OUCH! | 2015 年 12 月

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

OUCH!

今月のトピック...

- はじめに
- フィッシングとは
- 自分自身を守るために

フィッシングについて

はじめに

メールは、コミュニケーションのために広く使われており、毎日のように職場だけでなく、友人や家族とやり取りをするために利用しています。また、多くの企業はオンラインサービスを提供するためにメールを使用しています。例えば、オンラインショッピングの注文確認や銀行口座の収支報告書の確認などです。世界中の多くの人々がメールに頼っているため、サイバー犯罪者も攻撃のためにメールを使用しています。このニュースレターでは、メールを使った一般的な攻撃手法であるフィッシングに関して解説し、メールを安全に利用するためにできることを説明します。

ゲストエディター

ランス・ヘイデン博士は、Berkeley Research Group の Managing Director として活動しています。セキュリティ文化と行動の習性に関するエキスパートであり、McGraw-Hill から出版されている People-Centric Security: Transforming Your Enterprise Security Culture の著者です。LinkedInでも情報を発信しています。www.linkedin.com/in/drhayden

フィッシングとは

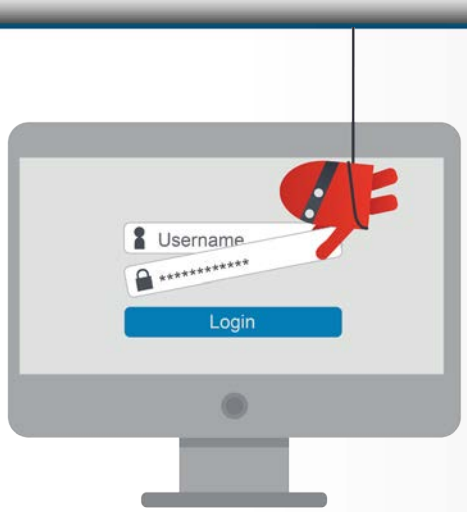
フィッシングとは、メールやソーシャルメディサイトなどで提供されるメッセージングサービスを悪用し、ユーザを騙した上でし、リンクをクリックしたり、添付ファイルを開かせたりする攻撃手法です。この攻撃を受けることで、機密な報を盗まれたり、パソコンが何かに感染したりしてしまう可能性があります。攻撃者は、時間をかけてメールの内容をより本物らしく工夫します。例えば、メールを友人またはよく使う業者などから来たかのように見せます。銀行のロゴを足したり、メールアドレスを偽装したりして、メールをより正規のものであるかのように細工するのです。そして、この出来上がったフィッシングメールを多くの人に一斉に送ります。攻撃者は、誰が被害に遭うかは分かりませんが、大量のメールを出すことで、攻撃が成功する確率が上がるということは把握しています。フィッシングは、漁で使う網と似ており、何が釣れるかは分からないが、大きな網を使えばより多くの魚が釣れるのと同じです。攻撃者は、いくつかの手法のフィッシング攻撃を用いて目的を果たします。

- **情報収集**: 攻撃者の目的は、パスワード、クレジットカード番号や銀行口座などの情報を取得することにあります。情報を取得するにあたり、リンク付きのメールを送り、正規のサイトと思われるサイトに誘導されます。このサイトでは、アカウント情報や個人情報の入力を求められます。しかし、このサイトは不正のもので、入力された情報は攻撃者の元に送られてしまいます。
- **悪意あるリンク**: 攻撃者の目的はデバイスを乗っ取ることにあります。乗っ取るためにリンク付きのメールを送ります。リンクをクリックすることでデバイスに対し攻撃を行うウェブサイトに誘導され、攻撃が成功し

フィッシングについて

た場合、アクセスしたデバイスは感染してしまいます。

- **悪意ある添付ファイル**: 攻撃者の目的は、先ほどと同じで、デバイスを乗っ取ることにあります。この攻撃では、リンク付きのメールではなく、WORD形式などのファイルを悪意ある形に細工しメールに添付して送ります。この添付ファイルを開くと、攻撃が行われ、攻撃が成功するとデバイスが乗っ取られてしまいます。
- **詐欺**: フィッシングメールの中には、デジタル的な手法に変わっただけの詐欺師が送ったものも存在します。宝くじが当たった、募金が必要な慈善活動や多額のお金を動かす支援が必要である、などの名目を使って騙そうとしてきます。これらのメールに返信をした場合、サービスを利用するために支払いが必要、銀行口座へのアクセスが必要などと言って、お金を騙し取られてしまいます。



一番の対策は常識の範囲内で行動することです。メールもしくはメッセージが奇妙、もしくは出来過ぎている場合は、フィッシング攻撃の可能性があります。

自分自身を守るために

ほとんどの場合において、メールやメッセージを開いて、読むことは問題ありません。フィッシング攻撃を成立させるためには、攻撃者はユーザに対し何かの動作をしてもらう必要があります。幸いなことに、メッセージが悪意あるものであると判断するためのヒントはいくつかあります。よくあるものとして、以下のようなケースがあります：

- メールから緊急を要する何かが記載されている。例えば、銀行口座を解約するなどの「即時に対応」しないと悪いことが起こる。攻撃者は、考える間もなく誤った行動を取って欲しいことが狙いです
- 予期せぬ添付ファイル付きのメールを受信したり、受信したメールの中に添付ファイルを開くように誘導されるような文面が書かれていたりした時。例えば、添付ファイル付きのメールで一斉解雇に関する通知、従業員の年収に関する情報やIRS（国税庁）から起訴に関する通知などがあります
- メール本文の中で氏名を使うのではなく、「お客様へ」などの特定の人を指さない書き方をしているメール。連絡をしてくる多くの企業および知人はあなた自身の名前を知っています
- メールの中で、クレジットカード番号やパスワードなどの機密情報を要求しているもの
- メールの中で、実在する企業から来ていると書かれているが、言葉遣いやスペリングミスがあったり、@GMAIL.COM、@YAHOO.COM、@HOTMAIL.COM などの個人メールのアカウントから送付されたりしているもの
- 記載されているリンクが奇妙もしくは正規のものでは無い場合。対策として、マウスのカーソルをリンクの上に持っていき、どこに誘導されるのかポップアップで確認することができます。メールに記載されているリンクとポップアップに記載されている誘導先が一致しない場合は、リンクをクリックしないでください。モバイルデバイスで

フィッシングについて

も、リンクを長押しすることで同様のポップアップを確認することができます。さらに安全な手段として、メールからURLをコピーして、ブラウザに貼り付けるまたは、正しいURLを直接ブラウザに打ち込むことです。

- 知人と思われる人からメッセージを受信したが、いつもの言葉遣いと違う場合。怪しいと思った場合、本人にそのメッセージを送信したか否かを電話で確認してみてください。サイバー攻撃者にとって、あたかも友人や同僚が作成したようなメールを作成するのは容易です。

メールもしくはメッセージがフィッシング攻撃と思われる場合は、そのメールまたはメッセージを削除してください。最終的には、常識の範囲内で行動することが一番の対策になります。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。
http://www.securingthehuman.org

日本語版翻訳チーム

日本語版翻訳ー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、国内最大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

リソース

ソーシャルエンジニアリングについて:	https://www.securingthehuman.org/ouch/2014#november2014
セキュアに保つための5つのステップ:	https://www.securingthehuman.org/ouch/2014#october2014
ハッキングされてしまったら？:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 内山　貴之, 時田　剛