OUCH! | 2017 年 10 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
・ 5つの簡単なステップ
・ 外出している子供を安全にするために

他者を安全にする手助けをするために

はじめに

ゲストエディタ

ランディー・マルケニー氏(@randymarchany)は、バージニア工科大学のCISOで SANS Institute 公認の講師としても活躍しています。

多くの人は、安全に利用することも含め、テクノロジーと抵抗なく接することができています。しかし、友人や家族の中で同じように抵抗なく接することができない人もいると思います。さらに言えば、困惑していたり、怖がったり、怯えていたりしていることもあるでしょう。これが、昨今のサイバー攻撃者に対し脆弱な部分を生み出しているのです。サイバーセキュリティについて過度に怖がる必要はなく、基本的なことが分かると実はとても単純なことだと納得するでしょう。これらの人たちは、基本的なことを理解するために、知見を有する人からのガイダンスが少し必要なだけです。

5つの簡単なステップ

以下に、これらの人たちが昨今のテクノロジーに対する恐怖を乗り越えるためにできる5つの簡単なステップを紹介します。それぞれのステップに関する詳細な情報は、このニュースレター末尾にある「リソース」の項を参考にしてください。

1. **ソーシャルエンジニアリング**: ソーシャルエンジニアリングとは、攻撃者がユーザに対し、本来すべきでない行動として、例えばパスワードの共有、パソコンを感染させる、機微な情報を共有させるためにアプローチを仕掛けてくるといった典型的な攻撃手法です。これは、特段新しい手法ではなく、詐欺や詐欺師は千年以上も前から存在しています。違いは、悪者が同様のコンセプトをインターネットに適用していることです。誰かが緊急性を煽ってきたリ、話が出来過ぎていたり、サイバー攻撃者が友人を騙ったり、違和感があったりした場合などがソーシャルエンジニアリング攻撃を特定するためのヒントになることを教えてあげてください。また、ソーシャルエンジニアリング攻撃の典型的な例として、例えばフィッシングメールや有名なマイクロソフトのサポートを騙る電話攻撃に関する情報を共有してください。最低でも、家族の人たちが他社とパスワードを共有したり、パソコンへのリモートアクセスを許可してはいけないことを理解してもらってください。
2. **パスワード**: オンライン上のアカウントや機器を保護するための重要なポイントは、強いパスワードを設定することです。家族の方に強いパスワードの作り方を教えてください。記憶しやすく打ちやすいパスフレーズを推奨します。パスフレーズは、複数の単語から成り立つパスワードに過ぎません。さらにパスワードマネージャのインストールと使い方も教えてください。それぞれの機器およびアカウントに設定されているパスワードは異なるものであるこ

他者を安全にする手助けをするために

とが重要です。パスワードマネージャの使用が難しい場合には、パスワードを紙に書き出し、安全な場所に保管するよう指導してください。最後に、重要なアカウントに対し、2段階認証（または2要素認証）の設定をしてあげてください。2段階認証は、アカウント保護の面から見て、一番有効な手段です。

他の人が安全にテクノロジーを利用できるようにするため、この5つの簡単なステップを共有してください。

3. **パッチの適用**: 機器の安全を確保するために誰でもできることとしては、システムを常に最新の状態に保つことです。パソコンやモバイル機器だけでなく、ゲーム機や温度計、電球、スピーカーなどのインターネットに接続されている全ての機器に同じことが言えます。機器を常に最新の状態とするためにできる一番簡単な事は、自動更新を有効にすることです。
4. **アンチウイルス**: 人は誰でも間違いを犯します。まれにインストールしてはいけないものをインストールしてしまったり、クリックしてはいけないものをクリックしたりして、システムを感染させてしまうことがあります。アンチウイルスはこれらの間違いから保護してくれるように設計されています。アンチウイルスは、すべてのマルウエアを阻止することはできませんが、広く使われている攻撃を検知し、防いでくれます。そのため、自宅にあるパソコンにはアンチウイルスをインストールし、有効にし、最新の状態に保ってください。そして、多くのアンチウイルスソリューションは、ファイアウォールやブラウザ保護などの機能も提供しています。
5. **バックアップ**: 他が全部駄目になったり、ファイルを誤って削除したり、ランサムウエアなどのサイバー攻撃から復旧する際に利用できるのはバックアップのみです。家族や友人が自動でバックアップを取れるようにセットアップしてあげてください。簡単なソリューションとしてクラウドにバックアップを取る手法があり、一時間おきやファイルが更新される度にバックアップが行われます。これらのソリューションは、バックアップを取るのが簡単なだけでなく、復旧も楽チンです。

外出している子供を安全にするために

テクノロジーに抵抗が無い場合、自分だけでなく、自分の子供も安全な状態にしているでしょう。しかし、テクノロジーに抵抗がある親戚、例えば祖父母を子供が訪れた場合、インターネット上で子供を保護するための手法を知らなかったり、自分の期待することを理解していなかったりします。特に親戚などを訪問する際に、子供を守るためにできることをいくつか紹介します。

- **ルール**. 子供のセキュリティを確保するためのルールや期待していることがあるのであれば、それを適切な人に伝えてください。例えば、子供がインターネットを利用する時間に制限があるか、誰とコミュニケーションを取ってよいか、遊んでいいゲームや遊んではいけないゲームがあるか？などが挙げられます。親戚に対して、子

他者を安全にする手助けをするために

供にルールを説明させるようなことをしてはいけません。例えば、「ルールシート」を作成して頻繁に訪問する親戚の家に配布すると良いでしょう。

- **コントロール**: 子供が大人よりもテクノロジーに関する理解度が高い場合、それを悪用することがあります。例えば、子供は祖父母のパソコンに対する管理者権限を貰った上で、本来だと遊んではいけないゲームをインストールして遊ぶなど、好きなことをしようすることがあります。親戚が、子供に対して本来の権限を超える権限を与えてはいけないことに関して理解を得るようにしてください。

最後に、今後も学び続けるために、この OUCH! ニュースレターを購読するよう推奨してください。これは、20か国語以上に翻訳され無料で毎月配信されています。購読はこちら：https://securingthehuman.sans.org/ouch。

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－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
パスフレーズについて:	https://securingthehuman.sans.org/ouch/2017#april2017
パスワードマネージャ:	https://securingthehuman.sans.org/ouch/2017#september2017
2段階認証について:	https://securingthehuman.sans.org/ouch/2015#september2015
バックアップと復旧について:	https://securingthehuman.sans.org/ouch/2017#august2017
Securing Today's Online Kids:	https://securingthehuman.sans.org/ouch/2017#may2017

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