SANS SECURITY AWARENESS

OUCH!

全民資訊安全意識月刊

網路釣魚，止於智者

概述

電子郵件和訊息傳遞服務（如Skype, Twitter或Snapchat）已成為現今重要的溝通方式。我們不但每天都會在工作上使用到這些科技，也會用於與朋友和家人保持聯繫。由於全世界許多人都相當依賴這些科技服務，它們已成為網路攻擊者的主要攻擊手段之一，也被稱之為網路釣魚。不管是在職場或家庭，我們都應了解什麼是網路釣魚，以及如何發現並預防這些攻擊。

什麼是網路釣魚?

網路釣魚是一種使用電子郵件或訊息傳遞服務來誘騙您做出錯誤行動的網路攻擊，例如點擊惡意連結、騙取您的密碼或打開受感染的電子郵件附件。攻擊者寄送的假訊息會用各種方式讓它彷彿是真的，並會運用其中撩人心弦的關鍵因素，例如緊急情況或好奇心。這些有問題的訊息會被包裝成看起來像來自某些您認識的人事物，例如經常連絡的朋友或值得信賴的公司。他們甚至可能會加上銀行標誌或偽造電子郵件地址，以使郵件看起來更加合理。攻擊者會將這些偽造的訊息發送給數百萬人。其實攻擊者不知道誰會上鉤，但只要發出越多的釣魚訊息，就會有越多人成為受害者。

如何保護自己

在大部份情況下，開啟和閱讀電子郵件或訊息是安全的。但為了使釣魚攻擊發揮作用，攻擊者會誘騙您做某些事。所幸攻擊行為通常是有跡可循，下面列舉出目前常見的手法:

- 營造出高度緊迫感，要求「立即採取行動」以免發生不良事件，如威脅要關閉帳號或將您送入監獄。攻擊者意圖讓您在未經冷靜思考下做出錯誤行為。
- 迫使您跳過或省略工作中原本應被執行的政策或程序。
- 引發強烈的好奇感或令人難以置信得到天上掉下來的禮物（但您其實並沒有贏得樂透）。

- 使用像是「親愛的顧客」來稱呼您。絕大多數與您聯繫的公司或朋友都應該知道您的名字。
- 請求提供高度敏感的資訊，例如信用卡號碼或密碼；或是正常來說，發件人應該早就知道的任何其他資訊。
- 顯示來自官方組織的訊息，但文法或拼寫有誤差；或使用@ gmail.com等個人電子郵件地址。
- 看似來自公司的電子郵件（例如您的老闆），但回信地址卻是某人的個人電子郵件帳戶。
- 訊息來自您認識的人，但語氣或措辭聽起來根本不像他。如果您不確定真假，請向寄件人確認他們是否寄送了該郵件，因為網路攻擊者很容易就能創建看起來是來自朋友或同事的消息。

總而言之，具備相關常識通常是最好的自保方式。如果電子郵件或消息看起來很古怪，或像是天上掉下來的禮物，請先合理懷疑已遭到網路釣魚攻擊。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站http://www.tsc-tech.com/或臉書@tsctech了解更多訊息。

客座編輯

Tonia Dudley自2011年起開始發起倡導資安認知的相關活動，包含曾創立一項得獎的網路釣魚訓練計畫。可以在www.linkedin.com/in/toniadudley關注她的消息。

參考資料

社會工程:	https://www.sans.org/u/Cb1
幫助他人自我保護:	https://www.sans.org/u/Cb6
電子郵件，行所當行，止所當止:	https://www.sans.org/u/Cbg
CEO欺詐:	https://www.sans.org/u/Cbl
OUCH！翻譯和檔案:	https://www.sans.org/u/Cbq

授權