電腦用戶安全意識月刊

OUCH!

本期話題

- **什麼是加密？**
- **什麼是您可以加密的？**
- **正確使用加密**

加密

什麼是加密?

您可能會聽到人們用“加密”和您應該如何使用它來保護自己和您的信息。然而, 加密可能會造成混淆, 您應該了解它的局限性。在本月刊裡, 我們深入淺出的講解什麼是加密, 它是如何保護您和如何正確實現它。

客座編輯

Francesca Bosco（**@francibosco**）是研究員和項目官員， 管理涉及網絡犯罪， 網絡安全和技術濫用的項目。她正在聯合國區域間犯罪和司法研究所和她共同創立的技術和法律中心工作。

您的個人文件, 照片和電子郵件等大量敏感信息在您的設備中。如果您的設備丟失或被盜, 誰得到它就可以訪問您所有的敏感信息。此外, 您或许進行網上敏感的交易, 如銀行或在線購物。如果被別人監視這些活動, 他們可以竊取您的信息, 比如您的財務帳戶或信用卡號碼。在這些情況下加密可以保護您, 幫助確保未經授權的人無法訪問或修改您的信息。

加密已經存在了幾千年。如今, 加密是更為複雜, 但它有異曲同工之妙 - 確保從一個地方傳遞秘密信息到另一個只有通过授權才可以訪問它以及讀取信息。當信息沒有被加密, 它被稱為純文本。這意味著任何人都可以輕鬆讀取或訪問它。加密將此信息轉換成非可讀格式叫做密文。今天的加密工作原理是利用複雜的數學運算和獨特的密鑰使您的信息轉換成密文。密鑰是用来鎖定或解鎖您的信息。在大多數情況下, 您的密鑰是密碼。

什麼是您可以加密的?

一般有兩種類型的數據加密, 在休息的數據（如存儲在移動設備上的數據）, 在運動的數據（如接收電子郵件或發短信给朋友）。

加密

對休息數據進行加密是对保護信息至關重要的，尤其是您的計算機或移動設備丟失或被盜。今天的設備是非常強大的，它持有大量的信息，但也很容易丟失。此外，其它類型的移動媒體也能容納敏感信息，例如一個USB閃存驅動器或外部硬盤驅動器。全磁盤加密（FDE）是一種廣泛使用的加密技術來加密系統中的整個驅動器。這意味著，在系統上一切都為您自動加密，您不用決定什麼加或不加密。今天，大多數的電腦配備了FDE，但您可能必須手動開啟或啟用它。在Mac計算機上它被稱為FileVault的，而在Windows計算機上，根據不同的版本，您可以使用BitLocker或設備加密。大多數移動設備還支持FDE。一旦在iPhone和iPad上的密碼已設置，iOS就会自動啟用FDE。採用Android 6.0（棉花糖），谷歌要求FDE默認啟用，但需提供的硬件是滿足特定的最低標準。

加密是以一個強大的方式來幫助保護您的信息，但它只能和您的密鑰一樣強。

信息在運輸途中也是脆弱的時候。如果數據是不加密的，它可以被監視，修改和在線捕獲。這就是為什麼您要確保任何敏感網上交易和通信進行加密。在線加密常見的類型是HTTPS。這意味著您的瀏覽器和一個網站之間的所有通信是被加密的。尋找https: //開頭的網址，該網址欄上的瀏覽器出現一个鎖的圖標，或着網址變成绿色。另一個例子是，當您發送或接收電子郵件。大多數電子郵件客戶端提供加密，但您可能需要啟用加密功能。在傳輸過程中加密數據的第三個例子是兩個用戶互相聊天，如用的iMessage, Wickr, Signal, WhatsApp的或Telegram之間。這些應用程序使用端至端加密以防止第三方在數據從系統一端或設備到另一個的轉移中訪問數據。這意味著只有您和與您溝通的人才可以讀到。

正確使用加密

為了確保您得到加密時保護， 最重要的是您能正確地使用它。

加密

- 您的加密只能和您的密鑰一樣強。如果有人猜測或獲取您的密鑰，他們將有機會獲得您的數據。保護您的密鑰。如果您正在使用您的密鑰的密碼或密碼，請確保它是一個強大的，唯一的密碼。密碼越長，攻擊者就越難猜測或暴力破解它。但是不要忘記您的密碼，沒有它，您將不可以再解密您的信息。如果您不記得您所有的密碼， 推薦大家使用密碼管理器。
- 您的加密只能和您的設備的安全性一樣強。如果您的設備已經失密或者被惡意攻擊者的網絡感染他們就可以繞過加密。這就是為什麼很重要的一點是您採取其他措施來保護您的設備，包括使用抗病毒，強密碼，並保持更新。
- 許多移動應用和電腦應用程式現在提供強大的加密保護您的數據和通信。如果應用程序或應用程序您正在考慮並不支持加密，您應該考慮另一種。

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

加密說明: http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

口令: https://securingthehuman.sans.org/ouch/2015#april2015

密碼管理: https://securingthehuman.sans.org/ouch/2015#october2015

什麼是惡意軟件: https://securingthehuman.sans.org/ouch/2016#march2016

保護您的新平板: https://securingthehuman.sans.org/ouch/2016#january2016

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