SANS SECURITY AWARENESS

OUCH!

電腦用戶安全意識月刊

首席執行官欺詐/ BEC

什麼是CEO欺詐/ BEC?

網絡攻擊會繼續演變為CEO欺詐或商業電子郵件妥協Business Email Compromise (BEC) 的電子郵件攻擊。這些是針對性的電子郵件攻擊, 誘使受害者採取他們不應採取的行動。在大多數情況下, 壞人都追求金錢。這些攻擊如此危險的原因是網絡攻擊者在發起攻擊之前研究他們的受害者。安全技術也很難阻止這些攻擊, 因為沒有受感染的電子郵件附件或惡意鏈接要檢測。以下是攻擊的工作原理。

網絡攻擊者使用互聯網來研究他們想要的受害者和他們的受害者與之交互的人。例如, 如果他們針對您, 他們會研究誰是您工作的老闆, 或者是您在家工作的房地產經紀人。然後網絡攻擊者製作一封電子郵件, 假裝是這些人中的一員並將電子郵件發送給您。電子郵件是緊急的, 要求您立即採取行動, 例如處理發票, 更改付款人或說服您回复敏感文件。電子郵件通過施壓使您做他們想做的事。以下是兩個這樣的攻擊如何發揮作用的例子。

電匯: 網絡犯罪分子想要的是錢。他們研究您所工作的公司, 例如確定誰在應付賬款部門中工作或負責轉移資金的人。然後, 犯罪分子製作並發送電子郵件給這些假裝自己的老闆或高級執行人員。電子郵件告訴他們有緊急情況, 必須立即將錢轉移到新的銀行賬戶。電子郵件迫使他們犯了一個錯誤, 實際上他們正在向網絡犯罪分子匯款。

稅務欺詐: 網絡犯罪分子利用人們的個人信息進行稅務欺詐。獲得此信息的最快方法之一是竊取公司所有員工的信息。網絡犯罪分子研究並確定誰在人力資源部門工作。然後他們向這些人發送假電子郵件, 冒充高級管理人員或者可能是合法的人。電子郵件講了一個緊急事件, 必須立即提交所有員工的稅務信息。人力資源部門的人員認為他們正在向高級管理人員發送敏感文件, 而實際上他們正在將他們發送給網絡犯罪分子。

保護自己

那麼您可以做些什麼來保護自己? 常識是您最好的防守。以下是最常見的線索。

- 電子郵件非常短且緊急 (通常只有幾句) , 簽名表示電子郵件是從移動設備發送的。
- 有強烈的緊迫感, 迫使您忽視或繞過雇主的政策。一定要始終遵循與工作相關的政策和程序, 即使電子郵件似乎來自您的老闆甚至CEO。
- 電子郵件與工作相關, 但使用個人電子郵件地址, 例如@ gmail.com或@ hotmail.com。
- 電子郵件似乎來自您認識或合作的高級領導, 同事或供應商, 但消息的語氣聽起來並不像他們。
- 提供付款說明, 這些說明與您已收到的說明不同, 例如要求立即向其他銀行帳戶付款。

如果您懷疑在工作中自己已成為目標, 請停止與攻擊者的所有互動並將其報告給您的主管。如果您在家已經成為目標, 或者您已經成為受害者並且已經進行了電匯, 請立即向您的銀行報告, 然後再向執法部門報告。

客座編輯

Don Cavender是前FBI特工, 擁有22年以上的數字取證和網絡犯罪經驗。他最近作為華盛頓特區BEC協調員專門打擊將網絡犯罪組織。他提供培訓並開展數字取證和網絡調查方面的研究。 您可以在 @don_cavender https://www.linkedin.com/in/donald-cavender 上找到他。

參考資料

社會工程:	https://www.sans.org/u/HE3
阻止那個網絡釣魚:	https://www.sans.org/u/HE8
阻止惡意軟件:	https://www.sans.org/u/HEd
鎖定您的登錄信息:	https://www.sans.org/u/HEi