OUCH!

SANS SECURITY AWARENESS

您的每月安全意識通訊

簡單使用密碼

概觀

您經常被告知您的密碼是保護您帳戶的關鍵（這是真的！），但很少有一種簡單的方法可以安全地創建和管理您的所有密碼。下面我們將介紹三個簡單的步驟，以簡化您的密碼，鎖定您的帳戶並保護您的未來。

密碼短語

使用瘋狂和複雜密碼的日子結束了。這些密碼難以記憶，難以打字，而今天的超快速電腦很容易被網絡攻擊者破解。密碼的關鍵是讓它們變長，您擁有的字符越多越好。這些被稱為密碼短語，一種使用短句或隨機單詞的強密碼。這里有兩個例子：

Time for strong coffee!（是時候喝濃咖啡！）
lost-snail-crawl-beach （迷失的蝸牛爬海灘）

這兩個都很強大，超過二十個字符，易於記憶，易於打字，但難以破解。您將遇到要求您在密碼中添加符號，數字或大寫字母的網站或情況，也沒關係。記住它的長度是最重要的。

密碼管理員

每個帳戶都需要一個唯一的密碼。如果您為多個帳戶重複使用相同的密碼，那麼您將面臨極大的危險。所有網絡攻擊者需要做的就是破解您使用的網站，竊取包括您的所有密碼，然後使用您的密碼登錄您所有的其他帳戶。它的發生頻率遠遠超出您的意識。不相信嗎？查看網站www.haveibeenpwned.com，您就能了解到哪些使用的網站被黑客入侵過以及您的密碼可能遭到破壞。那您該怎麼辦？使用密碼管理器。

這些是特殊的電腦程序, 可以將所有密碼安全地存儲在加密的保管庫中。您只需記住一個密碼, 即密碼管理器的密碼。然後, 密碼管理器會在您需要時自動檢索您的密碼, 並為您登錄網站。它們還具有其他功能, 例如存儲您的秘密問題的答案, 在重複使用密碼時發出警告, 確保使用強密碼的密碼生成器以及許多其他功能。大多數密碼管理器也可以在幾乎任何電腦或設備上安全地同步, 因此無論您使用何種系統, 您都可以輕鬆, 安全地訪問所有密碼。

最後, 請務必將密碼寫入密碼管理器並將其存儲在家中的安全位置。有些密碼管理器甚至允許您打印出密碼管理器恢復工具包。這樣, 如果忘記了密碼管理器的密碼, 就可以進行備份。或者, 如果您生病或發現自己處於緊急狀態, 您的配偶或可信賴的家庭成員可以代表您檢索信息。

兩步驗證

兩步驗證 (通常稱為雙因素身份驗證或多因素身份驗證) 增加了額外的安全層。它要求您在登錄帳戶時做兩件事, 密碼和由智能手機生成或發送到手機的數字代碼。此過程可確保即使網絡攻擊者獲取您的密碼, 他們仍然無法進入您的帳戶。兩步驗證很容易設置, 您通常只需在從新電腦或設備登錄時使用一次。盡可能啟用此功能, 尤其是對於您最重要的帳戶, 例如您的銀行或退休帳戶或訪問您的電子郵件。如果您使用的是密碼管理器, 我們強烈建議您使用強大的密碼短語和兩步驗證進行保護。

這可能聽起來很滑稽, 但這三個簡單的步驟對保護您的工作, 聲譽和財務未來有很大幫助。

客座編輯

Justin Henderson (@SecurityMapper) 是H&A安全解決方案的聯合創始人, 是SANS研究院的認證講師, 也是SANS網絡防禦和SIEM課程的作者。他熱愛所有網絡防禦, 並且已經諮詢了十五年。

參考資料

我有沒有被入侵過: https://haveibeenpwned.com/
雙因素身份驗證站點: https://twofactorauth.org/
NIST SP800-63B數字身份指南: https://pages.nist.gov/800-63-3/sp800-63b.html
海報: 您是一個目標: https://www.sans.org/u/OGi

OUCH! 由SANS Security Awareness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 www.sans.org/security-awareness/ouch-newsletter. 編輯委員會: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | 翻譯: 巴珊珊