OUCH! | 2017 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...

- パスフレーズについて
- パスフレーズを安全に利用する
- 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、オンラインバンキング、買い物やスマートフォンへのアクセスを行うために毎日利用するものです。しかし、パスワードは一番の弱点でもあります。第三者にパスワードを推測または知られてしまったら、自分自身に成りすまされた状態でアカウントにアクセスされてしまいます。結果として、あなたが意図しない送金をしたり、メールを読んだり、なりすまし犯罪の被害者になったりしてしまうということです。そのためにも、自分を保護するための強いパスワードは不可欠です。しかし、パスワードを複雑なだけにしてしまうと、あなたが記憶することも入力することも大変になるでしょう。このニュースレターでは、記憶することが容易で、入力することも簡単な強いパスワードの作成方法を紹介します。これらは、パスフレーズと呼ばれているものです。

ゲストエディタ

ミー・ノップ・ウィン氏は、Secured IT Solutions社のCEO/Pricinpal Consultantであり、SANS認定講師として活躍しています。彼女は、14年以上、様々な業界に対しセキュリティプログラムの開発や成熟度に合わせた助言の提供、およびマネジメントをしてきた経験を活かして、様々な専門知識を提供しています。また、ツイッターやLinkedInで情報も発信しています。(@MenopN、My-Ngoc "Menop" Nguyen)

パスフレーズについて

今、直面している課題として、サイバー攻撃者はパスワードに対してブルートフォース攻撃（総当たりかつ自動推測）を行う高度で効果的なツールを開発していることが挙げられます。そのため、弱いパスワードまたは推測が容易なパスワードを利用している場合、攻撃者によって容易に解析されてしまいます。自分自身を保護するためにできる重要なことは、強いパスワードを利用することです。通常、これは複雑なパスワードを作るところから始まりましたが、これらの多くは記憶することが難しく、複雑で入力するのも大変でした。そこで、一つの文章または複数の言葉を組み合わせたパスフレーズの利用を推奨するようになってきています。パスフレーズに使われる文字数が多ければ多いほど強くなるだけではなく、覚えやすく、入力もしやすく、さらにサイバー攻撃者によってハッキングされにくくなるという利点もあります。以下に2つの例を示します。

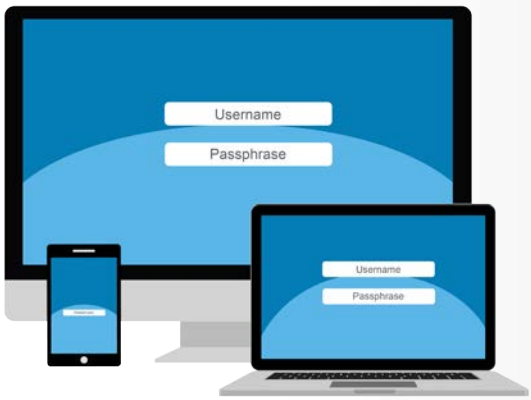
SUSTAIN-EASILY-IMPRISON
TIME FOR TEA AT 1:23

これらのパスフレーズが強い理由は、長いだけでなく、大文字と記号（スペースや句読点も記号です）を使っていることです。そして、これらは、覚えやすく、入力もしやすいでしょう。文字を数字や記号に置き換えることでパスフレーズをさらに強くすることができます。例えば、'A' を '@' に 'O'を数字のゼロで置き換えるなどが挙げられます。ウェブサイ

© SANS Institute 2017

パスフレーズについて

トまたはプログラムによってパスワードに文字数制限が設けられている場合、許可されている最大の文字数を利用してください。



パスフレーズを利用することで、強いパスワードをより簡単に作成・記憶することができます。

パスフレーズを安全に利用する

パスフレーズの利用にも気をつけなければなりません。攻撃者によってパスフレーズを簡単に盗まれてしまったり、コピーされてしまったらパスフレーズを利用しても意味はありません。

1. それぞれのアカウントと機器ごとに異なるパスフレーズを利用してください。例えば、業務やオンラインバンキング用に使っているパスフレーズを FACEBOOKやYOUTUBE、TWITTERなどで利用しないでください。こうすることで、一つのアカウントがハッキングされても、他のアカウントは安全なままです。記憶し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）、パスワードマネージャの活用を検討してください。これは、すべてのパスフレーズを安全に保管してくれる特殊なプログラムです。これで記憶しなければならないパスフレーズは、パソコンまたはデバイスのパスフレーズとパスワードマネージャ用のパスフレーズのみになります。
2. パスフレーズやパスフレーズを生成するための手法を同僚や上司など、他人と共有しないでください。パスフレーズは秘密の情報であることを忘れてはいけません。他人に知られてしまったら、安全ではなくなります。パスフレーズを誤って他人と共有してしまった場合、あるいはパスフレーズを盗まれたという疑念を持った場合は、直ちに変更してください。例外として、緊急の際に利用できるように信頼できる家族のメンバーと一部の重要なパスフレーズを共有することが挙げられます。一つの共有方法として、これらのパスフレーズを紙に書き（業務用のものは除きます）、安全な場所に保管することで、その場所を家族と共有することができます。こうすることで、自分自身に何かあった場合でも、家族によって重要なアカウントへのアクセスが可能になります。
3. ホテルやインターネットカフェなどの公共のパソコンを利用して、インターネットサービスや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できるため、何かに感染していた場合、キーストロークのログが取られる可能性があります。アカウントへのログインは、信頼できるパソコンまたはモバイルデバイスのみから行ってください。
4. 個人情報に関する質問をしてくるウェブサイトには注意してください。これらの質問は、パスフレーズを忘れた際にリセットするために聞かれます。これらの質問に対する回答の問題は、インターネット上に回答が公開されていることが多い事です。自分自身のFACEBOOKのページなどが例として挙げられます。このような個人的な質問に対する回答には、非公開の情報または自分で作った偽物の情報を使うようにしてください。これらの質問に対する回答をすべて覚えられない場合…　この場合は、映画のキャラクターなど、テーマを決めて、このキャラクターに関することを

© SANS Institute 2017

パスフレーズについて

回答にしてみてください。もう一つの手法として、パスワードマネージャの利用が挙げられます。多くのパスワードマネージャには、これらの質問と回答を保管する機能が付いています。

5. 多くのオンラインアカウントでは、2段階認証または2要素認証と呼ばれる機能が提供されています。これは、ログインするためにパスフレーズ以外にも何かの入力を必要とするものです。例えば、スマートフォンに送られるコードなどがありますが、パスフレーズのみを利用するよりも安全です。利用が可能な場合は、この機能を有効にして、強い認証方法を優先的に利用してください。
6. モバイルデバイスは、多くの場合、アクセスするためにPINを要求します。PINは、単なるパスワードであることを忘れないでください。PINは、長ければ長いほど安全になります。多くのモバイルデバイスでは、PIN番号をパスフレーズや指紋などの生体認証に変更できます。
7. アカウントを利用していない場合は、アカウントの閉鎖、削除または無効に設定してください。

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。
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、国内でも有数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

パスワードマネージャ:	https://securingthehuman.sans.org/ouch/2015#october2015
2段階認証について:	https://securingthehuman.sans.org/ouch/2015#september2015
Lock Down Your Login (ログインの保護):	https://lockdownyourlogin.com
SANS SEC301 - Five day course on cyber security basics :	https://sans.org/sec301

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, Cathy Click, Cheryl Conley
Translated By: 内山　貴之, 時田　剛