OUCH! | 2015 年 07 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
- プライバシー
- セキュリティ

ソーシャルメディアについて

はじめに

フェイスブック、ツイッター、インスタグラムや LinkedIn などのソーシャルメディアサイトは、素晴らしいリソースです。これらのサイトでは、世界中にいる人と出会い、接し、情報を共有することができます。しかし、これらのサービスは、情報共有などがオンライン上でできることによりリスクも生じます。このリスクは、自分だけでなく、家族、友人や所属している会社にもその影響が及ぶ可能性があるのです。このニュースレターでは、これらのサイトを利用する上で生じる危険性と安全に利用する方法を解説します。

ゲストエディター

ターニャ・バッカムは、長らくセキュリティコンサルタントとして活躍しているほか、10年以上SEC502, SEC542, SEC401, MGT414, AUD507 といったSANSコースの著者および講師をしており、ツイッター (@tbaccam) でも情報発信を行っています。

プライバシー

ソーシャルメディアを利用する上での共通の懸念は、個人情報の保護です。潜んでいる危険には、以下のものが上げられます。

- **将来への影響**： 身辺調査の一環としてソーシャルメディアサイトを確認する組織があります。恥ずかしい、もしくは自分に不利な写真や投稿は、どんなに古いものでも昇進や採用を妨げる要因になる可能性があります。また、多くの大学は、入学の願書と併せて似たような確認を行っています。プライバシーの設定だけでは、情報を完全に保護できません。ほかにも、複数のサイトでアーカイブされている特定のページやグループに対し「いいね」や参加を要求することがありますので、注意が必要です。
- **自分に対する攻撃**： サイバー攻撃者は、あなたの投稿を分析し、これらの情報を利用して所属している企業に関する情報にアクセスできるおそれがあります。例えば、共有されている情報をもとに「秘密の質問」の回答を推測して、パスワードを変更することを試みたり、スピアフィッシング呼ばれる手法で標的型のメール攻撃を行ったり、あなたになりすました上で同僚と接したりすることがあります。これらの攻撃は、実生活にも影響を及ぼす可能性があり、どこで仕事をしているのか、またどこに住んでいるのかを特定される可能性もあります。
- **雇用主に意図せず悪影響を及ぼす**： 犯罪者や競合他社は、あなたが投稿した組織に関する機密情報を、雇用主が不利になるように悪用することがあります。また、自分の投稿によって組織の評判に傷をつけてしまうこともあります。ソーシャルメディアに関する組織のポリシーを確認した上で、業務に関連した情報を投稿するようにしてください。さらに付け加えると、ソーシャルメディアの投稿が監視下にある可能性があることも頭に入れておいてください。

一番有効な保護は、投稿を制限することです。プライバシーの設定は、一定の保護を与えてくれますが、多くは分かりづらく、気付かないうちに変更されていることがあります。プライベートだと思って投稿した情報が様々な理由で公開されてしまうこともあります。また、投稿のプライバシーは、共有された人々のセキュリティ意識に依存しています。共有

ソーシャルメディアについて

した人数が多ければ多いほど、その情報が公開されてしまう確率は高くなります。投稿したすべての情報がどこかのタイミングで公開され、永遠にインターネット上に残るという前提で投稿してください。

最後に、友人が投稿する自分に関連した情報にも関心を持つべきです。友人が不愉快な情報を投稿してしまった場合は、削除するよう依頼してみてください。無視もしくは拒否された場合は、ソーシャルメディアサイトに直接連絡して、その情報を削除してもらうよう依頼してください。同時に、他人に関する情報を投稿する際は、細心の注意を払ってください。



ソーシャルメディアサイトは、とても楽しい上に便利だが、誰にどういう情報を共有しているのかを常に意識してください。

セキュリティ

プライバシーに関する懸念に加え、ソーシャルメディアのアカウントやオンライン上での行動を保護するためにできることをいくつか紹介します：

- **ログイン**： それぞれのアカウントを強い、そして固有のパスワードで保護し、これらのパスワードを誰とも共有しないでください。また、多くのソーシャルメディアサイトは、2段階認証などの強い認証方式をサポートしています。強い認証方式が利用可能な場合は、必ず適用するようにしてください。最後に、ソーシャルメディアサイトのログイン情報を使って他のサイトにログインしないでください。これらがハッキングされると、ログイン情報を共用するすべてのアカウントが危険に晒されてしまいます。
- **プライバシー設定**：プライバシー設定を利用している場合、定期的に確認を行ったうえでテストしてみてください。ソーシャルメディアサイトは、頻繁にプライバシー設定を変更するため、簡単に過ちを犯してしまう可能性があります。また、多くのアプリやサービスには、位置情報を投稿にタグ付けする機能 (ジオタギングと呼ばれている) があります。物理的な位置情報を公開したくない場合は、これらの設定を定期的に確認してください。
- **暗号化**： ソーシャルメディアサイトは、HTTPSと呼ばれる暗号化を行うことで、サイトとのオンライン通信を保護しています。ツイッターやGoogle+は、デフォルトで有効になっていますが、他のサイトでは、手動でHTTPSを有効にする必要があります。ソーシャルメディアサイトのアカウント設定を確認し、利用可能な場合において、デフォルトでHTTPS通信が行われるようにしてください。
- **電子メール**： ソーシャルメディアサイトを騙る電子メールは、常に疑ってください。これらは、サイバー犯罪者がなりすまし攻撃のために送っている可能性が高いからです。これらのメッセージに対する、一番安全な返信方法は、保存されているブックマークなどから直接ソーシャルメディアサイトにログインし、ウェブサイトからのメッセージや通知を読んで返信することです。
- **悪意あるリンク / 詐欺**： ソーシャルメディアサイトに投稿されている複雑な、あるいは短縮アドレスや詐欺行為には気を付けてください。攻撃者は、ソーシャルメディアを悪用して攻撃活動の範囲を広めてきています。友人によって投稿されたメッセージだからといって、本当にその友人による投稿とは限りません。アカウントがハッキングされた可能性があるからです。家族の人や友人が確認できないメッセージ（例えば、強盗に遭ったためお金を送ってほ

ソーシャルメディアについて

しい、など）を投稿した場合、携帯電話に電話をかけるなどの手段で連絡を取り、その情報が本当に本人によって投稿されたものであるかを確認してください。

- **モバイルアプリ**： 多くのソーシャルメディアサイトは、オンラインアカウントへのアクセスを可能にするためのモバイルアプリを提供しています。これらのモバイルアプリは、信頼できるサイトのみからダウンロードしてください。また、スマートフォンを強いパスワードを使って保護してください。スマートフォンを紛失してしまった際に、ロックされていない場合、誰でも自分になりすましソーシャルメディアサイトにアクセスし、投稿ができてしまいます。

ソーシャルメディアサイトは、世界中の人々とコミュニケーションを取るための素晴らしい手段です。ここで記載されている助言を守ることで、オンライン上でのやり取りをより安全に行うことができます。ソーシャルメディアサイトをさらに安全に利用したい場合や、不正な行動を報告したい場合は、ソーシャルメディアサイトのセキュリティページを確認してください。

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。
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

パスフレーズについて:	http://www.securingthehuman.org/ouch/2015#april2015
2段階認証:	http://www.securingthehuman.org/ouch/2013#august2013
モバイルアプリをセキュアに利用するには:	ihttp://www.securingthehuman.org/ouch/2015#january2015
子供に教えるインターネットセキュリティ:	http://www.securingthehuman.org/ouch/2015#june2015
フェイスブックのセキュリティ:	https://www.facebook.com/safety

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