SANS SECURITY AWARENESS

OUCH!

您的每月安全意識通訊

個性化詐騙

概觀

網絡犯罪分子繼續提出愚弄人們的新方法。一種新型騙局越來越普遍，　就是個性化詐騙。網絡犯罪分子查找或購買數百萬人的信息，然後使用該信息來個性化他們的攻擊。下面我們將向您展示這些騙局如何運作並引導您完成一個常見示例。您對這些騙局了解得越多，就越容易發現並阻止它們。

它是如何運作的?

電子郵件或電話詐騙並不新鮮，網絡犯罪分子多年來一直試圖愚弄人們。例如“您贏了彩票”或臭名昭著的尼日利亞王子騙局。然而，在這些傳統騙局中，網絡犯罪分子並不知道他們的目標對象。他們只是創建一個通用消息並將其發送給數百萬人。因為這些騙局非常通用，所以通常很容易發現。個性化的騙局是不同的，網絡犯罪分子首先進行研究，並為每個目標受害者創建定制的信息。他們通過查找或購買人員姓名，密碼，電話號碼或其他詳細信息的數據庫來實現此目的。在所有被黑客攻擊的網站都可以輕鬆獲得此類信息。它也常見於社交媒體網站和公開的政府記錄中。犯罪分子然後針對他們掌握每個人的信息。

網絡罪犯使用的一個常見技巧是恐懼或勒索迫使您付錢給他們。攻擊類似這樣：他們查找或從黑客網站購買獲取人員登錄和密碼的信息。他們發現您的帳戶信息包含在此類數據庫中，並向您（以及數據庫中的其他人）發送一封電子郵件，其中包含您的一些個人詳細信息，包括您在被黑網站上使用的原始密碼。犯罪分子將您的密碼稱為“入侵您自己的電腦或設備的證據”，這當然不是真的。犯罪分子然後聲稱，雖然他們攻擊了您的電腦，但他們也發現您在線觀看色情內容。然後，該電子郵件威脅說，如果您不支付敲詐勒索費，他們將與您的家人和朋友分享令人尷尬的在線活動的證據。

問題是，在幾乎所有這種情況下，網絡犯罪分子都沒有攻擊您的系統。他們甚至不知道您是誰或您訪問過哪些網站。詐騙者只是試圖利用他們對您的一些個人細節來嚇唬您，使您相信他們攻擊了您的電腦或設備，並欺騙您付錢給他們。請記住，壞人也可以使用相同的技術進行電話詐騙。

我該怎麼辦?

認識到像這樣的電子郵件或電話就是騙局。當某人掌握有關您的個人信息時，自然會感到害怕。但是，請記住發件人在撒謊。攻擊是自動化大規模活動的一部分，而不是直接針對您的嘗試。今天的網絡犯罪分子越來越容易找到或購買個人信息，所以未來會有更加個性化的騙局。這裏可以找到的一些線索:

⚠

- **每當收到高度緊急的電子郵件時，郵件或電話都會非常可疑。如果某人正在使用恐懼或緊迫感等情緒，他們會試圖催促您犯錯誤。**
- **當有人要求使用比特幣，禮品卡或其他無法追踪的方法付款時**
- **當您收到可疑電子郵件時，請在Google上搜索其他人是否報告過此類攻擊。**

最終，常識是您最好的防守。但是，我們還建議您始終為每個在線帳戶都使用唯一的長密碼。記不起您的所有密碼? 可以使用密碼管理器。此外，盡可能啟用兩步驗證。

客座編輯

Lenny Zeltser是一名網絡安全老手。他在Minerva實驗室構建反惡意軟件解決方案，並在SANS Institute教授安全課程。他的經驗還包括託管安全服務和諮詢。您可以在 zeltser.com/blog 和Twitter @lennyzeltser 上關注他。

參考資料

社會工程: https://www.sans.org/u/MUU
停止那個網絡釣魚: https://www.sans.org/u/MUZ
在線搜索自己: https://www.sans.org/u/MV4
密碼管理器: https://www.sans.org/u/MV9