電腦用戶安全意識月刊

OUCH!

本期話題

- **概述**
- **密碼**
- **兩步驗證**

兩步驗證

概觀

證明您是誰 (稱為認證) 的過程的關鍵是保護您的信息。強大的身份驗證嘗試只是為了確保您可以訪問您的信息, 如電子郵件, 照片, 或者您的銀行帳戶。有三種不同的方式來確認您是誰; 您所知道的 - 例如密碼, 您有什麼 - 比如您的駕駛執照, 以及您是什麼 - 比如您的指紋。這些方法的每一個都有優點和缺點。最常見的方法是密碼, 您知道的東西。在本月刊, 我們將教您如何使用兩步驗證保護自己, 這遠遠不僅僅使密碼更安全, 而使用起來非常簡單。為了更好地了解兩步驗證, 我們需要從使用密碼開始。

編輯嘉賓
Keith Palmgren擁有超過30年在信息安全方面的經驗。他是SANS研究所認證講師和作者, 也是SANS SEC301, 為期五天的信息安全介紹講師。課餘時間, Keith側重於諮詢和寫作項目。您可以在基思@kpalmgren找到他。

密碼

密碼證明您是誰基於您知道的東西。使用密碼的危險是, 他們是一個單一防線。如果有人能猜到或者獲取您的密碼, 那麼他們就可以假裝是您和訪問由它獲得所有信息。這就是為什麼您要遵循一些措施來保護您的密碼, 如使用他人難以猜到的強密碼, 為每個帳戶使用不同的密碼或不與他人分享您的密碼。雖然這個建議仍然有效, 密碼的用處不止於這些, 在今天的現代社會他們不再是有效的。最新的技術使網絡攻擊者太容易獲取密碼。我們需要的是一個易於使用, 更加安全的解決方案, 強大的身份驗證。幸運的是, 這樣的選擇是現在常用的所謂兩步驗證。

兩步驗證

兩步驗證 (有時也被稱為雙因素身份驗證或2FA) 不僅僅是一個密碼更安全的解決方案。它的工作原理是要求不是一個而是兩個不同的方法來驗證自己的身份。一個例子是ATM卡。當您從ATM提款機取錢, 您實際上是使用兩個步驟驗證

兩步驗證

的一種形式。要提取錢，您需要兩樣東西，您的ATM卡（您所擁有的）和您的PIN碼（您知道的）。如果您失去了您的ATM卡，錢還是安全的。任何人發現您的卡無法取您的錢，因為他們不知道您的密碼（除非您在卡寫上您的PIN碼，這是一個非常糟糕的主意）。同樣是如此，如果他們只有您的PIN和沒有卡。攻擊者必須兩樣都擁有才能危及您的ATM帳戶。這是為什麼使兩步驗證安全很多，因為您的安全有兩層。

只要有可能，就儘量使用兩步驗證，這是您可以用來保護您的信息最強的步驟之一。

採用兩步驗證

兩步驗證是為每個帳戶單獨設置的東西。幸運的是許多在線服務現在提供它。其中一個兩步驗證的領導者是Google。Google帳戶是網絡攻擊的主要目標，因為它提供世界各地數以百萬計的人們各種免費在線服務。因此Google需要提供更強的身份驗證，並且是大部分的在線服務中第一個組織推出兩步驗證。如果您了解Google的兩步驗證的工作原理，您就會明白如何兩步驗證適用於大多數其他網站，如Twitter，Facebook和蘋果，Instagram的和許多銀行。

首先，您對您的Google帳戶啟用兩步驗證，並註冊您的手機號碼。一旦完成，兩步驗證的工作原理如下。正如之前您登錄到您的帳戶用您的用戶名和密碼。這是第一次兩個因素 - 您知道的東西。Google然後發送包含唯一代碼的短信到您的手機，六個具體數字的字符串。就像您的密碼，您再輸入網站上的六個號碼。這是這兩個因素的第二個。因此，要成功登錄到您的帳戶，您要知道您的密碼和您的手機接收的唯一代碼。即使攻擊者有您的密碼，他們無法訪問您的Google帳戶，除非他們也有您的電話。為了確保您的賬號是真正安全的，Google會在每次您登錄時發送給您一個新的，唯一的代碼。

還有另外一個與Google和其他許多網站的兩步驗證選擇。相反於通過短信接收的唯一代碼，您可以在您的智能手機上安裝一個應用程序的認證。您每次登錄，該應用程序會產生唯一的代碼。使用移動應用程序的優點是您不需要連接

兩步驗證

到電話服務來收到您的唯一代碼，您的手機會產生給您。另外由於代碼從您的手機上產生，而不是發送給您，它不會被截獲。

記住，默認情況下兩步驗證不開啟，您必須自己啟用它。雖然兩步驗證開始可能看起來像更多的工作，我們強烈建議您只要有可能就使用它，特別是對關鍵服務，如電子郵件帳戶，網上銀行或在線存儲您的文件。兩步驗證比僅僅使用簡單的密碼來保護信息更進了一步。

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

密碼短語:	http://www.securingthehuman.org/ouch/2015#april2015
支持兩步驗證的網站:	https://twofactorauth.org
停一停|想一想|連接:	http://stopthinkconnect.org/2stepsahead
Google兩步驗證:	http://www.google.com/landing/2step/
SANS每日安全提示:	http://www.sans.org/tip_of_the_day.php

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