SANS SECURITY AWARENESS

OUCH!

全民資訊安全意識月刊

電話詐騙攻擊

概述

當提到網路犯罪份子時, 大多數人可能會聯想到有個邪惡的策劃者坐在電腦後面發起一連串複雜的網路攻擊。儘管許多網路犯罪份子使用電子郵件或即時通訊軟體之類的技術攻擊, 但壞人也會利用電話誘騙受害者。使用電話有兩大優勢: 首先, 與電子郵件不同的是, 能夠監控電話並偵測阻止攻擊的防護技術比較少; 其次, 透過電話表達情感要容易得多, 這使得壞人更有機會誘騙受害者。我們接下來將學習如何發現和阻止這些攻擊。

電話攻擊如何運作

首先, 必須了解這些攻擊者的目的: 他們通常要的是您的錢、個人資訊或侵入您的電腦 (也可能以上皆是) 。他們會誘騙做出他們想要您做的事以達目的。電話攻擊對象涵蓋全世界, 通常會營造似乎非常緊急的情境。他們希望您被嚇到而不知所措, 在缺乏清楚思緒的情況下, 促使犯下錯誤。一些常見的例子包括:

來電者假裝是政府稅務部門或稅務服務機構, 告知您有未付的稅款。來電者聲稱若不立即支付稅款, 您將會被判刑入監, 而迫使您用信用卡電話支付。這完全是個騙局, 包括國稅局在內的許多稅務部門都不會以電話或電子郵件進行聯絡。所有官方稅務通知皆是以正常郵件發送。

來電者假裝是Microsoft技術支援人員, 並宣稱您的電腦已受到感染。一旦您相信了對方的說詞, 接下來對方就會催促您購買他們的軟體或者要求遠端登入您的電腦權限。請留意: 微軟不會打電話給您。

您可能會收到一則語音訊息, 通知您的銀行帳戶已被取消, 必須撥打另一個號碼以重新啟動。撥通後則是一個自動語音系統, 要求確認您的身份, 並且詢問各種私人問題。事實上, 這不是您的銀行所為, 壞人只是藉此記錄您的個資以盜用身份。

如何保護自己

防範電話詐騙攻擊最有效的方法是由自己本身做起，請記住以下事項:

不論何時何人，只要在來電中營造了強烈的急迫感，試圖迫使您去做一些事情，請對此抱持高度懷疑。即使通話內容起初還算合理，但之後只要感到任何不對勁，可以隨時停止交談。

如果您覺得已接到詐騙電話，只要掛斷通話就好。如果想確認來電內容的真實性，請在對方的官方網站（例如您的銀行）查詢客服電話號碼並直接打過去確認。這樣就能確定對方通話者的身份是正確無誤。

請千萬不要相信來電顯示。壞人通常會偽裝來電的號碼，讓它看起來像是正常來源或者與您的電話號碼具有相同的區號。.

絕對不要讓來電者有任何機會控制您的電腦或誘騙您下載軟體。這都是壞人讓電腦受到感染的方法與途徑。

如果接到陌生來電，請直接將電話轉到語音信箱，如此一來，您可以利用自己的餘裕時間查看未知來電。更方便的是，許多手機可以設定「請勿打擾」功能，預設啟用轉接語音信箱。

電話詐騙攻擊事件與日俱增，自己提高警覺往往是最有效的偵測和阻止攻擊防禦措施。

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

Jen Fox在All Covered擔任資深安全顧問，提供安全認知、社交工程防護和風險評鑑服務。可以在Twitter以@j_fox找到Jen Fox。

資源

防詐騙專線（臺灣內政部警政署）：	165
全民防騙網（臺灣內政部警政署）：	https://www.165.gov.tw/
社交工程攻擊:	https://www.sans.org/u/Fi5

編輯委員會：Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 翻譯群：黃意雯、宋亞倫、顧君毅、孫權劭、葉力維、莊銘輝

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