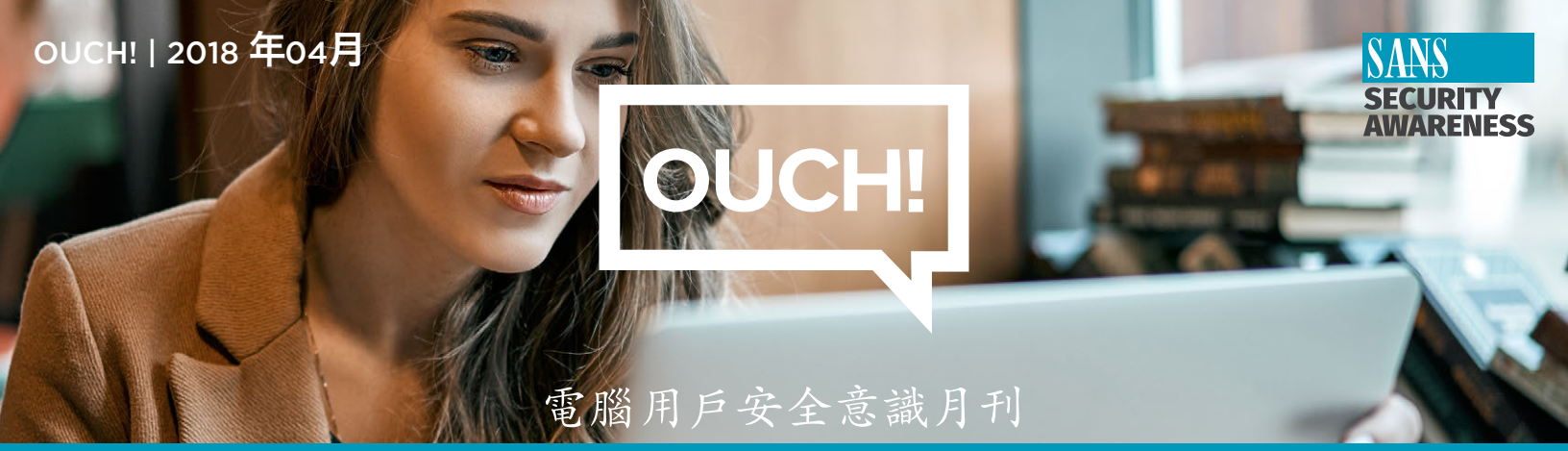

SANS SECURITY AWARENESS

OUCH!

電腦用戶安全意識月刊

阻止網絡釣魚

概觀

電子郵件和消息服務 (如Skype, Twitter或Snapchat) 是我們溝通的主要方式之一。我們不僅每天都使用這些技術來工作, 還要與朋友和家人保持聯繫。由於世界各地的許多人都依賴這些技術, 因此它們已成為網絡攻擊者所使用的主要攻擊手段之一, 這是一種被稱為網絡釣魚的攻擊手段。了解什麼是網絡釣魚, 以及如何發現和阻止這些攻擊, 無論您是在工作還是在家。

什麼是網絡釣魚?

網絡釣魚是一種攻擊類型, 它使用電子郵件或消息傳遞服務欺騙您採取不應該採取的措施, 例如點擊惡意鏈接, 共享密碼或打開受感染的電子郵件附件。攻擊者會努力使這些信息令人信服, 並挖掘您的情緒觸發因素, 如緊迫感或好奇心。他們可以使這些信息看起來像來自某人或某些您認識的人, 例如您的朋友或值得信賴的公司。或者, 他們甚至可能會添加銀行商標或偽造電子郵件地址, 以使郵件顯得更加合法。攻擊者然後將這些消息發送給數百萬人。他們不知道誰會上當, 但是他們知道發送的越多, 就越會有人成為受害者。

保護自己

在多數所有情況下, 打開和閱讀電子郵件或消息都很沒有問題。為了使釣魚攻擊發揮作用, 壞人需要誘騙您做某件事。幸運的是, 有些是攻擊的線索, 這是最常見的:

- 極度緊迫感, 在發生不良事件前要求“立即採取行動”, 如威脅要關閉賬戶或將您送入監獄。攻擊者想要讓您誤入歧途。
- 迫使您繞過或忽略您的工作中的政策或程序。

- 強烈的好奇感或者太好以至於不真實（不，您沒有贏彩票）。
- 像“親愛的顧客”這樣的普通稱呼。大多數與您聯繫的公司或朋友知道您的名字。
- 請求高度敏感的信息，例如您的信用卡號碼或密碼或合法發件人應該知道的任何其他信息。
- 該消息表示它來自官方組織，但語法或拼寫較差，或使用@ gmail.com等個人電子郵件地址。
- 郵件來自官方電子郵件（例如您的老闆），但回复地址是至某人的個人電子郵件帳戶。
- 您收到來自您認識的人的消息，但語氣或措辭聽起來不像他或她。如果您懷疑，請致電發件人以確認他們發送了該郵件。網絡攻擊者很容易創建好像是來自朋友或同事的消息。

最終，基本的常識是您最好的防守。如果電子郵件或消息看起來很古怪，可疑或太好，那可能是一種網絡釣魚攻擊。

客座編輯

Tonia Dudley自2011年以來一直在開發和運行安全意識計劃，其中包括建立一個屢獲殊榮的網絡釣魚培訓計劃。您可以在www.linkedin.com/in/toniadudley找到她。

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
電子郵件做與不做:	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

執照