電腦用戶安全意識月刊

OUCH!

本期話題

- **概述**
- **網絡釣魚**
- **保護自己**

網絡釣魚

概述

電子郵件是我們溝通的主要方式之一。我們不僅用它每天的工作，還用它與我們的朋友和家人保持聯繫。除此之外，　電子郵件是現在大多數企業提供在線服務的途徑，如確認您的網上銀行對賬單購買或可用性。由於世界各地這麼多的人依賴於電子郵件，它已成為網絡罪犯使用的主要攻擊手段之一。在本月刊，我們將解釋網絡釣魚，一個常見的電子郵件攻擊方法，並採取安全地使用電子郵件的步驟。

編輯嘉賓

Lance　Hayden博士是Berkeley大學研究小組的董事總經理。是安全文化和行為方面的專家，　他就是”　以人為本的安全：將您的企業安全文化”(McGraw-Hill出版)的筆者。您可以在www.linkedin.com/in/drhayden找到他。

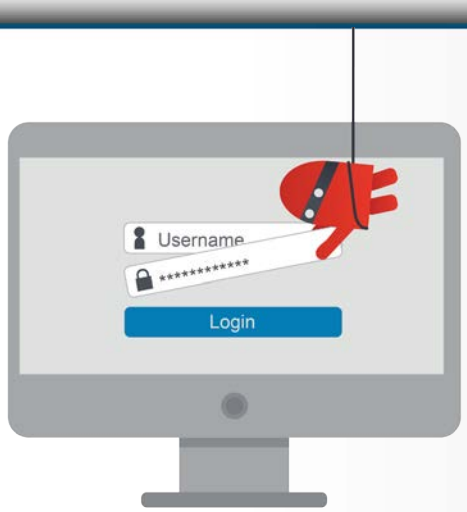
網絡釣魚

網絡釣魚是指使用電子郵件或短信服務，如社交媒體網站的攻擊技巧，或騙您採取行動，如點擊鏈接或打開附件。這種攻擊的犧牲品是您的高度敏感信息被盜和/或您的電腦被感染。攻擊者努力使自己的釣魚郵件有說服力。例如，他們將他們的電子郵件看起來像是來自您知道某人或您知道的東西，如朋友或您經常使用值得信賴的公司。他們甚至會加銀行的標誌或偽造的電子郵件地址，以便消息看起來更合法。然後，攻擊者發送這些釣魚郵件給以百萬計的人。他們不知道誰將會成為受害者，他們所知道的是更多的電子郵件就會有更大的機會獲得成功。網絡釣魚是類似於使用漁網捕魚，您不知道誰會落網，　但是您越大的網會有越多的魚。有幾種攻擊者利用網絡釣魚來獲得他們想要的東西的方法。

- **收集信息**：攻擊者的目標是要收穫您的個人信息，如密碼，信用卡號碼或銀行信息。要做到這一點，他們向您發送電子郵件的鏈接看起來像是合法的網站。然後要求您提供您的帳戶信息或個人信息。但該網站是假的，您輸入的所有信息將直接給攻擊者。

網絡釣魚

- **惡意鏈接**: 攻擊者的目標是控制您的設備。要做到這一點, 他們向您發送電子郵件的鏈接。如果您點擊鏈接, 它把您帶到一個網站, 啟動對您的設備的攻擊, 如果成功的話, 會感染您的系統。
- **惡意附件**: 攻擊者的目標是相同的, 感染並控制您的設備。但是, 不是通過一個鏈接, 攻擊者發電子郵件給您附帶一個被感染的文件, 如Word文檔。您打開附件觸發攻擊, 這可能使您的系統被攻擊者控制。
- **騙局**: 還有一些釣魚郵件是數碼騙子。他們試圖說您中獎了, 或假裝是一個慈善需要捐贈或詢問您的幫助來挪用數百萬美元。如果您有所反應, 他們會說, 他們首先需要支付他們的服務費或訪問您的銀行帳戶, 欺騙您出錢。



您最好的防守就是常識。如果電子郵件或消息是奇怪的, 可疑的或好得不似真實的, 它可能是一個釣魚攻擊。

保護自己

在幾乎所有情況下, 打開和閱讀電子郵件或消息是沒問題的。對於釣魚攻擊, 壞人是需要誘騙您做一些事情。幸運的是攻擊是有線索的, 這裡是最常見的:

- 電子郵件產生一種緊迫感, 要求如不 “立即採取行動”, 將會有壞事發生, 如關閉您的帳戶。攻擊者要趕您沒有時間思考而犯錯誤。
- 您收到一封您沒有想到的電子郵件, 誘您打開附件。例子包括一封電子郵件, 它有一個附件關於突擊裁員, 員工工資信息。或來自稅務局一封信, 說您被起訴的細節。
- 不要使用您的名字, 電子郵件使用一個通用的稱呼, 如 “尊敬的客戶”。大多數公司或朋友需要聯繫您都知道您的名字。
- 電子郵件請求高度敏感的信息, 如信用卡號或密碼。

網絡釣魚

- 電子郵件說, 它來自一個官方組織, 但語法或拼寫差, 或者使用類似@ gmail.com, @ yahoo.com或@ hotmail.com個人電子郵件地址。
- 鏈接看起來很奇怪或不正式。一個技巧是將鼠標懸停在鏈接上， 等到一個指示彈出告訴您該鏈接真正會接到 哪裡。如果彈出的指示與電子郵件中的鏈接不匹配, 不要點擊它。在移動設備上用您的手指上按住鏈接會得到相同的彈出式窗口。一個更安全的步驟是複製, 然後從電子郵件中的URL粘貼到瀏覽器或鍵入正確的鏈接。
- 您收到來自您認識的人的消息, 但語氣和措辭聽起來並不像他或她。如果您懷疑, 請打電話給發件人確認是來自他們。這是很容易的網絡攻擊, 攻擊者創建看似來自朋友或同事的電子郵件。

如果您認為電子郵件或消息是網絡釣魚攻擊, 只需將其刪除。最終, 常識是您最好的防禦。

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

社會工程:	https://www.securingthehuman.org/ouch/2014#november2014
五個步驟保證安全:	https://www.securingthehuman.org/ouch/2014#october2014
我被黑客攻擊， 現在該怎麼辦？:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard在線:	https://www.onguardonline.gov/phishing
每日SANS安全提示:	https://www.sans.org/tip_of_the_day.php

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