網路攻擊鎖定您的三大方式

概述

社交工程攻擊是網路攻擊者常用的一種手法，他們利用欺詐手段誘使人們做出不應該做的事情。這個概念已被詐欺犯和騙徒使用了數千年。最新的狀況是，網際網路讓全球任何一個地方的網路犯罪分子都能輕易地偽裝成他們想要的任何人，並針對任何他們想要的目標進行攻擊。以下是網路攻擊者常用的三種社交工程方法，他們試圖利用這些方法來誘騙您。

網路釣魚 （Phishing）

網路釣魚是最傳統的社交工程攻擊方式，當網路攻擊者發送電子郵件給您，試圖欺騙您採取不應該採取的行動時，就屬於這種攻擊。最初稱為網路釣魚是因為它就像在湖中釣魚一樣：您投出一條釣線和鉤子，但不知道會釣到什麼。這種手法背後的策略是網路犯罪分子發送的網路釣魚郵件越多，受害者就越多。如今的網路釣魚攻擊變得更加複雜和具針對性（有時被稱為魚叉式網路釣魚），網路攻擊者常常在發送前量身打造釣魚郵件。

簡訊釣魚 （Smishing）

Smishing是基於簡訊的釣魚攻擊，而不是電子郵件。網路攻擊者會使用應用程式，像是iMessage、Google Messages或WhatsApp，向您的手機發送簡訊。簡訊釣魚變得流行有幾個原因。首先，過濾簡訊比過濾電子郵件攻擊要困難得多。其次，網路攻擊者發送的訊息通常非常簡短，這意味著幾乎沒有上下文，這使得判斷訊息是否合法很困難。第三，簡訊通常更加隨興及動態，因此人們習慣於快速回覆或動作。最後，人們越來越能夠辨識釣魚電子郵件攻擊，因此網路攻擊者簡單地換了一種新的方法—簡訊。

語音釣魚（Vishing）

Vishing，或稱語音詐騙，是一種利用撥打電話或語音訊息而不是電子郵件或簡訊的策略。語音釣魚需要攻擊者花費更多時間來執行，因為他們直接與受害者交談並互動。然而，這類型的攻擊也更有效，因為通過電話創造強烈情緒，如迫切感，要容易得多。一旦一名攻擊者開始與您通話，他們將不會讓您掛斷電話，直到他們得到想要的。

識別和阻止攻擊

幸運的是，無論攻擊者使用三種方法中的哪一種，都有一些常見的線索可以辨識：

- **迫切性**：任何讓您感到非常急迫的訊息，攻擊者試圖催促您迅速採取行動並犯下錯誤。例如，一則假冒來自政府機關的訊息聲稱您逾期繳稅，如果您不立即支付，將會被送進監獄。
- **壓力**：**任何施加壓力，要求員工忽略或規避公司安全政策和程序的訊息。**
- **好奇**：任何引起極大好奇心或看似過於美好的訊息，例如未投遞的UPS包裹或收到亞馬遜退款通知等，都可能是假的。
- **語氣**：**任何看似來自您認識的人，如同事，但措辭不像他們，整體語氣或簽名不正確的訊息。**
- **敏感資訊**：任何要求非常敏感資訊的訊息，例如您的密碼或信用卡資訊。
- **通用**：一封來自信任組織的訊息，但使用通用的稱呼，如「親愛的顧客」。如果亞馬遜有包裹送給您，或者電話服務有帳單問題，他們會知道您的姓名。
- **個人電子郵件地址**：任何看似來自合法組織、供應商或同事的電子郵件，但使用個人郵件地址，如 @gmail.com 或 @hotmail.com。

尋找這些常見線索，您能夠最大程度的保護自己。

客座編輯

瑪麗·簡·蘇亞雷茲·帕坦（Mary Jane Suarez Partain）是網路安全女性（WiCyS）的計畫主管。她的職務重點是提供資源、倡議和計畫，旨在網路安全領域招募、留住和推動女性。她熱衷於打造一個包容的環境，讓所有人感受到被重視、受歡迎和被看見的重要性。

參考資源

阻止電話詐騙：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt34ab9c85009af1bb/64933658d40ad010436827f0/ouch!_july_2023_chinese_(Traditional_Taiwan)_stop_those_phone_call_scams.pdf
日漸棘手的網路釣魚攻擊：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltfc2ad8cb2ede245b/62b245cfbc32396c52cd7679/ouch!_july_2022_chinese_(traditional_taiwan)_phishing_attacks_are_getting_trickier.pdf
觸發情緒—網路攻擊者如何欺騙您:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltfc2ad8cb2ede245b/62b245cfbc32396c52cd7679/ouch!_july_2022_chinese_(traditional_taiwan)_phishing_attacks_are_getting_trickier.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

翻譯：宋亞倫 德欣寰宇科技股份有限公司