電腦用戶安全意識月刊

OUCH!

本期話題

- 概述
- 隱私
- 安全

社交媒體

概述

社交媒體網站，如Facebook，微博，Instagram和LinkedIn是驚人的資源，讓您見面，互動，並與世界各地的人們分享。然而這一切權力來的風險，不只是對您，還有您的家人，朋友和雇主。本月刊我們會講解這些危險，以及如何安全地使用這些網站。

編輯嘉賓

Tanya Baccam是一個長期的安全顧問。十多年來她一直是SANS作者和導師，包括SEC502，SEC542，SEC401，MGT414，AUD507等多門課程。可以在Twitter上@tbaccam跟隨她。

隱私

人們普遍關心的社交媒體問題是保護您的個人信息。潛在的危險包括:

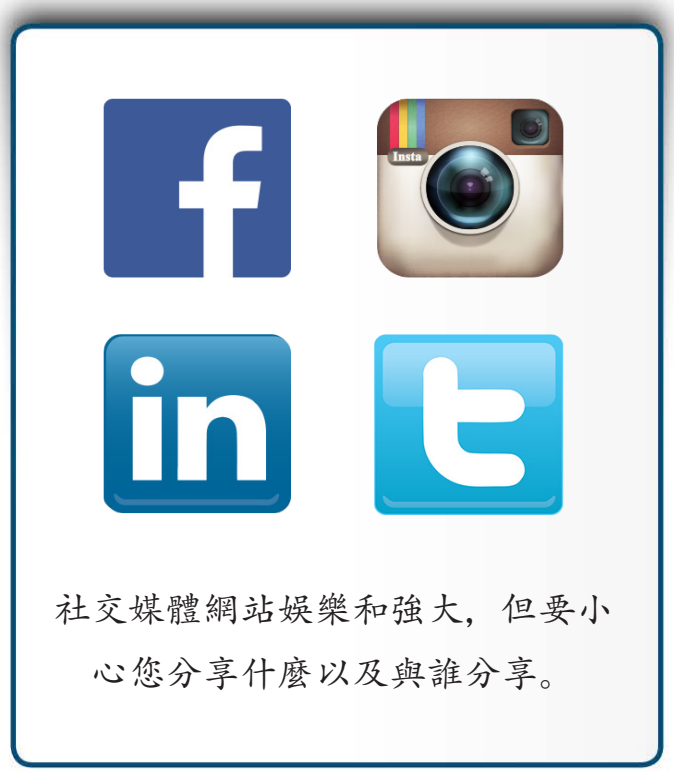
- **影響您的未來**: 有些組織搜索社交媒體網站作為背景檢查的一部分。尷尬或罪證照片或帖子，不管多久，仍能防止您被聘用或晉升。此外，許多大學對新的學生簽證申請進行類似的檢查。隱私選項可能無法提供保護，因為這些組織可以讓您“喜歡”或加入他們的網頁或某些網貼可能會在多個網站上存檔。
- **攻擊您**: 網絡攻擊者可以分析您的文章，並用它們來獲得您或您的組織的信息訪問。例如，他們可以使用您的信息共享猜您的“秘密問題” 答案來重置您的網上密碼，創建有針對性的電子郵件攻擊您(稱作魚叉捕魚)，或打電話給您的組織裡其他人假裝是您。此外，這些攻擊可以蔓延到現實世界，如確認您在哪裡工作或生活。
- **無意中傷害您的雇主**: 不法分子或競爭對手可以使用您張貼的關於您的雇主組織中的任何敏感信息。此外，您的帖子可能會導致您的組織的名譽損害。請務必在發布與您的任何工作事情之前檢查您的組織的策略，而且您的一些社交媒體的帖子可能會被監控。

最好的保護就是限制您發布的內容。是的，隱私選項可以提供一些保護，但他們往往是混亂，或在您不知道的情況下頻繁更改。您以為是私人的帖子可以以各種理由迅速成為公眾的。另外，您的帖子的隱私是否安全在於與您分享的人。更多的朋

社交媒體

友或聯繫人與您分享，更多的可能是信息將被公開。您應該假設您發布的任何事情將成為公眾和互聯網的永久組成部分。

最後，要注意朋友都張貼關於您的些什麼。如果他們張貼的東西使您不舒服，要求他們把它拿下來。如果他們拒絕或忽略您，請與社交媒體網站聯絡，並要求該網站為您刪除該內容。同時，要尊重您發布的他人的內容。



安全

除了隱私問題，這裡有一些措施來保護您的社交媒體賬戶和網上活動。

- **登錄**：保護您的每個帳戶用強烈的，獨特的密碼，不要與其他人分享。此外，許多社交媒體網站支持更強的身份驗證，如兩步驗證。務必儘可能使用這些更強的身份驗證方法。最後，不要用您的社交媒體賬號登錄到其他網站，如果它被盜用，所有帳戶都將有危險。
- **隱私設置**：如果您使用隱私設置，請確保您定期審查和測試。社交媒體網站經常更改隱私設置，很容易犯錯誤。此外，許多應用程序和服務讓您標記您發布的內容的位置，（被稱為地理標記）。如果您想保持您的物理位置隱私，　請定期檢查這些設置。
- **加密**：社交媒體網站採用加密稱為HTTPS，以確保該網站的在線連接。有些網站如Twitter和Google+啟用此默認，而有些則需要您手動啟用HTTPS。檢查您的社交媒體帳戶設置並盡可能啟用HTTPS作為默認連接。
- **電子郵件**：對聲稱來自社交媒體網站的電子郵件持懷疑態度，這些很容易被被網絡犯罪分子入侵來發送攻擊。回復此類郵件的最安全的方法是直接登錄到您的社交媒體網站上，或可以從保存的書籤登錄，然後閱讀和回復來自網站的任何消息或通知。
- **惡意鏈接/詐騙**：要小心可疑鏈接或張貼在社交媒體網站的潛在欺詐。壞人利用社會媒體來傳播攻擊。僅僅因為一個朋友的發布消息，並不意味著消息是真正來自他們，他們的帳戶可能受到了入侵。如果一個家庭成員或朋友發布了一個奇怪的消息，您無法驗證（比如他們已經被搶劫而需要您寄錢），以他們的移動電話或其他方式聯絡他們以確認該消息確實來自他們。

社交媒體

- **移動應用程序**: 大多數社交媒體網站提供移動應用程序來訪問您的在線帳戶。確保您從受信任的站點和您的智能手機使用強密碼保護下下載這些移動應用程序。如果您的智能手機丟失去而它被解鎖, 任何人都可以通過智能手機訪問社交媒體網站, 並開始以您的身份張貼。

社交媒體網站是以一個奇妙的溝通方式, 保持與世界的聯繫。如果您遵循這裡列出的技巧, 您應該能夠享受到更安全的在線體驗。要了解更多關於如何安全使用社交媒體網站或報告未經授權的活動, 請檢查您的社交媒體網站的安全網頁。

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
兩步驗證:	http://www.securingthehuman.org/ouch/2013#august2013
安全使用移動應用程序:	http://www.securingthehuman.org/ouch/2015#january2015
教育孩子網絡安全:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook的安全性:	https://www.facebook.com/safety

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