SANS SECURING THE HUMAN
NRI SECURE TECHNOLOGIES

OUCH! | 2016 年 01 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...

タブレットを安全に使用するには

はじめに

新しいタブレットの入手、おめでとうございます。このテクノロジは、他社とコミュニケーションを取ったり、オンラインショッピングをしたり、映画を見たり、ゲームをして遊んだりするにはとても便利なものです。今後タブレットは、パソコンに代わって日常生活の中でとても重要なものとなるでしょう。そこでタブレットや自分の個人情報を安全に守るためにできることを紹介します。

ゲストエディター

ローリー・ローゼンバーグ氏は、従業員や顧客向けのセキュリティに関する教材作成の経験が豊富であり、様々な手法を使って知識を共有することに意欲的である。彼女は、Twitterにて情報を発信している（@InfoSecLori）

タブレットを安全に使用する

聞いて驚くかもしれませんが、タブレットに対する一番の脅威はハッカーではなく、実は自分自身なのです。ハッカーによって侵入されるよりも自分自身でタブレットをどこかに忘れてしまったり、紛失してしまったりする事の方がはるかに高確率で発生します。タブレットを安全にするために、まずやるべきことは画面の自動ロックを設定することです。設定すると、タブレットを利用する際に毎回、強いパスコードの入力や、パターンをなぞる、あるいは指紋を使って認証しなければ使うことができなくなります。つまり、タブレットを紛失または窃盗されたりした場合、自分以外の誰も内部に保存されたデータにはアクセスできないため、個人情報、モバイルアプリなどで保存されている情報は保護された状態になります。画面の自動ロックを有効にした後、タブレットを守るために追加でできることを以下に列挙します：

1. タブレットをリモートからトラッキングする機能を有効化、あるいはソフトウェアをインストールしてください。こうすることで、タブレットを紛失または窃盗されたりした場合、インターネットからタブレットに接続し、在り処が分かるだけでなく、最悪の場合は、リモートからすべてのデータを削除することも可能になります。
2. デバイスを更新し、自動更新機能も有効にして、常に最新版のオペレーティングシステムが動作している状態にしてください。攻撃者は常にソフトウェアに存在する新たな脆弱性を探しており、ベンダは常に新たなアップデートやパッチを提供しながらこれらの脆弱性に対応しています。オペレーティングシステムやモバイルアプリを最新版に保つことで、攻撃者によるハッキングを難しくすることができます。
3. 購入したタブレットの設定を始めて行うとき、特にプライバシーに関する設定を行うときは気を付けてください。タブレットを利用するにあたり、プライバシーに関して大きな問題は、他人によって自身の居場所をトラッキング

タブレットを安全に使用するには

タブレットを安全に使用するためにできることは、画面ロックを有効にすること、プライバシー設定の見直し、およびタブレットを常に最新の状態にすることです。

されるだけでなく、特定できてしまうことです。ここで推奨したいのは、すべてのアプリでトラッキング機能を一度無効にし、必要と思われるアプリのみ有効にすることです。大半のアプリは、リアルタイムで居場所をトラッキングする必要はありません。必要となりそうなアプリの例として、地図アプリや、レストランなどを探すアプリなどがあります。

4. 多くのタブレットとアプリは、情報をクラウド上に保存します。そのため、どこにデータが保存されているだけではなく、どのように安全性が担保されているのかを把握してください。例えば、位置情報が埋め込まれたプライベートな画像を誰でも閲覧可能な状態でインターネット上に公開されたくはないでしょう。このような場合は、デフォルトの設定としてクラウドとの情報共有は無効にし、特定のものを共有したい場合のみ、都度有効にするようにしてください
5. タブレットは他のデバイス、例えばスマートフォンやノートパソコンと同期する機能があり、その利用頻度も増加傾向にあります。同期は素晴らしい機能ですが、どのアプリ・機能を同期させるかは慎重に選択してください。同期を有効にしている場合、タブレットのブラウザで訪れたサイトが、業務端末のブラウザに現れることがあるということです。

安全性を維持する

タブレットを安全な状態にしたら、安全性を保った状態を保持させてください。以下は、タブレットの安全性を保つためにできることを列挙しています：

- 自分のタブレットを脱獄（改造）もしくはハッキングしないでください。これらの行為は、多くのセキュリティ機能や設定を回避または無効にしてしまい、悪意ある第三者による攻撃の被害を受ける確率が高くなります。
- 必要なアプリのみダウンロードし、信頼できるとこからだけ入手するようにしてください。iPad の場合は、アプリのダウンロードをiTunesに限定するようにしてください。これらのアプリは公開前に Apple によって審査されています。Google の場合は、Google Play に限定してダウンロードすることを推奨します。Amazonタブレットの場合は、Amazon App Store のみを推奨します。アプリは他のサイトからもダウンロードすることが可能ですが、これらのアプリは審査などを経ていないため、何かに感染している恐れがあります。最後に、どこから入手したアプリであっても、必要が無くなった時や利用することが無くなったアプリはタブレット上から削除してください

タブレットを安全に使用するには

- 新しいアプリをインストールする際は、プライバシーの設定を見直した上で設定を行ってください。これは、タブレットを最初に設定した時と同じです。アプリが何に対しアクセス権を獲得するのかに注意を払ってください。例えば、新たにダウンロードされたアプリは、本当にすべての連絡先情報へのアクセスを必要するのでしょうか。アプリに対し与えなければならないアクセス権に少しでもためらいがあるのであれば、別のアプリを探すようにしてください。また、定期的にアクセス権を確認し、変更されていないかを確認してください

タブレットは、とても便利で多くの楽しみを与えてくれるデバイスです。ここで紹介したことを実施すると、タブレットを安全に保つことができ、自分自身を守ることにつながります。

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

モバイルアプリをセキュアに利用するには:	https://www.securingthehuman.org/ouch/2015#january2015
パスフレーズについて:	https://www.securingthehuman.org/ouch/2015#april2015
クラウドを安全に利用するには:	https://www.securingthehuman.org/ouch/2014#september2014
携帯端末の処分方法:	https://www.securingthehuman.org/ouch/2014#june2014
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