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**
- **參考資料**

密碼短語

背景

密碼是您幾乎每天使用的東西, 從訪問您的電子郵件或在線銀行購買商品或訪問您的智能手機。然而, 密碼也是您的弱點之一;如果有人知道或猜測到您的密碼, 他們可以隨時訪問您的帳戶, 使他們能轉移您的錢, 閱讀您的電子郵件或竊取您的身份。這就是為什麼強大的密碼對於保護自己是如此至關重要。然而, 密碼通常會令人困惑, 很難記住或輸入。在本月刊中, 您將學習如何創建強大的密碼, 方便您記住並容易輸入 - 稱為密碼短語。

客座編輯
My-Ngoc Nguyen（發音為Me-Nop Wynn）是SANS的認證講師, 也是Secured IT Solutions的CEO /首席顧問。她擁有頂尖的認證和14年多的開發, 完善和管理各種 行業的網絡安全計劃的專業知識。 可以在Twitter：@MenopN或 LinkedIn：My-Ngoc"Menop"Nguyen。上找到她。

密碼短語

我們所面臨的挑戰是, 網絡攻擊者已經開發出複雜而有效的方法來強力破解 (自動猜測) 密碼。這意味著如果秘密很弱或很容易猜到, 壞人則可以取得您的密碼 。保護自己的一個重要步驟是使用強密碼。通常這是通過創建複雜的密碼來完成的, 但這些密碼可能難以記住, 令人困惑以及難以輸入。相反, 我們建議您使用密碼短語, 一系列隨機單詞或句子。您的密碼短語字數越多就越強。優點是這些更容易記住和輸入, 但對於網絡攻擊者來說依然很難入侵。這裡有兩個不同的例子。

Sustain-Easily-Imprison （維持-容易-監禁）

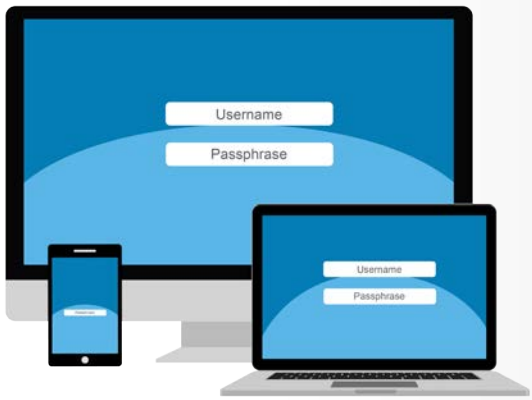
Time for tea at 1:23 （下午茶時間1:23）

這類密碼短語如此強大是因為它們不僅長, 而且使用大寫字母和符號 (記住, 空格和標點符號都屬於符號)。

© SANS Institute 2017

密碼短語

同時這些密碼短語也很容易記住和輸入。如果您想通過用數字或符號替換字母，例如用 “@” 符號替換字母 “a” 或 字母 “o” 代替為零的數字，則可以使您的密碼更強。如果網站或程式限制您可以在密碼中使用的字數，請在用允許的情況下使用最大字數。



密碼短語是創建和記住強密碼的一種更簡單的方式。

安全地使用您的密碼短語

您也必須小心如何使用密碼短語。如果壞人可以輕易竊取或複制，使用密碼短語則不會有幫助。

1. 為您擁有的每個帳戶或設備使用不同密碼短語。例如，對於您用於個人帳戶 (如Facebook, YouTube 或Twitter)， 工作或銀行帳戶之間，絕對不要使用相同的密碼短語。這樣，如果您的一個帳戶被黑客入侵，您的其他帳戶仍然安全。如果您有太多的密碼短語需要記住 (這很常見)，請考慮使用密碼管理器。密碼管理器是一個特殊的程式，可以安全地存儲您的所有密碼短語。這樣，您需要記住的唯一密碼短語只是從您的電腦或設備用來登入密碼管理器程式的。
2. 不要與其他任何人 (包括同事或主管) 分享密碼或您的密碼短語設定策略。記住，密碼短語是一個秘密；如果有人知道您的密碼短語，那就不再安全了。如果您不小心與他人分享了密碼短語，或相信您的密碼可能已被盜用或被盜，請立即更改。唯一的例外是如果您想在緊急情況下與高度信任的家庭成員分享您的個人密碼短語。一種方法是記下您的個人密碼短語 (確保它們不是工作相關的)，將其存儲在安全位置，並與高度信任的家庭成員共享該位置。這樣，如果發生某些事情，您需要幫助，您的親人可以訪問您的關鍵帳戶。
3. 不要使用公共電腦，如酒店或網吧上的電腦登錄帳戶。由於任何人都可以使用這些電腦，它們可能被感染並收集所有的擊鍵信息。只能在受信任的電腦或移動設備上登錄您的帳戶。
4. 小心那些需要您回答個人問題的網站。如果您忘記了密碼短語並需要重設，則需要使用這些問題。問題是

這些問題的答案通常可以在互聯網上找到，甚至在您的Facebook頁面上。確保如果您回答個人問題，您只能使用不公開的信息或您起的虛構信息。不記得您的安全問題的所有答案？選擇一個像電影角色的主題，並將您的答案放在該角色上。另一個選擇是再次使用密碼管理器，大多數允許您安全地存儲這些附加信息。

5. 許多在線賬戶提供了稱為雙因素身份驗證，也稱為兩步驗證。這樣您不僅僅是需要您的密碼短語登錄， 而是還需要將密碼發送到您的智能手機上。這個選項本身比一個密碼短語更安全。只要有可能，盡量啟用和使用這些更強大的身份驗證方法。
6. 移動設備通常需要一個PIN（密碼）來保護他們的訪問。記住PIN只不過是另一個密碼。您的PIN字數越長，它就越安全。許多移動設備允許您將PIN號碼更改為實際的密碼短語，或使用生物特徵，如指紋。
7. 如果您不再使用某個帳戶，請確保關閉，刪除或禁用此帳戶。

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securingthehuman.sans.org/ouch/archives.

參考資料

密碼管理器:	https://securingthehuman.sans.org/ouch/2015#october2015
兩步驗證:	https://securingthehuman.sans.org/ouch/2015#september2015
鎖定您的登錄:	https://lockdownyourlogin.com
SANS SEC301 - 網絡安全基礎五天課程:	https://sans.org/sec301

OUCH! 由SANS Securing The Human發行刊登，遵從Creative Commons 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，你可以自由分享此月刊或使用於你的安全意識計劃。有關翻譯或更多咨詢，請聯絡ouch@securingthehuman.org.

編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
翻譯：巴珊珊