OUCH! | 2015 年 04 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...

- パスフレーズとは
- パスフレーズを安全に利用するために
- リソース

パスフレーズについて

はじめに

パスワードは、メールへのアクセスやオンラインバンキング、買い物およびスマートフォンへのアクセスなどで、ほぼ毎日利用しています。しかし、パスワードは同時に大きな弱点です。他人にパスワードを知られてしまったら、身元（アイデンテティー）をなり済まされて勝手にお金を送金したり、個人情報にアクセスする可能性があります。このような脅威から自身を守るためには、強いパスワードは必須です。このニュースレターでは、簡単に記憶できる強いパスワードの作り方を、パスフレーズと言う種類のパスワードを使ってお伝えします。

ゲストエディター

ギー・ブルーノ氏は、IPSS Inc. のシニアセキュリティコンサルタントで、SANS認定講師およびISCハンドラでもあります。同氏は、SANSのGSEを取得しており、SANS Cyber Guardianプログラムを修了しています。ツイッター(@GuyBruneau)や handlers.sans.org/gbruneau でも積極的に情報を発信しています。

パスフレーズとは

サイバー攻撃者は、パスワードを推測または、”ブルートフォース”する高度な手法を開発しているだけでなく、これらの手法がどんどん高度化しているのが目下の課題です。つまり、弱いパスワードや簡単に推測できるパスワードを使っている場合、パスワードを攻撃者にハックされてしまうということです。一般的にパスワードの文字列が多ければ多いほど、強度が上がり、攻撃者は推測しにくくなりますが、長く複雑なパスワードは記憶するのは大変です。そこで、パスフレーズの利用を推奨します。これは、記憶することが容易な短いフレーズや文章をパスワードにしたもので、覚えやすくかつ攻撃者がハッキングしづらいものです。以下は、一例です。

Where is king Julian? (Julian王はどこにいる？)

このパスフレーズが強い理由は、21文字であるだけでなく、大文字や記号（スペースや句読点は記号と見なされます）を使っているからです。さらに、文字を数字や記号と置き換えることでパスフレーズを強くすることもできます。例えば、’a’ を ‘@”、’o’を数字のゼロと置き換えることです。ただし、ウェブサイトやプログラム側でパスワードに使える文字数に制限がある場合は、許可されている最大限の文字数を使用してください。

パスフレーズを安全に利用するために

パスフレーズを利用する際に注意しなければならない点がいくつかあります。攻撃者によって簡単にパスフレーズを取得されたり、コピーされたりするようでは、意味がありません。

パスフレーズについて

1. 各アカウントやデバイスごとに違うパスフレーズを設定してください。例えば、会社や銀行用のアカウントのパスフレーズを、Facebook、YouTubeやTwitterなどの個人アカウントと同じものを設定してはいけません。こうすることで、一つのアカウントがハッキングの被害に遭っても、他のアカウントの安全性を維持することができます。覚えなければならないパスフレーズが多い場合（良くあることですが）、パスワードマネージャーの利用を検討してください。パスワードマネージャーは、すべてのパスフレーズを安全に保管するための補助プログラムです。これを利用することにより、パソコンとパスワードマネージャー用のパスフレーズだけを記憶するだけで済ませることができます。

個人情報や身元情報を守るために、パスフレーズを利用するのは、非常に効果的な手段です。

2. 会社の同僚も含めて、他人とパスフレーズや作り方を共有してはいけません。パスフレーズは、秘密であることを思い出してください；他人にパスフレーズを知られるということは、もはや秘密ではないということです。パスフレーズを誤って共有してしまった場合、パスフレーズが漏えいまたは窃取された恐れがある場合は、直ちにパスフレーズを変更してください。

3. パスワードと同様に、推測が容易または一般的に利用されるパスフレーズを設定しないようにしてください。例えば、“Four score and seven years ago（訳注：リンカーンによる演説の一節）”は広く知られているフレーズであるため、良いパスフレーズとは言えません。

4. 空港や図書館などに設置されている公共利用が可能なパソコンを使って、会社や銀行のアカウントにログインしないでください。これらのパソコンは誰でも利用可能であるために、すべてのキーストロークをキャプチャするための悪意あるコードやプログラムが仕込まれているかもしれません。

5. 個人的な情報を引き出す質問をするウェブサイトには気をつけてください。これらの質問は、パスフレーズを忘れてしまったときに、そのパスフレーズをリセットする目的で使われます。しかし、これらの質問に対する回答をFacebookなどの投稿から見つけることが可能である場合があるため、これらの個人的な秘密に対する回答を設定する際には、インターネット上で公開していないものや、架空の情報を使うようにしてください。多くのパスワードマネージャーは、このような追加の情報も保管可能ですので、ご活用ください。

パスフレーズについて

6. 多くのオンラインアカウントは、2段階認証という機能を提供しています。この機能は、ログインする際にパスフレーズ以外の情報、例えば、スマートフォン宛に送られるパスコードなども必要とするログイン方法などを指します。この方法は、パスフレーズのみを使った場合と比べ、セキュリティは格段に向上させることができます。可能な限り、提供されているシステムの中から強い認証方法を利用するようにしてください。

7. モバイル機器は、PINを使ってアクセスを制限する機能を提供しています。PINは、パスワードの一種に過ぎないということを頭に入れてください。PINが長ければ長いほど、安全です。多くのモバイル機器は、PIN番号から、パスフレーズに変更する機能を提供しています。

8. 最後に、使用していないアカウントは、閉鎖、削除または無効化してください。

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

2段階認証について:	http://www.securingthehuman.org/ouch/2013#august2013
パスワードマネージャーについて:	http://www.securingthehuman.org/ouch/2013#october2013
ソーシャルエンジニアリングについて:	http://www.securingthehuman.org/ouch/2014#november2014
一般的なセキュリティ用語:	http://www.securingthehuman.org/resources/security-terms

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