フィッシングによる被害に遭わないために

フィッシング詐欺とは、実在する公的機関や有名企業を装ったメールや SMS（ショートメッセージサービス）を送信し、正規のウェブサイトを模倣したフィッシングサイト（偽のウェブサイト）に誘導して、名前や生年月日などの個人情報、ID やパスワードなどのアカウント情報、クレジットカード番号やセキュリティコードなどのクレジットカード情報を盗み出す行為のことをいいます。フィッシング（phishing）の語源は、「fishing」（魚釣り）と「sophisticated」（洗練された）で、フィッシングはこれらを組み合わせた造語だといわれています。また、盗まれた情報は、不正購入や不正送金などに悪用され、金銭的な被害が発生しています。

最近では、電子メールの送信者名を偽り、【緊急】や【重要】などの言葉をつけて受信者の不安を煽るタイトルにしたり、誘導先のフィッシングサイトも本家本元の Web サイトをコピーして作られているため、ひと目ではフィッシングサイトであると判別できないケースが多く、手口が年々巧妙になっています。

○ 攻撃手口

（出典　IPA 独立行政法人情報処理推進機構）

● 企業等を装ったメールや SMS を不特定多数のアドレスに送信する

実在する企業を装い、フィッシングサイトへの URL が表示されたメールや SMS 等を送信し、フィッシングサイトへ誘導する。

正規のウェブサイトの問い合わせフォームの自動返信機能を悪用してメールをばらまく方法もある。

● 電子掲示板や SNS の投稿サイトから誘導する

電子掲示板や SNS の投稿サイトに、フィッシングサイトの URL を投稿し、その書き込みを見たユーザーに URL リンクをクリックさせ、フィッシングサイトへ誘導する。

● 検索サイトの検索結果に偽の広告を表示させる

検索エンジンの画面に表示される広告の仕組みを悪用して偽の広告を表示させ、フィッシングサイトへ誘導する。

対策

● 多要素認証を活用する

ワンタイムパスワードや指紋認証など、複数の認証方式を組み合わせ、セキュリティを向上させる。

● メール、SMS、SNS に表示された URL に、安易にアクセスしない

金融機関などの ID・パスワードを入力する Web ページにアクセスする場合は、金融機関からあらかじめ通知されている URL を Web ブラウザに直接入力するか、普段利用している Web ブラウザのブックマークに金融機関の正規の URL を登録しておき、ブックマークからアクセスする。

● 重要な情報の入力時は、SSL(Secure Socket Layer)が採用されているかを確認する

通常、インターネットバンキングへのログイン画面やクレジットカード番号などの重要な情報の入力画面では、SSL という暗号化技術が使用されており、重要な情報の入力を求めるページで、SSL が使用されていない場合は、フィッシング詐欺の可能性を疑う。

SSL の通信であるかどうかは、Web ブラウザの URL 表示部分（アドレスバー）や運営組織名が緑色の表示になっているか、鍵マークが表示されているか、などで確認する。

【参考】・ IPA 独立行政法人情報処理推進機構(情報セキュリティ 10 大脅威 2021[個人編]) https://www.ipa.go.jp/files/000089480.pdf

・ 総務省-国民のための情報セキュリティサイト（フィッシング詐欺に注意） https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/05.html

岩手県警察本部サイバー犯罪対策課の公式ツイッターはQRコードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

岩手県警察本部生活安全部サイバー犯罪対策課

令和3年 11 月 1 日発行

@Iwate_cyber