

OUCH!

您的資訊安全意識月刊。

識別並阻止簡訊攻擊

什麼是簡訊攻擊？

Smishing（簡訊和網路釣魚的結合詞）是網路攻擊者使用簡訊、文字訊息或類似的傳訊功能誘使您做出不應該採取的行動的攻擊。他們也許會欺騙您提供信用卡的詳細資料，讓您撥打電話號碼以取得銀行資訊，或者說服您填寫線上問卷以獲取您的個人資料。和電子郵件網路釣魚攻擊一樣，網路犯罪份子經常利用您的情緒來讓您採取行動，例如製造緊迫感或激起好奇心。然而，使簡訊攻擊如此危險的原因在於，與電子郵件相比，文字訊息中的資訊和線索要少得多，這使您更難發現有問題。

有一種常見的騙局：一則告訴您贏得了 iPhone 的訊息，您只需要點擊一個連結並填寫問卷即可領取。實際上，沒有中獎手機，問卷的目的是收集您的個人資料。另一個例子：一則說明無法遞送包裹的訊息，並附有導向網站的連結，該網站要求您提供完成遞送所需的資訊，包括支付「服務費」的信用卡詳細資料。在某些情況下，這些網站甚至可能會要求您安裝未經授權的行動應用程式，以感染並接管您的裝置。

有時，網路犯罪份子甚至會結合電話和簡訊攻擊。例如，您可能會收到銀行發來的緊急簡訊，詢問您是否授權一筆異常付款。該簡訊要求您回覆「是」或「否」以確認付款。如果您回覆了，網路犯罪份子現在知道您願意行動，並會假裝成銀行的詐欺部門打電話給您。然後，他們會試圖說服您交出您的財務和信用卡資訊，甚至是您的銀行帳戶登入名稱和密碼。

識別和阻止簡訊攻擊

以下是一些您能自問的問題，以找出簡訊攻擊最常見的蛛絲馬跡：

- 該訊息是否會產生強烈的緊急感，試圖催促或迫使您採取行動？
- 該訊息是否會將您帶到要求您提供個人資料、信用卡、密碼或其他不應被外人取得的敏感資訊的網站？
- 訊息內容棒得讓人難以置信？不，您並沒有真的免費贏得一支新 iPhone。
- 連結的網站或服務是否會強制您使用非標準方式（例如比特幣、禮品卡或西聯匯款）付款？
- 該訊息是否要求您提供發送到您的手機，或由您的銀行應用程式生成的多因子身份驗證碼？

- 這則訊息是否看起來就是來自一個「錯誤的號碼」？如果是這樣，請不要回覆或嘗試聯絡發件人；刪除它就是了。

如果您收到來自官方機構提醒您的訊息，請直接回電該機構。不要使用訊息中包含的電話號碼，而是使用可信任的電話號碼。例如，如果您收到銀行傳來的簡訊，說您的帳戶或信用卡有問題，請從銀行的網站、帳單或金融卡及信用卡背面取得可信任的電話號碼。另外請記住，大多數政府機構，例如稅務或執法機關，絕不會以簡訊與您聯絡，他們只會以傳統郵件與您聯繫。

當面對簡訊攻擊時，您就是自己的最佳防禦。

客座編輯

Jeff Lomas 是拉斯維加斯大都會警察局網路調查小組的警探，教授 SANS SEC487 開源情報收集和分析 (OSINT) 課程。Jeff 調查高科技金融犯罪，包括商業電子郵件入侵、簡訊詐騙、勒索軟體以及複雜的加密貨幣竊盜和洗錢案件。



參考資源

阻止網路釣魚：

[https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt527c2b83f3fc033a/606f39b61609c821964d9cdf/201804-OUCH-April-ChineseTraditional\(Taiwanese\).pdf](https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt527c2b83f3fc033a/606f39b61609c821964d9cdf/201804-OUCH-April-ChineseTraditional(Taiwanese).pdf)

社交工程攻擊：

[https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt5665cdf1e2dd80e4/6048fecc5aedc043351b76ce/OUCH! Nov 2020 - Social Engineering v.3-Chinese \(Traditional Taiwan\).pdf](https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt5665cdf1e2dd80e4/6048fecc5aedc043351b76ce/OUCH! Nov 2020 - Social Engineering v.3-Chinese (Traditional Taiwan).pdf)

釣魚電話—電話攻擊與詐騙：

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt86e9957fde58bb2c/60902abb7b4f5110164a4b39/OUCH-Traditional Taiwan May 2021 - Vishing Phone Call Attacks and Scams v3-English-Chinese.pdf>

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院 Security Awareness 發行，遵從 [Creative Commons BY-NC-ND 4.0\(創意公用授權條款4.0版\)](https://creativecommons.org/licenses/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, Les Ridout, Princess Young.