Microsoft Security

データとインターネット接続されたデバイスを保護するための 12 のヒント

メール、アカウント、デバイス (組織のネットワークに接続されているものを含む) をサイバー攻撃からより安全に保護するための 12 のヒントをご紹介します。

1

リンク付きのメッセージ、特に個人情報を求めるものには注意が必要

偽のリンクや Web サイトはとても巧妙に作られている場合があります。リンクを信頼することなく、差出人の公式 Web サイトで電話番号を探し、直接電話をかけてメッセージが本物であるかを確認するようにしましょう。

2

添付ファイル付きのメッセージに気を付ける

信頼できる人や組織からのものだと思っても、想定外の添付ファイルは決して開かないでください。重要なメッセージかもしれないと心配な場合は、差出人に電話して確認しましょう。

3

個人情報の共有はリアルタイムでのみ行う

個人情報の共有は、対面または電話で行うのがベストです。どうしても個人情報をメールで送らなければならない場合は、Microsoft Outlook の暗号化ツールを使用してください。

4

パスワードレスに移行し、認証アプリを使用してセキュリティを強化する

パスワードがなければ、パスワードを盗まれることはありません。Microsoft アカウントの パスワードレスをオンにして、電話または Windows Hello でサインインしましょう。

5

パスワードを使用する必要がある場合は、パスワード マネージャーを使用して強力でユニークなパスワードにする

強力なパスワードには、14 以上のランダムな文字と記号を使用します。Microsoft Edge を使用すると、パスワードの記憶や変更管理を行うことができます。

6

すべてのモバイル デバイスでロック機能を有効にする

デバイスのロック解除には、PIN、指紋、または顔認証を必須としましょう。

7

ソフトウェアの更新プログラムをすぐにインストールする

アプリ、ブラウザー、オペレーティング システムの更新プログラムの多くには、現在進行中の問題に対するセキュリティ修正プログラムが含まれているため、速やかにインストールして最新のセキュリティ基準を維持してください。

8

デバイス上のすべてのアプリが正当なものであることを確認する

デバイスに対応した公式のアプリ ストアからのみ、アプリをインストールしてください。

9

Windows 11 を使用し、改ざん保護をオンにしてセキュリティ設定を保護する

常に最新バージョンの Windows を使用しましょう。改ざん保護機能は、セキュリティ設定に対する不正な変更をブロックしてくれます。

10

攻撃対象となる領域を削減する

不要なインターネット接続を消去し、開いているポートを制限して、スキャン ツールでデジタル環境の潜在的な弱点を確認することにより、対策を講じてリスクを軽減することができます。

11

ファームウェアのスキャン ツールを使用する

作業環境に潜在的な弱点がないかを確認することにより、対策を講じてリスクを軽減することができます。

12

システム定義を含むファイルを転送しないこと

セキュリティ保護されていない経路や、関係者以外の人物にシステム定義を送ることは、デジタル環境への攻撃を可能にし、プロセスの破壊や環境の脆弱性を招くおそれがあります。

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、下記のページをご覧ください https://aka.ms/cybersecurity-awareness

Microsoft Security