帳號劫持：情感掠食者

措手不及：艾瑪的故事

艾瑪正在瀏覽 Facebook 時，看到她的表姊莎拉發佈了一則感人的貼文。貼文分享了一則令人心碎的消息：莎拉年邁的父親已搬進養老院，並正在出售他的東西來幫助支付醫療費用。其中包含了一些物品的照片，像是他的汽車、珠寶和古董家具，價格低得令人難以置信。

想要幫忙並撿個便宜，艾瑪立刻透過 Facebook Messenger 聯絡莎拉，這是她們多年來首次對話。莎拉很高興收到表妹的訊息，並向艾瑪更新了父親的近況。莎拉很快將話題轉向付款細節，催促艾瑪儘快行動，因為許多物品已經有人預訂了。艾瑪立刻匯出款項，卻在之後才發現整則貼文竟是一場詐騙。

艾瑪根本不是在與她的表姊對話。莎拉的 Facebook 帳號已被駭客入侵，並被詐騙者接管。在完全取得帳號存取權後，詐騙者發布了有關莎拉父親的假消息，並假冒出售他的物品，利用莎拉信任的朋友和家人網絡進行詐騙。當人們以為自己是在向莎拉購買物品（並支持她的父親）時，實際上他們是在把錢交給詐騙者，後者隨即帶著他們的錢消失。

發生了什麼事？

詐騙者正透過破解使用者名稱和密碼，劫持像是Facebook或Instagram等平台上的社交媒體帳號。一旦取得帳號，他們會冒充帳號擁有者，分享假的貼文，這些貼文通常包含情緒化細節，以製造緊迫感並驅使人們採取行動。這些詐騙通常包含像是在某個城市遭遇搶劫需要幫助，或是發生車禍需要金錢，或者親人過世且他們的物品正在被賣掉的故事。

受害者會被吸引進來，因為他們相信這些貼文來自他們認識並信任的人。他們會透過無法追蹤的方式付款，如P2P應用程式或匯款，但之後會發現自己並非與家人或朋友交易，而是上當受騙，且錢財已經不見。

這類詐騙為何如此危險？

- **被劫持的信任**：詐騙者利用他們劫持的社交媒體帳號所擁有的信任網絡。貼文看起來來自信任的朋友或家人，使其更具說服力。
- **操弄情感**：**詐騙者利用個人和情緒話題，這些話題常常營造出強烈的緊迫感或機會，迫使人們最終做出錯誤的決定。**
- **快速傳播**：一旦受害者的帳號遭到入侵，詐騙者可以迅速聯繫到數百甚至數千人。此外，許多人在多個社交媒體帳號上使用相同的密碼，因此一旦其中一個帳號被劫持，該密碼就可以用來控制受害者的其他社交媒體帳號。

如何保護自己和他人

- **對於涉及金錢的情感性貼文保持懷疑態度**：如果一則貼文看起來異常情緒化或緊急，並涉及匯款給某人，請先暫停並查證，這可能是詐騙。
- **直接向對方驗證**：透過其他管道聯繫對方以確認故事的真實性。例如，可以打電話給他們或與他們當面交談。許多時候，受害者甚至不知道自己的帳號已經被劫持，也不知道詐騙者在他們的帳號上發布了詐騙貼文。
- **檢查警訊**：詐騙者經常要求以無法追蹤的方式付款，像是點數卡或比特幣。另一個警訊是他們要求您轉換平台繼續聯絡（例如從Facebook Messenger轉移到WhatsApp）。
- **保護您的帳號：**如果您的帳號被駭客劫持，網路犯罪分子通常會做的第一件事就是更改您的密碼，將您鎖定在外。一旦發生這種情況，恢復您的帳號將變得非常困難。從為每個帳號設置長且獨特的密碼開始保護自己。接著，為每個帳號啟用多因子驗證。這兩個簡單的步驟能大大提升帳號的安全性，詐騙者會因為這樣而恨您！

保持領先一步

面對帳號劫持詐騙，您就是自己最好的防禦。如果您懷疑自己遭遇了這種詐騙，請立即舉報該帳號並通報您的社交媒體平台。

客座編輯

Amie Dsouza 是一位在美國主要航空公司工作的資安專業人士。她曾在六個國家工作，並擔任WiCys的董事會成員。Amie 積極倡導教育每個人如何在網路上保護個人資料的安全。

參考資源

觸發情緒—網路攻擊者如何欺騙您：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt89db29f2df44dc94/63487f29885d1d218e485bd6/ouch!_october_2022_chinese_(Traditional_Taiwan)_emotional_triggers.pdf
揭露陰影：網路犯罪分子如何竊取您的密碼：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt9e4565bca6440027/673de041d1cb3b38f7e35a23/ouch!_chinese_(Traditional_Taiwan)_december_2024_credential_harvesting.pdf
密詞之力：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt848a55a198b7bb59/655518f625f479dc94d44a8b/ouch!_december_2023_chinese_(Traditional_Taiwan)_power_of_the_passphrase.pdf
被駭了怎麼辦？：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt5261dc118f7a80b4/6530346fff2cf7ab8799ae1c/ouch!_november_2023_chinese_(traditional_taiwan)_im_hacked_now_what.pdf

社群翻譯：宋亞倫 德欣寰宇科技股份有限公司

OUCH!是由美國系統網路安全研究協會（SANS Security Awareness）發行，遵從創意公用授權條款4.0版(Creative Commons BY-NC-ND 4.0)。在不更改本刊物內容或出售的前提下，您能夠自由分享及發佈此月刊。編輯委員會：Walter Scrivens、Phil Hoffman、Alan Waggoner、 Leslie Ridout、Princess Young。