Microsoft Security

サインイン プロセスを保護する

オンライン アカウントの安全性を確保するための最も重要な方法の 1 つは、サインイン プロセスをセキュアに保つことです。

このアドバイスに従って、悪意のある人の手からアカウントを守ることができます。

1 強力なパスワードを 作成する

ハッカーは押し入ることなく、サインインできてしまいます。 サインイン プロセスの一環としてパスワードを使用する場合は、可能な限り強力であることを確認する必要があります。

強力なパスワードとは

- 少なくとも 12 文字にする (14 文字以上が適しています)
- 大文字、小文字、数字、記号を組み合わせる
- 辞書に載っている単語や、人、キャラクター、製品、組織の名前を使用しない
- これまで使ったパスワードとまったく違う
- 覚えているのは簡単でも、他の人が推測するのは難しい
- 安全性の高いアカウント パスワードを Microsoft Edge が自動的に生成して保存することを許可する

2 パスワードをセキュアに保つ

ハッカーが解読できない強力なパスワードを作成したら、セキュアに保つ必要があります。パスワードを破ることができない場合、犯罪者はユーザーを騙して明らかにしようとします。

パスワードを可能な限りセキュアに保つには、次のガイドラインに従ってください。

- 誰ともパスワードを共有しない (友人や家族とも共有しない)
- メール、インスタント メッセージ、または確実にセキュアではないその他の通信手段によってパスワードを送信しない
- 同じパスワードを再利用しない。すべてのパスワードは一意である必要があります
- パスワードは頻繁に更新する
- 必ず信頼できるリンクを使用して Web サイトにアクセスする
- 侵害された恐れがあると思われるアカウントで、すぐにパスワードを変更することを躊躇しない

3 パスワードを完全になくす

強力なパスワードを作成してセキュアに保つには、多くの作業を伴う可能性があります。すべてのアカウントで覚えておいて管理する必要がある複数のパスワードがある場合は特にです。
しかし、パスワードをまったく管理する必要がなかったらどうでしょうか?
Microsoft Authenticator アプリ、物理的セキュリティ キー、生体認証などのパスワードレス サインイン手法は、盗難やハッキング、または推測される可能性のある従来のパスワードよりも安全です。

サイバーセキュリティ意識に関するその他のトピックとスキルアップの機会については、https://aka.ms/cybersecurity-awareness をご覧ください。

Microsoft Security