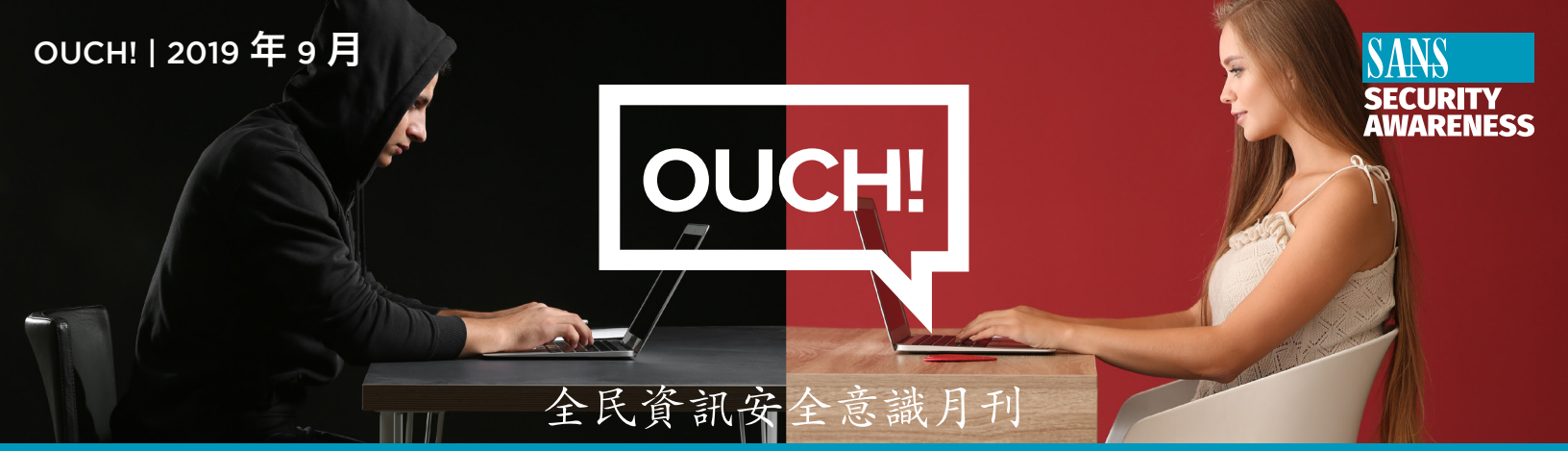

社群媒體詐騙

概述

我們大多都曾經在工作環境或家中遇過網路電子郵件釣魚攻擊。這些電子郵件看起來正常，像是來自您的銀行、長官或最喜歡的線上購物網站的郵件。然而，這其實是一種攻擊行為，試圖促使或欺騙您做出不該做的行為，例如打開電子郵件中受感染的附件，公開密碼或轉帳。我們面臨的挑戰是，越是有能力識別出這些電子郵件和阻止攻擊，網路犯罪分子便嘗試越多的方式欺騙人們。

從Skype、WhatsApp和Slack到Twitter、Facebook、Snapchat、Instagram甚至是遊戲應用程式，幾乎任何您使用的通訊形式都可能發生嘗試欺騙或愚弄您的行為。透過這些平台或管道進行交流讓人感覺更加輕鬆或受信任，這正是攻擊者利用它們欺騙他人的原因。此外，拜今日的技術所賜，世上各處的任何攻擊者都可以輕易地假裝成任何他們想要的人事物。重要的是要記住：那些您收到的通訊，可能都不如其表面所示，聯絡人也不一定就是本人。

關鍵重點

以下常見線索可能表示您剛剛收到的訊息或閱讀的文章是一次攻擊。

緊急性：一則具有緊迫感的訊息，要求在發生危機事件之前「立即行動」，例如威脅關閉您的帳戶或將您送進監獄。攻擊者想要促使您犯下錯誤。

壓力：迫使您繞過或忽略職場的政策或程序。

好奇心：強烈的好奇心或者好得難以置信的事物。不，您沒有中樂透。

敏感: 要求提供高度敏感的資訊, 例如您的信用卡帳號或密碼, 或者是您在分享時覺得有點怪怪的任何資訊。

官方訊息: 訊息中自稱來自官方機構, 但語法或拼寫很差。大多數政府機關與您的正式聯絡不會經由社群媒體。如果您不確定該郵件是否正當, 請聯絡該機關, 但要使用來源可信的電話號碼, 例如官網。

假冒: 當您收到來自朋友或同事的訊息, 但語氣或措辭聽起來並不像他們。如果您有疑慮, 直接打電話給寄件人以確認他們是否曾發送郵件。網路攻擊者很容易就能建立看似來自您認識的人的郵件。在某些情況下, 他們可以控制您的朋友的帳號, 然後偽裝成您的朋友與您聯繫。要特別注意簡訊、Twitter和其他簡短的訊息內容, 因為其更難以察覺發送者的特徵。

您是對抗這些詐騙、圈套和攻擊的最好防禦。若是貼文或訊息看起來很奇怪或可疑, 儘管忽略或刪除它; 如果訊息來自您認識的人, 請打電話確認是否真的是他們發送的。

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

Jessica Barker博士 (@drjessicabarker) 是一位有關網路安全人為面向的領導者。她同時是Cygenta的聯合執行長, 熱衷於積極影響全球的網路安全意識、行為和文化。她是ClubCISO的主席, 也是一位受歡迎的主題演講者。

參考資源

社交工程: https://www.sans.org/u/Uz6
電話詐騙攻擊: https://www.sans.org/u/Uzb
網路釣魚, 止於智者: https://www.sans.org/u/Uzg
個製化詐騙: https://www.sans.org/u/Uzl

編輯委員會: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | 翻譯群: 宋亞倫、顧君毅、葉力維、戴興望、李彥鋒

TSC 海航 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region