2021 年 9 月 16 日

日本マイクロソフト株式会社

あなたの Microsoft アカウントにパスワードレスの未来を

Vasu Jakkal
Corporate Vice President, Security, Compliance and Identity

※本発表は、米国時間 9 月 15 日に公開された “The passwordless future is here for your Microsoft account” の抄訳です。

パスワードが好きな人など存在しません。不便なうえに、攻撃の主なターゲットとなります。にもかかわらず、パスワードはメールや金融サービス、ショッピング、そしてビデオゲームなど、デジタルライフ全体で主要なセキュリティレイヤとして浸透しています。

私たちは日々複雑で独自のパスワードを作成し、それを覚えて頻繁に変更するよう求められますが、これらを好んで対応する人はいませんよね。 最近のマイクロソフトで行った Twitter 上の投票によると、5 人に 1 人が、パスワードをリセットするくらいなら、誤って「全員に返信」をクリックして恥をかいた方が良いと回答しています。

しかし、私たちに一体どんな代替となる手段があるというのでしょうか。

私たちは、ここ数年の間、パスワードレスの未来が来ることをお伝えしてきました。そして本日、パスワードレスの未来に向けたビジョンの次のステップを発表します。 2021 年 3 月、私たちは世界中の法人組織に向けて、パスワードレスのサインインの機能の提供開始を発表しました。

本日より、Microsoft アカウントから完全にパスワードをなくすことが可能になります。Microsoft Authenticator アプリ、Windows Hello、セキュリティキーもしくは、電話や email で受け取った確認コードで、Microsoft Outlook、Microsoft OneDrive、Microsoft Family Safety といったお気に入りのアプリケーションやサービスに、より便利に、そして安全にアクセスできるようになるのです。この機能は今後数週間をかけて展開していく予定です。

パスワードの問題点

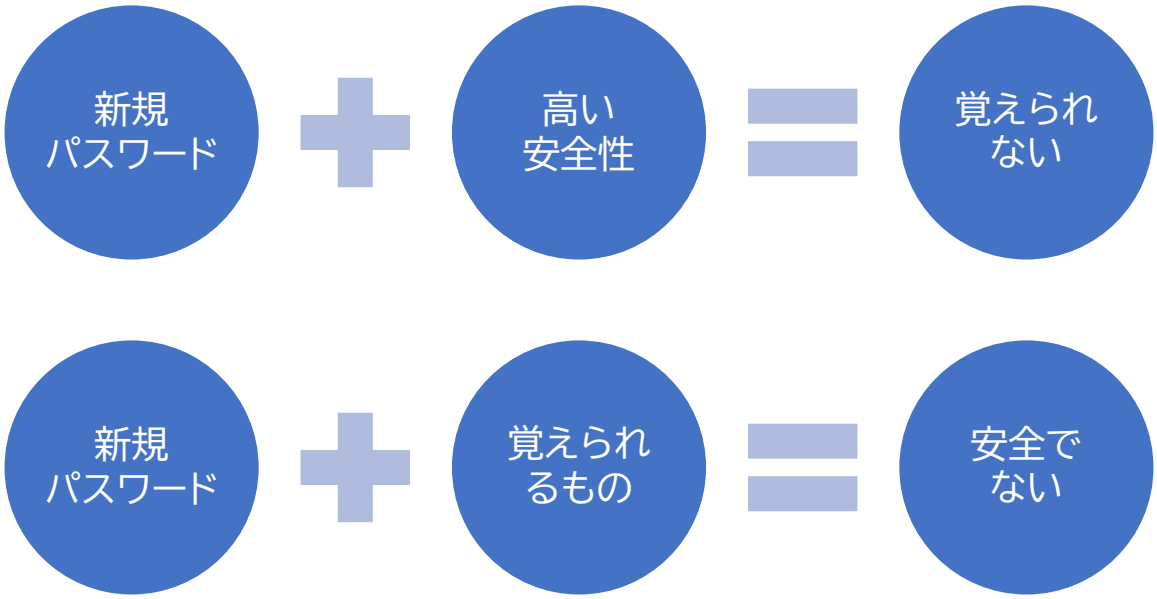
私の友人でマイクロソフトの CISO（最高情報セキュリティ責任者）であるブレット アーセナル（Bret Arsenault）は、「ハッカーは侵入するのではなく、ログインするのだよ」とよく言います。あまりにも核心を突いた言葉で、初めて聞いた時からずっと私の心に残っています。

大企業から一人一人のお客様に至るまで、脆弱なパスワードこそ大半の攻撃の入口となっています。事実、パスワード攻撃は毎秒 579 回もの頻度で発生しており、年間ではその件数が 180 億回にのぼります。

なぜパスワードはこんなに脆弱なのでしょう？ ここには2つの理由があります。

人間の本質そのもの

絶対覚えられそうにない自動生成のパスワード以外、私たちはだいたい自分でパスワードを作成しています。しかし、パスワードの脆弱性を考えると、パスワードの要件は、近年、複数の記号、数字、大文字と小文字の区別、以前のパスワードの禁止など、ますます複雑になっています。更新は定期的にかつ頻繁に求められますし、十分に安全で記憶に残るパスワードを作成し続けることは難しい課題です。私たちの生活の中で、すべてのアカウントを作成、記憶、管理をしなければならないパスワードは非常に不便なのです。



パスワードを忘れてしまうことも非常につらいですよね。私は、3 分の 1 近くの人が、紛失したパスワードに対峙するのではなく、**アカウントやサービスの利用そのものを完全にやめてしまう**と言っていることを知り、ショックを受けました。

問題を解決し、私たちが覚えられるパスワードを作るために、私たちは、よく知られた単語や個人的なフレーズなど自分たちにとってより簡単な方法を取ろうとしてしまいます。最近の調査では、**自身のペットの名前からパスワードを思いついたという人が 15%**であることがわかりました。他にも共通する回答として、家族の名前や誕生日のような重要な日付が含まれていました。また、**10 人に 1 人がサイト間でパスワードの再利用**を認めており、**40%がパスワードの数式を使用した**と言っています。例えば、Fall2021 というパスワードは Winter2021 となり、最終的には Spring2022 へとなっていくでしょう。

ハッカーの本質によるもの

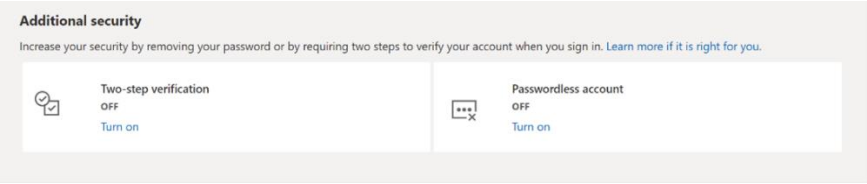
残念ながら、そのようなパスワードは覚えやすいかもしれませんが、一方でハッカーが推測しやすいことにもつながります。 誰かのソーシャルメディアをちらりと見ただけで、ハッカーは個人アカウントにログインするヒントを得ることができるのです。 一度パスワードと電子メールの組み合わせが侵害されれば、ダークウェブなどで販売され、多くの場合、さらなる攻撃に使用されてしまいます。

また、ハッカーは数多くのツールやテクニックを持っています。ハッカーはパスワードスプレーを使用し、さまざまなパスワードの候補を素早く試してアカウントにアクセスします。フィッシングを利用して偽サイトに認証情報を入力させることもあるでしょう。こうした手口は比較的単純で、何十年も前から使われているものですが、パスワードは人間が作成したものであるかぎり、今でもこの手口が通用するのです。

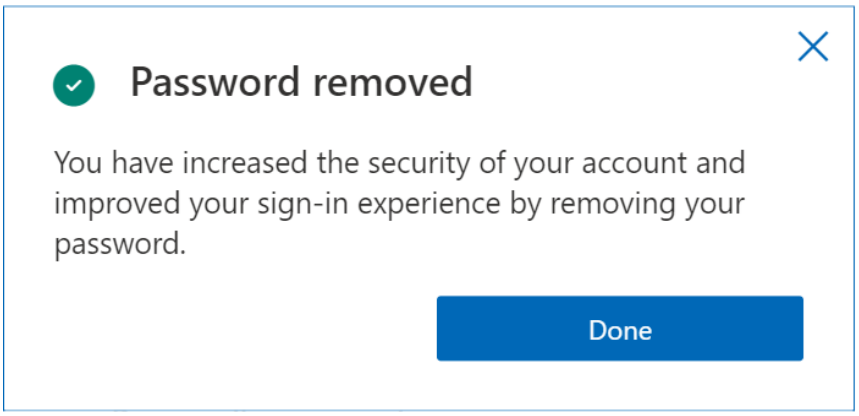
今日からたった数クリックでパスワードレスに

まず、Microsoft Authenticator アプリをインストールし、個人用のMicrosoft アカウントに紐付けてください。

次に、自身のMicrosoft アカウントにアクセスし、**「高度なセキュリティオプション」**を選択します。**「追加のセキュリティオプション」**の中に、**「パスワードレスアカウント」**があります。これを**オン**にしてください。



そして、画面の指示に従い、Authenticator アプリからの通知を承認してください。承認がされたら、あなたはパスワードから解放されます。



パスワードを使いたい場合は、いつでもアカウントにパスワードを追加することが可能です。でも、まずはパスワードレスを試してみてください - 1度使い始めたら、きっと戻れなくなるはずです。

パスワードレスをより深く知る

マイクロソフトと共にパスワードレスへの道のりを歩んでいる企業のお客様からは、すばらしいフィードバックをいただいています。マイクロソフトも自らが実験台となっており、従業員のほぼ 100%がパスワードレスを選択して企業アカウントにログインしています。

パスワードレスへの道のりについては、コーポレートバイスプレジデント Identity 担当の Joy Chik のブログに詳細が書かれています。また、Edge や Microsoft 365 アプリをお使いの方への利点をより詳しく知りたい方は、Liat Ben-Zur のブログをご確認ください。 Microsoft Active Directory や Microsoft Authenticator といったマイクロソフトソリューションを活用し、組織内のユーザーが保護された状態にありながら、パスワードを忘れることが許される方法をより詳しく知りたい方は、2021 年 10 月 13 日のデジタルイベント「Your Passwordless Future Starts Now」 に是非ご参加ください。

Microsoft Authenticator アプリを使ったパスワードレスを有効化する方法の詳細はこちらをご覧ください。