越多個字符的密碼越強, 攻擊者越難猜到。但是長的, 複雜的密碼可能難以記住。因此, 我們建議您使用密碼短語, 這些都是簡單的短語或句子, 很容易記住, 但很難破解。下面是一個例子。

Where is king Julian?

是什麼讓這個密碼如此強烈, 不僅是21個字符長, 而且它使用大寫字母和符號 (記住, 空格和標點符號都算符號) 。您可以讓您的密碼更強大, 如果您替換字母與數字或符號, 如更換字母’ A’ 與’ @’ 符號或者字母 “O” 為零。如果一個網站或程序限制您可以在密碼中使用字符的數量, 使用允許的最大數量的字符。

密碼短語

使用密碼短語安全地

如何使用密碼短語, 您也必須小心。使用密碼短語沒有幫助, 如果壞人能很輕易的竊取或複製。

使用密碼短語是您可以用來保護您的身份和信息的最有效的措施之一。

1. 一定要使用不同的密碼為您每個帳戶或設備。例如, 不要使用相同的密碼為您的工作或銀行賬戶以及您的個人賬戶, 如Facebook, YouTube或Twitter的。這樣, 如果其中一個帳戶被黑客攻擊, 另一個賬戶仍然是安全的。如果您有太多的密碼短語要記住 (這是很常見的) , 可以考慮使用一個密碼管理器。這是一個特殊的程序, 安全地存給您儲所有的密碼短語。這種方式唯一的密碼短語您需要記住是您的電腦密碼和密碼管理程序的密碼。

2. 千萬不要共享密碼或您創建它們的策略與其他任何人, 包括同事。請記住, 密碼是一個秘密;如果別人知道,您的密碼不再安全。如果您不小心分享密語與別人, 當作您的密碼可能已經洩露或被盜, 一定要馬上改變它。

3. 就像密碼, 避免容易猜測或常用短語。例如短語 “八十七年前” 不是一個好密碼, 因為它是那麼廣為人知。

4. 不要使用公共電腦, 例如那些在酒店或圖書館, 登錄到工作或銀行賬戶。因為任何人都可以使用這些電腦, 他們可能感染了惡意代碼, 抓住所有的按鍵。只有在受信任電腦或移動設備上登錄您的工作或銀行賬戶。

5. 小心要求您回答私人問題的網站。這些問題如果您忘記了密碼, 需要重置使用。問題是, 這些問題的答案往往可以在互聯網上找到, 甚至在您的Facebook頁面。確保如果您回答私人問題, 您使用的是不公開的唯一信息, 或您已經決定了的虛構信息。密碼管理器可以幫助您存儲這些額外的信息。

6. 許多在線賬戶提供一種叫做雙因素身份驗證, 也稱為兩步驗證。這就是您需要的不僅僅是您的密碼登錄, 例如

發送到您的智能手機的密碼。這個選項比僅僅是一個密碼本身更安全。只要有可能，總是使用這些身份驗證的更強方法。

7. 移動設備通常需要一個PIN來保護對它們的訪問。記得有一個PIN無非是另一個密碼。您的PIN越長，它越安全。許多移動設備讓您更改PIN號碼為實際密碼。

8. 最後，如果您不再使用一個賬戶，一定要關閉，刪除或禁用。

公共資源

不要使用任何公共電腦，如酒店大堂的，圖書館或在網吧的電腦。您不知道誰使用該電腦，然後，他們可能無意或有意傳染了公共電腦。只要有可能，只使用您可以控制和信任的設備進行任何在線活動。如果必須使用公共電腦，不使用任何需要您登錄或輸入密碼的服務。

進一步了解

歡迎訂閱OUCH!電腦用戶安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS安全意識的方案，請瀏覽我們的網站http://www.securingthehuman.org.

參考資料

兩步驗證:	http://www.securingthehuman.org/ouch/2013#august2013
密碼管理:	http://www.securingthehuman.org/ouch/2013#october2013
社會工程:	http://www.securingthehuman.org/ouch/2014#november2014
常見的安全條款:	http://www.securingthehuman.org/resources/security-terms

編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻譯：巴珊珊