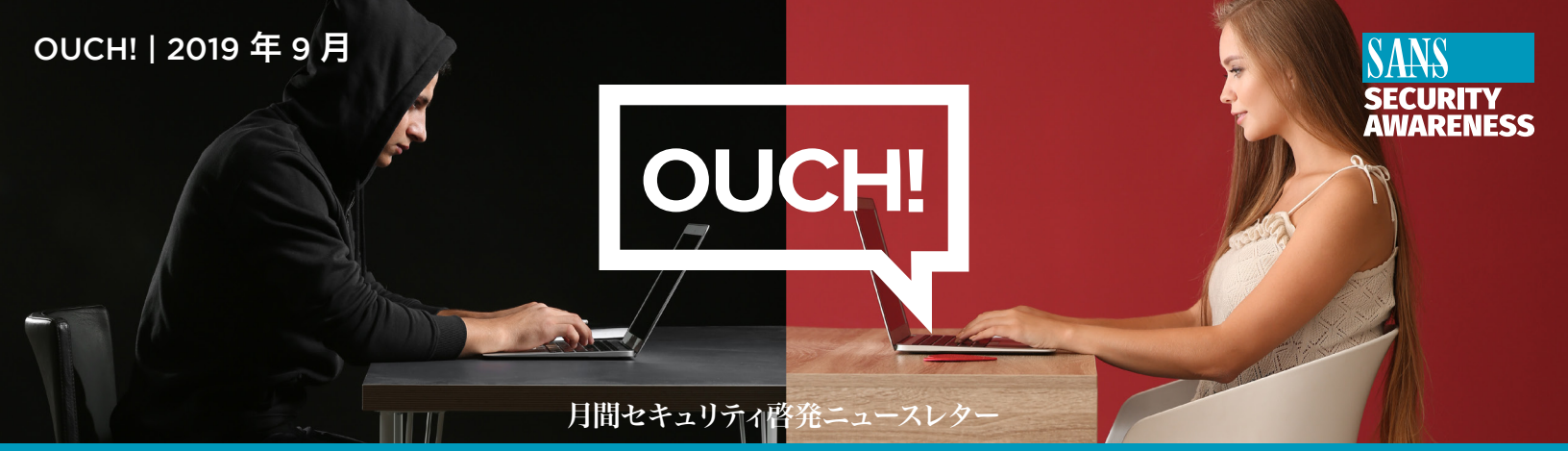

ソーシャルメディアを用いた詐欺

はじめに

私たちの中には、職場や自宅でフィッシングメールによる攻撃を受けたことがあるかもしれません。これらのメールは、銀行や上司・同僚、あるいはよく使うオンラインストアから来た正しいものに思えますが、実際には、マルウェアに感染した添付ファイルを開くように仕向けたり、あなたを急かしたりしながらもパスワードの共有や銀行送金をさせるような攻撃です。悩ましいことに、私たちがメールによる攻撃の検知や防止について詳しくなると、サイバー犯罪者は連絡の取りかたをメール以外の方法に変更したり、別のやり方を試みたりするようになります。

あなたを騙したり罠にかけたりする試みは、SkypeやWhatsApp、Slack、Twitter、Facebook、Snapchat、Instagram、さらにはゲームアプリに至るまで搭載されている様々なコミュニケーションツール上で行われます。これらのプラットフォームやコミュニケーションツールは、電子メールのように形式的なやり取りにはならないことから、警戒心が緩んで相手を身近に感じるようになってしまうため、攻撃者もこれらのツールを攻撃に利用するようになっています。また、最近のテクノロジーを用いることで、世界中のどこからでも誰かになりすますことが容易になりました。このような場合、あなたの元に流れてくるメッセージがいつもとは違う違和感を抱かせたり、通信相手が表示されている人物とは異なったりする可能性があることを覚えておくことが大切です。

重要なポイント

受信したメッセージや目にした投稿が、攻撃である可能性を示す最も一般的なヒントを次に挙げます。

緊急性を謳う：口座の凍結や警察などによる拘束を示唆するなど、悪いことが起こる前に「今すぐに行動する」ように仕向ける緊急性を煽るメッセージであるもの。攻撃者はあなたを急かすことで、間違いが起きることを期待しています。

圧力をかける：仕事上のポリシーや手順を、回避または無視するようあなたに圧力をかけるメッセージであるもの。

好奇心を煽る：好奇心を掻き立てることや、嘘のような出来事が示されたメッセージであるもの。

機微な情報：クレジットカード番号やパスワード、その他のあなたが共有したくないと思うセンシティブな情報を要求するようなメッセージであるもの。

公的機関を騙る：メッセージには公的な機関から送られたものであると書かれていますが、文法が稚拙であったり誤字が目立ったりします。政府機関の大半は、公式なやり取りを個人相手に行う際にソーシャルメディアは使用しません。メッセージが正当なものかわからない場合は、そのメッセージを送付した組織に電話を掛けてみましょう。ただし、電話は該当する組織のウェブサイトに掲載されているような、信頼できる番号に掛けることを心がけてください。

なりすまし：友人や同僚からメッセージを受信したとします。しかしそのトーンや文面が彼らのものには見えない、あるいは違和感を抱いた場合は、送信者やメッセージの発信元である番号に電話を掛けてメッセージを送ったかどうか確認してみましょう。攻撃者にとって、あなたの知人から発せられているかのように見えるメッセージを作成することは、容易なことです。場合によっては、攻撃者はあなたの友人のアカウントを乗っ取り、その友人になりすましてあなたに連絡を取ることも手段としてはあります。テキストメッセージやTwitter、その他の文字数が少ないフォーマットの短文メッセージには特に気をつけてください。これらのメッセージからは、送信者のパーソナリティを詳しく知ることがより困難となります。

言葉巧みな詐欺や甘い言葉による誘惑、そしてこれまでに挙げた攻撃に対する最大の防御はあなた自身です。投稿やメッセージに怪しいと感じる部分がある場合は、単純に無視や削除すればいいでしょう。メッセージの相手が個人的に知っている人からのものである場合は、直接その人に電話を掛け、その投稿やメッセージが本当にその人が発したものであるかを確認するようにしましょう。

ゲストエディタ

ジェシカ・バーカー氏は、（@drjessicabarker）サイバーセキュリティを人間面からアプローチすることに関して世界的な第一人者と言って良いでしょう。バーカー氏はCygenta社の共同創立者であり、サイバーセキュリティに関する啓発や行動、文化について世界中に良い影響を与え続けています。また、彼女はCLUBCISOの代表であり、基調講演をたびたび行う著名なスピーカーとしても名を知られています。

リソース

ソーシャルエンジニアリングについて:	https://www.sans.org/u/Uz6
電話攻撃と詐欺:	https://www.sans.org/u/Uzb
フィッシングを阻止する:	https://www.sans.org/u/Uzg
個人を標的とした詐欺:	https://www.sans.org/u/Uzl

OUCH!はSANS Security Awareness プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。翻訳その他に関しては、www.sans.org/security-awareness/ouch-newsletter までお問合せください Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田　剛