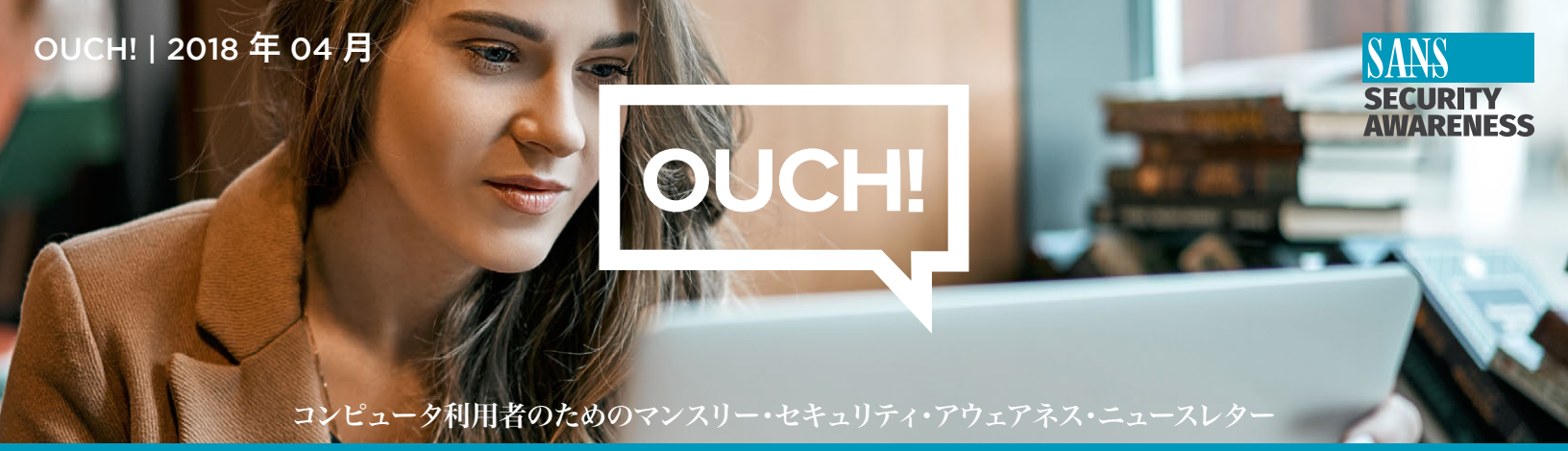

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

フィッシングを阻止する

はじめに

メールやメッセージサービス (例えば、SkypeやTwitter、Snapchat など) は、コミュニケーションを取るための主な手段として現在使われており、これらのテクノロジーは業務上だけでなく、家族や友人間とのコミュニケーションにも利用されています。世界中の人々が、これらのテクノロジーに頼っているため、サイバー攻撃者たちは、これらを悪用した攻撃を多く展開しており、その手法は、フィッシングと呼ばれています。このニュースレターでは、フィッシングとは何かを紹介し、職場、自宅に関わらずフィッシング攻撃を発見、あるいは阻止するための手法を紹介します。

フィッシングとは

フィッシングは、メールやメッセージサービスを使った攻撃で、通常なら取るべきでない行動、例えば悪意あるリンクをクリックする、パスワードを共有する、感染されているメールの添付ファイルを開くなどのアクションを介して、攻撃者がユーザから情報などを騙し取る攻撃手法です。攻撃者は、送付するメッセージに信ぴょう性を持たすために時間を費やして好奇心や緊急性を煽ってくるほか、友人や頻繁に利用する信頼している企業から来ているかのように偽装されます。他には、銀行の口ゴを追加したり、メールアドレスを偽装したりすることで、メッセージをより正規のものに近づけようとします。そして、攻撃者はこのメッセージを大量の人に送りつけるのです。誰が騙されるか分かりませんが、多くの人に送れば送るほど、騙される人が多くなることだけは明らかなようです。

自分自身を保護する

多くの場合、メールやメッセージを開いて、読むことは安全です。フィッシング攻撃が成功するためには、攻撃者はユーザを騙して、何か行動を取らせることが必要になってきます。幸いなことにメッセージ内に攻撃であることのヒントがあります。以下に、一般的に見られるものを紹介します。

- 緊急性が高いことを煽っているもの。「即時の対応」を求め、対応を取らなかった場合には、アカウントの閉鎖や刑務所に送られるなど、何か良からぬことが起きると記載されています。攻撃者は、誤った判断を急いでさせようとしてくるのです。
- 職場でのポリシーや手順を迂回したり、無視したりするようにプレッシャーをかけてくるもの
- 好奇心を煽ってきたり、出来すぎた話が記載されたりしているもの (急に宝くじは当たりません)

- 宛名が「お客様へ」などを使っているもの。連絡を取ってくる企業や友人は、あなたの名前を知っています。
- クレジットカード番号、パスワードなど送信元が知っているはずであろう機密性の高い情報を求めてくるもの。
- メッセージが正規の団体から来ているはずなのに文法が変だったり、スペリングミスがあったり、@GMAIL.COM などの個人用アドレスから来ているもの。
- メッセージが正規のメールアドレス (例えば、上司の) から来ているが、REPLY-TO のアドレスが他社の個人アドレスに設定されているもの。
- 知人からメッセージを受信したが、いつものトーンや言葉遣いがいつもと違うもの。怪しいと判断した場合は、送信者に連絡を取り、そのようなメッセージを送信したか、確認してみてください。サイバー攻撃者にとって、友人や同僚からメッセージが来たかのように細工することは簡単なことです。

最終的には、一般常識が最大の防御となります。メールやメッセージがおかしいと判断した場合、出来すぎた話の場合は、フィッシング攻撃の可能性があります。

日本語版翻訳チーム

日本語版翻訳－NRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内でも有数の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションなどの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。http://www.nri-secure.co.jp

ゲストエディタ

トニア・ダドリー女史は、2011年からセキュリティ啓発に関する取り組みを開発・運営しています。その中には、表彰もされたフィッシングに関するトレーニングプログラムが含まれています。また、LINKEDIN　経由で情報も発信しています (www.linkedin.com/in/toniadudley)。

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/Cb1
他者を安全にする手助けをするために:	https://www.sans.org/u/Cb6
メールのすべきこととすべきではないこと:	https://www.sans.org/u/Cbg
CEO詐欺:	https://www.sans.org/u/Cbl
OUCH! Translations and Archives:	https://www.sans.org/u/Cbq

ライセンス

 Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | **Translated By:** 内山　貴之, 時田　剛