OUCH! | 2015 年 02 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...

- 事前チェック
- 紛失/盗難された機器
- Wi-Fiアクセス
- 公共のコンピュータ

出張や旅行中にセキュリティを保つために

はじめに

今回のニュースレターでは、旅行もしくは出張中に仕事をする際にインターネットへ安全に接続する方法を紹介します。

ゲストエディター

スティーブ・アームストロング氏は、Logically Secure社のCyberCPRにおけるテクニカルディレクターであり、SANS認定講師です。また、いくつかのコースの著者も過去に担当しており、ツイッター (@Nebulator)やGoogle+ (+SteveArmstrongSecurity) でも積極的に情報発信をしています。

事前チェック

会社や家のネットワークはセキュアであっても、旅先で接続するネットワークはセキュアではないと考えるべきです。外出先のネットワークには誰が接続しているかも分からない上に、どのような脅威があるかも分かりません。いくつかの簡単なことを出る前に行うことで、外出先でデータを守るために大きな一歩を踏み出すことができるでしょう。

1，2週間前にやるべきこと：

- デバイス上にあるデータの中から、外出先で必要なデータを特定し、不要なデータは削除してください。こうすることによって、デバイスの紛失や、盗難、税関・入出国審査において係官に押収されても影響を最小限に抑えることが可能になります。また、出張の場合は上司に相談し、出張先での利用を目的とした専用のデバイスが組織にあるか確認してください。。
- 海外へ渡航する場合は、その国の電源コネクタの形状などを調べた上で、必要に応じて変換アダプタ等を入手してください。また、利用している携帯電話のプロバイダ契約についても確認をしてください。プロバイダは海外でのデータ通信に対し、とても高い金額を請求することがあります。渡航先が海外の場合は、携帯電話のデータ通信機能を無効にする、もしくは海外向けに契約プランなどを変えた方が良いかもしれません。
- それぞれのデバイスにリモートからトラッキングするためのソフトウェアをインストールしてください。紛失や盗難に備え、リモートからのフォーマットも可能にしておくことをお勧めします。多くのモバイルデバイスでは、既にこの機能が提供いるので、単に機能を有効にするだけの状態になっている場合があります。（これらの機能が正常に動作するには、インターネット接続が必要であることを覚えておいてください）

1，2日前にやるべきこと：

- デバイス、アプリケーションおよびアンチウイルスソフトウェアの更新を行い、それぞれ最新版になるようにしてください。
- デバイスが提供するセキュリティ機能　たとえばファイアウォールなどを必要に応じて有効にしてください。

出張や旅行中にセキュリティを保つために

- すべてのモバイルデバイスは、強力なパスワード・パスコードで保護してください。これにより、モバイルが紛失・盗難にあっても、データにアクセスできないようにします。
- デバイスが紛失・盗難にあっても、データへのアクセスを防ぐために、すべてのデバイスを暗号化してください。iPhone などのデバイスはパスワード・パスコードを設定することで自動的に暗号化が行われます。
- すべてのデバイスのバックアップを取ってください。外出先でデバイスに何かあってもデータを安全に保管することができます。

外出先でセキュアを保つためのコツは、出発前にデバイスをセキュアにすること、物理的にセキュアにすること（いかなる時もどこにあるか把握すること）、および通信をすべて暗号化することです。

デバイスが紛失/盗難にあったら

外出先では、デバイスの物理的なセキュリティにも気を配ってください。例えば、デバイスを車の中に置く際は、外から見える場所に置かないようにしてください。犯罪者は、窓を割った後、デバイスのみならず金目のものをすべて盗みます。このような手口に対抗する一つの方法としては、デバイスを置いていく場合、ワイヤーロックを使用しデバイスを物理的にロックすることがあるでしょう。また、お気づきではないかもしれませんが、デバイスに対する犯罪リスクは高いにもかかわらず、盗難に遭う確率よりも紛失してしまう確率の方が高いのです。ベライゾン社のここ10年に渡る調査によると、デバイスが盗難に遭うよりもデバイスを紛失する確率の方が15倍も高いとしています。外出先でもデバイスが手元にあることを常に確認してください。例えば、空港のセキュリティチェックポイントを通過した後、タクシーを降りたりレストランを出た後、ホテルのチェックアウト手続きの後、および飛行機から降りる前などが確認ポイントとしては重要です。

Wi-Fiアクセス

外出先でのインターネットアクセスは、公共のWi-Fiアクセスポイントを使うことが多いでしょう。これらは、ホテルや喫茶店、空港などでサービス提供されています。公共のWi-Fiアクセスポイントにおける問題点は、接続マニュアルなどに記載されているSSIDと同じであっても、本物かどうか分からないだけではなく、誰によって設置されたのかが分からない、誰が接続しているのかも分からないという点なのです。従って、基本的には公共のWi-Fiアクセスポイントを信頼できないことになりますが、出発前にデバイスをセキュアにしたのは、このためです。Wi-Fiは、電波を使ってデバイスからアクセスポイントへの通信を行いますので、アクセスポイントやWi-Fiデバイスに物理的に近い人によって、通信を傍受される可能性もあります。

信頼できない公共のWi-Fiを使用する場合は、すべての通信を暗号化する必要があるでしょう。例えば、ブラウザを使ってウェブサイトを閲覧する場合も、通信が暗号化（URLには、https:// と記載され、鍵がかかったロックの絵が横にあります）されていることを確認してください。また、VPN (Virtual Private Network - 仮想プライベートネットワーク) を使用

出張や旅行中にセキュリティを保つために

して通信をすべて暗号化することも可能です。VPNアカウントは、会社によって発行される場合もあれば、VPN機能を提供するサービスを購入することも可能です。信頼できるWi-Fiアクセスポイントを探すことができるか心配な場合は、スマートフォンでテザリングすることも視野に入れてください。（注意：先ほども述べたように、海外での利用は高額な通信料金を請求される可能性があります。事前にプロバイダに確認してください）

公共のコンピュータ

ホテルのロビー、図書館、インターネットカフェに設置されている公共のコンピュータは利用しないでください。前に利用したユーザも分からない上に、意図的・無意識に何かに感染させた可能性もあります。可能な限り、オンライン上で何かを行うときは、自身が管理し、信頼できる機器のみを使用してください。公共のパソコンを使用しなければならない場合は、ログインやパスワードを必要とするサービスの利用は避けましょう。

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

パスワードマネージャー:	http://www.securingthehuman.org/ouch/2013#october2013
2段階認証:	http://www.securingthehuman.org/ouch/2013#august2013
暗号化機能について:	http://www.securingthehuman.org/ouch/2014#august2014
タブレット端末の安全な使い方:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

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