Microsoft Security

テクニカル サポート詐欺の 5 つの兆候

テクニカル サポート詐欺では、犯罪者がユーザーにソフトウェアやデバイスの修復が必要だと信じさせようとします。一部の詐欺師は、存在しない問題を「修正」するために料金を請求しようとすることがあります。また、個人データや財務データを盗もうとしたり、ランサムウェアを展開するためにネットワークにアクセスしようとしたりする詐欺師もいます。

テクニカル サポート詐欺の次の被害者にならないようにしましょう。ここでは、テクニカル サポート詐欺の 5 つの兆候と、攻撃を受けていると気づいたときの対処に役立つ情報をご紹介します。

1 もし、こうなったら...

テクニカル サポートと名乗る人物から、予期せず電話がかかってくる (注意してください。偽の発信者 ID を生成するツールを持っている詐欺師もいます)。

覚えておくべきこと

マイクロソフトが迷惑電話をかけることはありません。お客様からのご連絡がない限り、テクニカル サポートを提供するための電話をすることはありません。

2 もし、こうなったら...

至急電話するようにというエラー メッセージが表示される。

覚えておくべきこと

マイクロソフトのエラー メッセージに電話番号が含まれることはありません。Microsoft Edge ブラウザーは、Microsoft Defender SmartScreen を使用して既知のサポート詐欺サイトをブロックします。

3 もし、こうなったら...

テクニカル サポートの担当者から、「問題」を解決するために暗号通貨やギフト カードでの支払いを求められる。

覚えておくべきこと

正規のサポート技術者は、サービスを提供する前に料金をお伝えします。また、支払いが必要な場合でも、ギフト カードやビットコインなどの暗号通貨で支払うことはありません。

4 もし、こうなったら...

サポート技術者が、メールやサードパーティのWebサイトからソフトウェアをダウンロードするように求めてくる。

覚えておくべきこと

ソフトウェアは、必ず公式の Web サイトまたはアプリ ストアからダウンロードできるようになっているはずです。すべてのマイクロソフト ソフトウェアは、マイクロソフトの公式 Web サイトまたはパートナーの公式 Web サイトからダウンロードできます。

5 もし、こうなったら...

テクニカル サポートから、パスワードやその他の機密データを入力するよう求められる。

覚えておくべきこと

マイクロソフトのテクニカル サポートが、パスワード、社会保障番号、その他の個人データを求めることはありません。

テクニカル サポート詐欺に遭ったと思われる場合の対処方法

- インストールするように詐欺師から指定されたアプリケーションをすべてアンインストールする。
- Windows Security でフルスキャンを実行し、マルウェアがあればすべて削除する。
- コンピューターへのアクセス権を詐欺師に与えてしまった場合は、デバイスをリセットする。
- パスワードを変更する。
- 支払いを実行してしまった場合は、できるだけ早くクレジット カード会社に連絡する。
- www.microsoft.com/reportascam で詐欺を報告する。
- 危険な Web サイトを報告する。Microsoft Edge で、[設定など] > [ヘルプとフィードバック] > [安全でないサイトを報告する] を選択します。

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、
https://aka.ms/cybersecurity-awareness.

Microsoft Security