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...

- 出発前のチェック
- 紛失 / 盗難されたデバイス
- Wi-Fi アクセス
- 公共利用可能なパソコン

旅先で安全を保つために

はじめに

私は、旅先でもテクノロジーがもたらす恩恵を最大限受けて欲しいと願っています。このニュースレターでは、旅先においてインターネットへ安全に接続し、デバイスを安全に利用するためにできることを紹介します。

ゲストエディター

マーク・ウイリアムス氏は、ブルークロス・ブルーシールド協会のテネシー支部でEnterprise Security Architectをしています。また、SANSの認定インストラクターでもあり、ISSA Chattanoogaの会長も務めています。ウイリアムス氏は、様々なところへ出張しており、デバイスを一緒に持っていく上で起きる問題についての知見を広く持っています。

ソーシャルエンジニアリングとは

会社または自宅で利用するネットワークが安全であっても、旅先で接続するネットワークは信頼できないと思った方が良いでしょう。そのネットワークに接続している人は分からないだけでなく、さらに何をしているか分かりません。自分自身とデータを守るため、出発前にできる簡単なことをいくつか紹介します：

- 一番安全な情報とは、そもそも保持していない情報です。持参しようとしているデバイスが保持している情報のうち、旅先で必要の無い情報は削除してください。こうすることで、デバイスを紛失、盗難または税関・国境警備職員などによって破壊されても影響を抑えることができます。出張の場合は、上司に確認し、出張する際に貸し出ししているデバイスがあるかどうか確認してください。
- モバイルデバイスおよびノートパソコンを強いパスワードまたはパスフレーズで保護してください。こうすることで、デバイスを紛失、盗難されても外部から情報へアクセスされることは無くなります。さらに、ディスクを暗号化するツールをインストールまたは有効にしてください。多くのモバイルデバイスでは、スクリーンロックをかけることでこの機能は自動的に有効になります。
- 遠隔からデバイスを追跡するためのソフトウエアをインストールまたは有効にしてください。特にデバイスが紛失、盗難に遭った場合に備えて、追加で遠隔からデータを完全に消去できるようにすると良いです。
- 出発前にデバイス、アプリケーション、アンチウイルスソフトウエアを最新のバージョンにアップデートしてください。多くの攻撃は、古いバージョンのソフトウエアを標的にします。
- すべてのデバイスのバックアップを取ってください。旅先で何か起きても安全な場所に保管されている元のデータを残すことができます。

© SANS Institute 2017

旅先で安全を保つために

- 外国へ旅行または出張する際は、モバイルサービスのプロバイダとの契約内容を確認してください。海外でデータ通信をした場合、プロバイダによって高額な請求を受けてしまうことがあります。そのため、海外の旅先ではモバイルデータの通信を無効にし、プリペイドのSIMカードを現地で買って利用することを検討してみてください。

旅先で安全を保つためには、旅立つ前に安全な状態を準備すること。そして、物理的な安全を保ち、すべての通信を暗号化することです。

紛失 / 盗難されたデバイス

旅行または出張が始まったら、物理的にデバイスを保護してください。例えば、デバイスを誰にでも見える状態で車の中に置かないようにしてください。犯罪者によって車の窓を割られて、金目のものをすべて盗られてしまいます。犯罪はリスクですが、VERIZONが行った調査によると、デバイスが盗難に遭う確率よりもデバイスを紛失する可能性の方が100倍も高いという結果が出ています。つまり、旅先では常にデバイスを保持しているか確認するようにしてください。例えば、飛行場でセキュリティチェックポイントを通過した後、タクシーやレストランから出た後、ホテルからチェックアウト後や飛行機を降りた後、などが挙げられます。飛行機から降りる際は、特に前席にあるポケットの確認を忘れずに！

Wi-Fiアクセス

旅先でインターネットにアクセスするとしたら、公共の Wi-Fiアクセスポイントを利用することになるでしょう。これらは、ホテルや喫茶店、飛行場などで利用することが可能ですが、公共の Wi-Fiには、大きな問題が二つあります：誰によって設置されたか分からないことと、誰が接続しているか分からないことです。そのため、信頼できないということになります。また、Wi-Fiは、電波を使うため、物理的に近い距離にいる人によって通信を傍受される可能性があります。これらがあるために公共のWi-Fiを利用する際は、すべての通信を暗号化する必要があります。例えば、ブラウザを使った通信では、訪れるウェブサイトのコンテンツが暗号化されているか確認してください。ブラウザのアドレスバー内において「HTTPS://」という表記、または施錠された南京錠の画像があれば確認が可能です。また、VPN(仮想プライベートネットワーク)を有効にすることで、通信をすべて暗号化することができます。VPNは、会社によって支給されたり、個人で利用するためにVPNサービスを購入したりすることも可能です。信頼できるWi-Fiが無い場合は、スマートフォンのテザリング機能を利用してください。ただし、注意しなければならないのは、海外での利用において高額な請求を受ける可能性があります。事前にサービスプロバイダに確認してください。

© SANS Institute 2017

旅先で安全を保つために

公共利用可能なパソコン

ホテルのロビーやサイバーカフェなどで提供されている利用可能なパソコンを使って、アカウントへのログインまたは機微な情報へのアクセスは絶対に行わないでください。そのパソコンを過去に利用した人の素性は分からず、その人が誤ってまたは故意に何かに感染させたかもしれません。できるのであれば、自分がコントロールでき、信頼できるデバイスのみを利用してください。公共のパソコンの利用は、一般にアクセス可能な情報、例えば天気やニュースを確認するくらいの利用法しか考えられません。Googleなどのアカウントにログインする行為は、ハッカーに対して、見てくださいという招待状になりかねません。

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、国内でも屈指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

パスフレーズについて:	https://securingthehuman.sans.org/ouch/2015#april2015
バックアップと復旧:	https://securingthehuman.sans.org/ouch/2015#august2015
マルウエアとは:	https://securingthehuman.sans.org/ouch/2016#march2016
暗号について:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH! アーカイブ / 翻訳:	https://securingthehuman.sans.org/ouch/archives

OUCH!はSANS Securing The Human プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。翻訳その他に関しては、ouch@securingthehuman.org までお問合せください

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