FORTRA
Terranova Security | Microsoft Security

フィッシングから身を守るための 7 つの方法

フィッシングとは、犯罪者が欺瞞と策略によって情報やアクセスを得ようとする詐欺のことです。詐欺師は信頼できる企業や個人のふりをしたり、マルウェアを無害に見えるよう偽装させてシステムにインストールさせようとすることがあります。

一般的なフィッシング攻撃

コンテンツ インジェクション

この種のフィッシング攻撃は、メールのログイン ページやオンライン バンキングのポータルなど、使い慣れた Web サイトに悪意あるデータを注入するものです。ユーザーを別の Web サイトに誘導するリンク、フォーム、ポップアップなどがあり、誘導先で機密情報の入力を求めます。

リンクの操作

フィッシング詐欺は、大企業や有名ブランドなどの信頼できる発信元から来たように見える、悪意あるリンクの形式で行われることもあります。リンクをクリックしたユーザーは偽装 Web サイトに誘導され、アカウント情報の入力を求められます。

メール

このリストの中でも群を抜いて最もよく見られるフィッシング メールは、個人用または仕事用のメール アドレスに届く可能性があります。このメールには、手続きの指示、クリックするための Web リンク、開くための添付ファイルが含まれていることがあります。

中間者

中間者攻撃タイプのフィッシングでは、サイバー犯罪者が 2 人の人間を騙して互いに情報を送信させることで成り立ちます。詐欺師が虚偽の要求を送信したり、各当事者が送受信しているデータを改ざんしたりします。

スピア フィッシング

より高度な形式のフィッシングであるスピア フィッシングは、ランダムな標的ではなく特定の個人を標的にします。

フィッシング攻撃にかかると、機密情報の漏洩、ネットワークの感染、金銭の要求、データの破損、あるいはさらに悪い事態につながる可能性があります。そうならないための方法をこれからご紹介します。

1

差出人のメール アドレスを調べましょう。すべて問題ありませんか? 文字のずれやおかしなスペルがあれば、偽物の可能性があります。

2

一般的なあいさつ文(「お客様各位」など)を使用した、緊急の行動を求めるメールには注意が必要です。

3

差出人の連絡先情報を確認できるものを探しましょう。怪しいと感じた場合は、返信しないでください。代わりに新しいメールを開始して返信します。

4

機密情報は絶対にメールで送らないでください。個人情報を伝えなければならない場合は、電話を使用しましょう。

5

想定外のリンクをクリックする際、特にアカウントにログインするよう指示された場合は、よく考えてください。安全のために、公式 Web サイトからログインしましょう。

6

不明な差出人、普段添付ファイルを送ってこない友人からのメール添付ファイルを開くことは避けてください。

7

メール アプリ用のフィッシング フィルターをインストールし、メール アカウントのスパム フィルターを有効にしましょう。

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。

FORTRA
Terranova Security | Microsoft Security