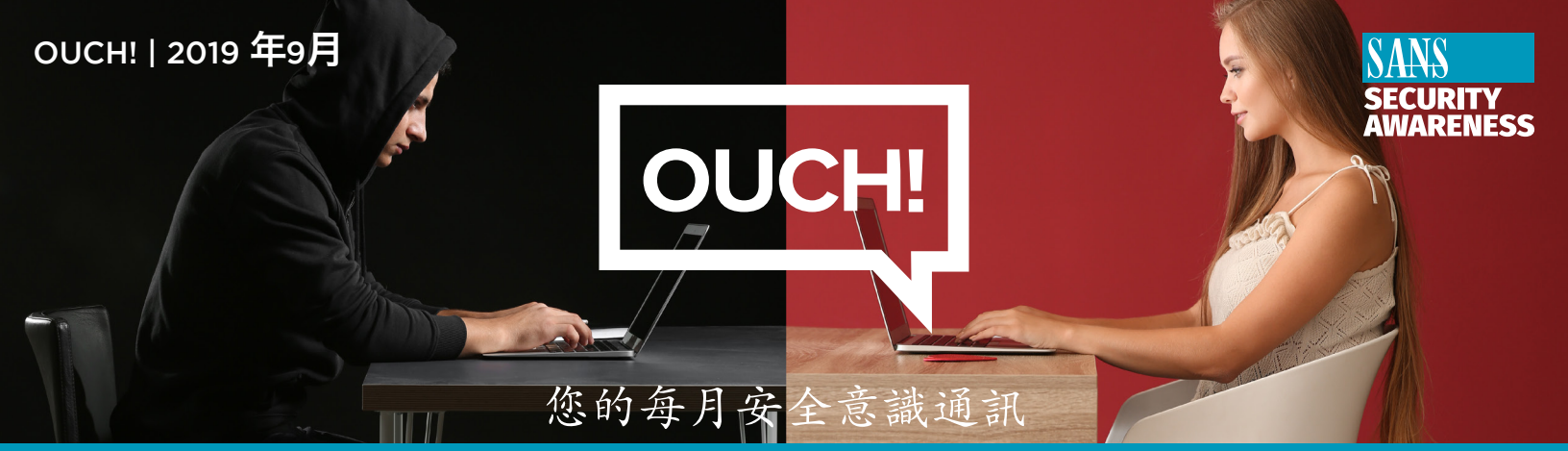

通過社交媒體欺騙您

概觀

我們中的許多人在工作或家中都收到了網絡釣魚電子郵件攻擊。這些是看起來合法的電子郵件，例如來自您的銀行，老闆或您最喜歡的在線商店。然而，這些確實是一種攻擊，試圖催您或欺騙您採取您不應該採取的行動，例如打開受感染的電子郵件附件，共享密碼或轉賬。困難的是，我們越是明智地發現和阻止這些電子郵件攻擊，越多的網絡犯罪分子會嘗試其他聯繫方式欺騙我們。

嘗試欺騙您可能發生在您使用的幾乎任何形式的通信上，從Skype，WhatsApp和Slack到Twitter，Facebook，Snapchat，Instagram甚至遊戲應用程序。通過這些平台或渠道進行溝通交流感覺更加非正式或值得信賴，這正是攻擊者利用它們欺騙他人的原因。此外，通過今天的技術，世界上任何地方的任何攻擊者都可以更容易地假裝成任何他們想要的東西或假裝成者任何人。所以您一定要記住，任何對您的溝通可能都不像他們看起來那樣，並且聯絡方不一定是他們看起來像是誰那樣。

關鍵要點

以下是您剛剛收到的消息或您剛剛閱讀的帖子有可能是攻擊的最常見線索。

緊急性: 一種具有緊迫感的信息，要求在發生不良事件之前採取“立即行動”，例如威脅關閉賬戶或將您送進監獄。攻擊者想要惹您犯錯誤。

壓力;迫使您繞過或忽略工作中的政策或程序。

好奇心: 強烈的好奇心或者太好的事情, 別好奇了, 您沒有贏得彩票。

敏感: 要求提供高度敏感的信息, 例如您的信用卡號或密碼, 或者您不願意共享的任何信息。

官方消息: 消息稱它來自官方組織, 但語法或拼寫很差。大多數政府組織不會直接與您使用社交媒體進行官方通信。如果您不確定該郵件是否合法, 可以回复該組織, 但一定要使用可信賴的電話號碼, 例如用其網站上的電話號碼。

假冒: 您收到來自朋友或同事的消息, 但語氣或措辭聽起來並不像他們。如果您有疑問, 請致電發件人以確認他們是否發送該郵件。網絡攻擊者很容易創建看似來自您認識的人的郵件。在某些情況下, 他們可以入侵您朋友的一個帳戶, 然後偽裝成您的朋友並與您聯繫。要特別注意短信, Twitter和其他簡短的信息方式, 這會更難以看得出發送者的個性。

您是對抗這些詐騙, 欺騙和攻擊的最好防禦。如果帖子或消息看起來很奇怪或可疑, 只需忽略或刪除它, 或者如果它來自您認識的人, 請打電話給該人確認他們是否真的發送過信息。

客座編輯

Jessica Barker博士 (@drjessicabarker) 是人性方面的網絡安全的領導者。她是Cygenta的聯合首席執行官, 她熱衷於積極影響全球的網絡安全意識, 行為和文化。她是ClubCISO的主席, 也是一位受歡迎的會議主題發言人。

參考資料

社會工程: https://www.sans.org/u/Uz6
電話詐騙: https://www.sans.org/u/Uzb
制止網絡釣魚: https://www.sans.org/u/Uzg
個性化詐騙: https://www.sans.org/u/Uzl