本号は３頁あります
風早北部ふるさと協議会
防犯防災部 作成
2023年10月20日
第 160 号

風早北部防犯情報 しょうなん

具体的行動に優る策なし

SHOW “No Action No-result”

フィッシング詐欺が着実に蔓延中

迷惑メール相談センターホームページより情報を 3 ページでご案内します

フィッシング対策委員会ホームページによりますと、フィッシング事案報告件数が、毎月の発生には増減がありますが、今年５月以降も着実に高水準で推移しており、問題が深刻化しています。

本号では、フィッシング詐欺の実情とその対応策を、「撃退！詐欺メール&SMS」サイト情報を引用してご案内します。詐欺で個人情報を盗まれたり、大切なあなたの資産が奪われないよう、是非警戒してください。

はじめに・・・フィッシング(サイト)とは？

実在する(著名な)企業名を装って詐欺のメールを送りつけ、そのメールを信じ込んで返信(応答)することで、偽のサイト(これをフィッシングサイトと称します)へ誘導、クレジットカード番号、アカウント情報の ID、パスワードといった個人情報を盗み取り、最終的に現金や預貯金･金融資産を騙し取られてしまいます。下の図説を参照ください。

事例：
詐欺メールの例

最近のフィッシング詐欺メールやSMSメッセージは、一段と悪質・巧妙になっています。紹介する事例を参考に、似たようなメールやメッセージがきたら、詐欺かもしれないと疑うクセをつけましょう。

ショッピングサイトになりすました偽メール

銀行やカード会社になりすました偽メール

宅配業者になりすました偽メール

SMSを利用した偽メッセージ（スミッシング）

性的な写真や動画をばらまくと脅迫し、仮想通貨を要求するメール

手口：
だましのテクニック

不審に思わせない手口

まず、ネットショッピングの注文確認、宅配会社の不在通知、カード会社の連絡など普段利用しているサービスを装って、不審感を持たせないようにします。

不安にさせる手口

次に、「重要」「警告」「セキュリティ」「アカウントロック」などの強い言葉で受信者の冷静な判断力を奪います。

不正サイトへ誘導する手口

不安にさせた後、「○○はこちら」などと、不安を回避するための手段（安心）を提示して不正サイトへ誘導します。

だまされないコツ：ゼロトラスト

最近の詐欺メールは非常に精巧に作られています。本物かニセモノかを見分けることが難しく、"日本語やURLがおかしくないか"などを確認する方法だけでは、見極めに限界があります。
そこで、「最初から信頼せずにきちんと確認を行う」というセキュリティ分野での考え方「ゼロトラスト」への転換が必要になります。
メールを受信したときは、たとえ、公式メールだと思っても、最初は『決して信頼せず、きちんと確認する』**ゼロトラスト3つの基本**の考え方が大切になります。

コツ１ メールを開かない

スマホでは、送信者と件名に、数行の本文が表示されています。それ以上開くことはやめましょう。件名で**「緊急」「重要」「セキュリティ」などを強調していれば、メールを開かない**方が安全です。

コツ２ リンクをタップしない

URL・リンクをタップすると詐欺サイトへ誘導されてしまう危険があります。**公式メールだと思ったとしてもタップしない**で、確認は、公式サイトやブックマーク、アプリから事業者サイトにアクセスするようにしましょう。

コツ３ 入力しない

クレジットカード情報や、ＩＤ・パスワードなどの情報の入力や確認を求められても、**絶対に入力しないようにし**ましょう。

予防＆対処法

予防：詐欺メールへの備え

詐欺メールやメッセージ、不正サイトでの被害にあわないため、日頃の備えを実施して予防しましょう。

迷惑メールフィルタリングの利用

携帯電話会社や多くのプロバイダでは、メールフィルタリングサービスを提供しています。このサービスを利用して、迷惑メールや詐欺メールを受信しないで済むようにしておきましょう。

セキュリティソフトの利用

セキュリティソフト（アプリ）を利用すれば、うっかりメールのリンクをタップしてしまった場合でも、詐欺サイトへのアクセスや不正ソフト（アプリ）のインストールリスクを低減できます。

OSは常に最新に

迷惑メールの中には、OSやソフト（アプリ）の脆弱性を利用してマルウェア（悪意のあるソフトウェア）を送り込もうとするものもあります。常に最新バージョンにして脆弱性を塞いでおくことを心がけましょう。

対処法：困ったらすぐ相談

詐欺の手口は高度化し、詐欺と気づかずだまされてしまったり、後になって不安に思う方も多くいます。二次被害を防ぐためにも、困ったときは一人で悩まず、**関係機関に相談**してください。

よくあるケース１： メールのURLを開いた

メールを開くだけでは危険性は低いですが、リンクをタップしてしまうと、アクセスしたことが送信者に伝わり、迷惑メールが増えたり、他の詐欺メールが届く可能性があります。**もし、覚えのない料金請求メールが届いても支払わず**、消費生活センターなどへ相談しましょう。

よくあるケース２： 個人情報を入力した

クレジットカード番号やアカウントID、パスワードなどを入力してしまうと不正利用される恐れがあります。**すぐにカード会社や銀行、ご利用サービスの相談窓口に連絡をして対応しましょう。**問い合わせは、メールのリンクではなく、ブックマークやアプリからアクセスするようにしましょう。

よくあるケース３： ウイルスに感染したかも

ウイルス感染が疑われるときは、まず**機内モードにして、インターネットに接続しないようにしましょう。**その後に、セキュリティアプリでスキャンして不審なアプリがインストールされていないかを確認したり、最終手段としてスマホを初期化するなどの対処法があります。詳しくは以下のページを参考にしてください。