SANS SECURITY AWARENESS

OUCH!

您的每月安全意識通訊

保持安全的四個簡單步驟

概觀

安全可靠地充分利用技術可能會讓人感到困惑。但是，無論您使用什麼技術或如何使用它，都可以通過以下四個簡單步驟來確保您的安全。

1.您自己：首先，最重要的是，技術無法完全保護您，您是您的最佳防禦。攻擊者了解到，獲得他們想要的東西的最簡單方法是針對您而不是您的電腦或其他設備。如果他們想要您的密碼，信用卡或電腦控制權，他們會試圖通過使人產生緊迫感來欺騙您，將其提供給他們。例如，他們可以稱自己為Microsoft技術支持，並聲稱您的電腦已被感染，而實際上，他們只是網絡犯罪分子，希望您允許他們訪問您的電腦。或者，他們可能會向您發送一封電子郵件警告，警告您無法遞送包裹，並迫使您單擊鏈接以確認您的郵寄地址，而實際上，他們卻在欺騙您訪問可入侵您電腦的惡意網站。最終，針對攻擊者的最大防禦方法就是您。通過使用常識，您可以發現並阻止許多攻擊。

2.密碼短語：現代的計算速度已令舊的8個字符的密碼過時且容易受到攻擊。當網站要求您創建密碼時，請創建一個強大而獨特的密碼短語。密碼短語是一種密碼，它使用一系列易於記憶的單詞，例如“ bee honey bourbon rain”。密碼短語越長，越強。唯一口令意味著對每個設備或在線帳戶使用不同的口令。這樣，如果一個密碼短語遭到破壞，您所有其他帳戶和設備仍然是安全的。記不清所有這些密碼短語？使用密碼管理器，這是一個專用程序，可以安全地以加密格式存儲所有密碼短語（以及許多其他重要功能）。

最後，啟用兩步驗證（也稱為兩因素或多因素身份驗證）。它在使用您的密碼的程度上，還增加了第二步，例如發送到智能手機的代碼或為您生成代碼的應用程序。兩步驗證可能是保護在線帳戶最重要的步驟，而且比您想像的要容易得多。

3.更新：確保您的每台電腦，移動設備，程序和應用程序都在運行其軟件的最新版本。網絡攻擊者一直在尋找設備使用的軟件中的新漏洞。當他們發現漏洞時，會使用特殊程序來利用這些漏洞併入侵您正在使用的設備。同時，為這些設備創建軟件的公司正在努力通過發布更新來修復它們。通過確保您的電腦和移動設備及時安裝這些更新，可以使某人更難於入侵您。要保持最新狀態，只要有可能就啟用自動更新即可。該規則幾乎適用於連接到網絡的所有技術，包括連接互聯網的電視，嬰兒監視器，安全攝像機，家用路由器，遊戲機，甚至您的汽車。

4.備份和恢復：有時，無論您多麼小心，都可能被攻擊入侵。在這種情況下，還原所有個人信息的唯一途徑通常是備份。確保對所有重要信息進行定期備份，並確認可以從中還原數據。大多數操作系統和移動設備都支持自動備份到外部驅動器或云。

客座編輯

SANS認證講師**Steve Anson**為全球IT安全團隊和政府提供指導，以改善其安全狀況。Steve是即將出版的《應用事件響應》（Applied Incident Response）一書的作者，並通過www.AppliedIncidentResponse.com為IT安全從業人員提供免費資源。

參考資料

社會工程學: https://www.sans.org/u/W3G
個性化騙局: https://www.sans.org/u/W3Q
使密碼變得簡單: https://www.sans.org/u/W3V
獲得備份: https://www.sans.org/u/W40