電腦用戶安全意識月刊

OUCH!

本期話題

- 什麼是CEO騙局？
- 保護自己

CEO騙局

什麼是CEO騙局?

網絡犯罪分子都是偷偷摸摸的, 他們都在不斷想出新的方法來得到他們想要的東西。他們的一個最有效的方法是針對您這樣的人。網絡攻擊者已經學會了人們本身是在任何組織中最薄弱的環節, 可是他們忘記了, 懂行的人都是喜歡本月刊 (OUCH!) 的讀者, 而且可以是一個組織的最好的防守

客座編輯

Angela Pappas是湯森路透（Thomson Reuters）的信息安全培訓和安全意識董事。在她的角色裡, Angela負責大使計劃, 電子教學和網絡釣魚等有關員工教育。

網絡犯罪分子已經開發出一種名為CEO騙局新的攻擊, 也被稱為企業郵箱妥協 (BEC) 。在這些攻擊中, 網絡犯罪分子假裝是您的從組織首席執行官或其他高級管理人員發送電子郵件給您試圖欺騙您做一些您不應該做的事情。因為網絡犯罪分子做過他們的研究, 這些類型的攻擊是非常有效的。他們搜索組織的信息網站, 比如誰是您的高管們, 和您一起工作的其他組織。網絡罪犯然後了解像LinkedIn, Facebook或Twitter的網站關於您的同事一切可能。一旦他們知道您的組織結構, 就開始研究和針對特定員工。他們挑根據自己的具體目的他們的目標。如果網絡犯罪分子正在尋找錢, 他們可以針對在應付賬款部門的工作人員。如果他們正在尋找的稅務信息, 他們可能會針對人力資源。如果他們想訪問數據庫服務器, 他們可以針對在IT的人。

一旦他們決定他們想要什麼和他們的目標, 他們就開始起草自己的攻擊。大多數情況下, 他們用魚叉式網絡釣魚。網絡釣魚是指攻擊者發送一封電子郵件給百萬計的人誘騙他們做一些事情, 例如打開受感染的附件或訪問一個惡意網站。魚叉式網絡釣魚類似於網絡釣魚;然而, 而不是發送一個普通的電子郵件給數以百萬計的人, 他們發送自

© SANS Institute 2016

CEO騙局

定義郵件給非常少數針對的人。這些魚叉式網絡釣魚電子郵件是非常真實的, 防不勝防。他們經常似乎來自您認識的人或工作, 如員工的同事或者甚至您的老闆。這些電子郵件看起來真實, 因為他們可能會使用您的同事相同的術語;他們可能會使用您的組織的標誌, 甚至是行政機關的正式簽名。這些郵件往往使人產生一種很大的急迫感, 要求您立即採取行動, 而不告訴任何人。網路罪犯的目標是您催促你犯一個錯誤。這裡有三個常見的場景:

CEO騙局是一個強大的攻擊, 它可以繞過大多數我們的安全性防禦。最終, 您是我們最好的防禦。

- **電匯**: 網絡犯罪是想要錢的。這意味著他們研究和學習誰在應付或處理您的組織的財務團隊工作的帳戶。然後犯罪分子設計和發送電子郵件假裝是他們的老闆;該電子郵件告訴他們有緊急情況需要轉錢到某個帳戶。

- **稅務騙局**: 網絡罪犯想竊取您的同事的信息, 以便他們能冒充員工進行稅務騙局。他們研究您的組織, 並確定誰處理員工的信息, 例如, 有人在人力資源。從那裡, 網絡犯罪分子發送偽造電子郵件, 假裝是從法律的高級管理人員或也許有人, 要求某些文件被立即提供。

- **律師模擬**: 並非所有的CEO騙局攻擊只涉及電子郵件;　還有其它方法, 如使用電話。在這種情況下, 不法分子通過電子郵件,　假裝是一個高層領導, 通知您會有律師打電話談一件緊急的事情。然後, 犯罪分子打電話給您假裝是律師。因為他們談論時間的敏感性, 和事情的保密性, 罪犯所創建的緊迫感油然而生。這種緊迫感技巧就逼您就範了。

© SANS Institute 2016

CEO騙局

保護自己

所以，您能做些什麼來保護自己和您的組織？常識是您最好的防禦。如果從您的老闆或同事收到一條消息，它不健全或覺得不對勁，這可能是一種攻擊。線索可以包括緊急感油然而生，看起來不正確的簽名，您想像不到的肯定的語氣，或者在電子郵件中使用的名稱是和現實中稱號您的有所不同。另一條線索是，攻擊者使用您從未見過的電子郵件地址或電話號碼，或者他們使用的電子郵件地址非常相似，但不完全相同於您的同事或者老闆。如有疑問，請撥打此人信任的電話號碼，或親自接觸他們（不要通過電子郵件回复），並確認他們是否發送該電子郵件。千萬不要繞過安全政策和程序。您的組織可能有定義授權資金轉移或機密信息發布的適當程序策略。試圖繞過這些政策的要求，不論其外表看起來如何，應被視為可疑，在採取任何行動之前進行驗證。如果您收到這樣的請求，不知道該怎麼做，請聯繫您的主管，幫助台或信息安全團隊。

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

社會工程:	https://securingthehuman.sans.org/ouch/2014#november2014
網絡釣魚:	https://securingthehuman.sans.org//ouch/2015#december2015
什麼是惡意軟件:	https://securingthehuman.sans.org/ouch/2016#march2016
兩步驗證:	https://securingthehuman.sans.org/ouch/2015#september2015
每日提示:	https://www.sans.org/tip-of-the-day

OUCH! 由SANS Securing The Human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ouch@securingthehuman.org.

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

© SANS Institute 2016