SANS SECURITY AWARENESS
NRI SECURE TECHNOLOGIES
OUCH! | 2017 年 11 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...

- 偽物のオンラインショップ
- 自分自身のパソコン / モバイルデバイス
- 自分自身のクレジットカード

安全にオンラインショッピングするには

はじめに

世界中の多くの人たちは、休暇シーズンが近づいているため、素敵なプレゼントを買い求めに行きます。多くの人は、長い列や混雑を避けるため、あるいは特売品などを探すためにオンラインショッピングすることを選ぶでしょう。しかし、この時期はサイバー犯罪者が偽物のオンラインショッピングサイトを立ち上げ、他人を騙し、お金を盗み取ろうとする時季でもあります。このニュースレターでは、オンラインショッピングのリスクを記載し、安全に掘り出し物を手に入れる方法を紹介します。

ゲストエディタ

レニー・ツェルター氏は、Mierva Labs でセキュリティ製品の開発に携わっているほか、マルウエア対策の講義をSANS Institute で行なっています。レニー氏は、ツイッター（@lennyzeltser）やセキュリティブログ（zelster.com）でも積極的に情報を発信しています。

偽物のオンラインショップ

多くのオンラインショップは正規のものですが、サイバー犯罪者が作成した偽物のウェブサイトもあります。犯罪者は、これらのウェブサイトを正規のサイトに似せて作ったり、著名な店名やブランド名を使ったりします。そして、この偽物のウェブサイトを使い、掘り出し物を探している人を標的にするのです。インターネット上で一番安い価格を探す場合、このような偽物のサイトに誘導される可能性があります。買い物をするためにウェブサイトを選択する際、他のウェブサイトと比較して極端に低い価格を提示しているウェブサイトや、全国的に在庫切れしている製品を大量に提供している場合は、特に注意してください。価格が極端に低い、製品の在庫がある理由は、受け取るものが正規のものではない、偽物であったり、盗まれたものであったり、場合によっては何も届かないこともあるということです。自身を保護するために以下の対策を実施してください：

- 可能な限り、既に知っている、信頼している、そして過去に利用したことのあるウェブサイトから買い物をしてください
- ウェブサイトには、セールスとサポート関連の質問を受け付ける正規の住所と電話番号があることを確認してください。サイトが怪しく見えた場合、一度人間と話すようにしてください。誰とも話ができない場合は、偽物のウェブサイトである、最初の重要な証拠となります
- 出来過ぎた話や不自然な言葉遣い、スペリングなどの目につきやすいものに気を配ってください
- ウェブサイトが、過去に利用したことのあるサイトと見た目が一緒で、そのウェブサイトのドメイン名や店名が微妙に違う場合は、特に気を付けてください。Amazon (https://www.amazon.com) で通常買い物をしているとした場合、Amazon と謳っていてもhttp://store-amazoncom.com というアドレスになっている場合、そのサイトは偽物の可能性があります。

安全にオンラインショッピングするには

- 店名またはURLを検索エンジンに入れて検索し、他人がそのウェブサイトに対して何を言っているか確認してみてください。「詐欺」、「不正」、「2度と利用しない」、「偽物」などの言葉があるか注意深く確認してみてください。また、レビューが少ないということは、ウェブサイトが新しく、信頼できない、ということを表している場合もあります。
- 買い物を完了させる前に、ウェブサイトとの通信が暗号化されていることを確認してください。多くのブラウザでは、暗号化されている通信を示す南京錠のマークが表示されていたり、HTTPS の文字列がウェブサイト名の隣に緑で表示されていたりします。

信頼できる、定評のあるウェブサイトのみで買い物することでインターネット上における自分の安全を確保してください。

大事なのは、ウェブサイトの見た目が良くても、正規のものでないことがある、ということです。そのウェブサイトを利用するにあたり、少しでも違和感がある場合は、利用しないでください。その代わりに信頼できる、過去に利用した著名なウェブサイトを利用するようにしてください。目的としている掘り出し物を手にすることはできないかもしれませんが、正規の製品が手元に届く可能性が高くなり、クレジットカードなどの個人情報が漏えいする可能性は低くなります。

自分自身のパソコン / モバイルデバイス

正規のウェブサイトで買い物することに加え、パソコンやモバイルデバイスを安全な状態にしておく必要があります。サイバー犯罪者は、銀行口座やクレジットカード情報、パスワードなどを窃取する目的でデバイスをハッキングしようとしてきます。デバイスを安全な状態に保つために以下の対策を実施してください。

- 子供がいる場合、子供用のデバイスと大人用のデバイスの2つを用意することを検討してください。子供はとても好奇心旺盛なため、興味の赴くままテクノロジーと触れ合います。そのため、ウイルスなどに感染してしまう可能性が高いのです。オンラインバンキングやオンラインショッピングなどのオンライン取引のために別のパソコンやタブレットを利用することで、感染する可能性を低くすることができます。
- 最新のアップデートインストールし、最新版のアンチウイルスソフトウエアを利用してください。こうすることで、サイバー犯罪者はデバイスをハッキングしづしにくくなります。

自分自身のクレジットカード

クレジットカードの明細を定期的に確認し、怪しい取引を特定するようにしてください。特にカードを利用して新しいオンラインサイトで買い物をした直後は確認する必要があります。クレジットカードのプロバイダによって、カ

安全にオンラインショッピングするには

ードを使った取引が発生した場合や設定した金額以上の取引が発生した際にメールやショートメールが届くサービスを提供しています。また、オンラインショッピング用のカードを用意し、何かが起きた場合でも他の取引に影響を与えないようにすることも可能です。何か詐欺にあったと感じた場合は、直ちにクレジットカード会社に連絡してください。このため、オンラインショッピングでは、デビットカードではなく、可能な限りクレジットカードを利用するべきです。デビットカードは、銀行口座から直接お金を引き出すため、詐欺が発生した場合、お金を取り戻すことが大変になる可能性があります。そして最後に、オンライン取引の度に固有のクレジットカード番号を生成するクレジットカードの利用やクレジットカード番号をお店に開示しなくても取引が可能な PayPalなどの著名な支払いサービスの利用を検討してみてください。

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。
securingthehuman.sans.org/ouch/archives

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

リソース

ソーシャルエンジニアリングについて:	https://securingthehuman.sans.org/ouch/2017#january2017
安全を保つための4つのステップ:	https://securingthehuman.sans.org/ouch/2016#october2016
自宅のネットワークを安全にするには:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

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

