大手ECサイトになりすました偽メール

●本物そっくりの詐欺メール・フィッシングサイトに要注意

スマートフォンのアプリやブラウザから気軽にオンラインで買い物をする機会が増えています。

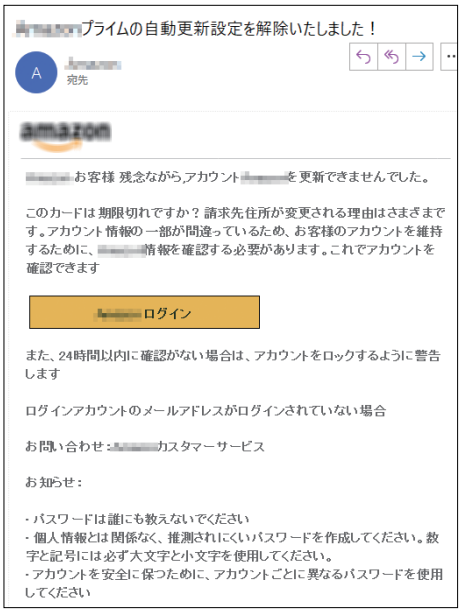
普段からお知らせや購入確認などのメールを受け取る機会が多いため、送信者は、受信者が思わずメールを開封してしまうことを狙っています。

メールの件名や本文には「アカウントを凍結する」「不正利用されている」などと、緊急性の高い言葉を記載してあわてさせ、本物そっくりのフィッシングサイトへ誘導する巧みな手口です。

「すぐに対応しなければいけない」と指示されたフィッシングサイトで、アカウント情報などを入力してしまうと、クレジットカードの不正利用や、サイトでの不正購入などの被害にあうおそれがあります。

決してメールのリンクをタップ（クリック）したり、個人情報を入力したりしないようにしましょう。

実在の企業と無関係に送信された偽メールの例



ポイント

✓ 大手ECサイトでは顧客へ未納料金を督促するSMSを送信することはありません。また、登録のアカウント情報の開示をメールやSMSで求めることもありません。
✓ もし、アカウント情報を入力してしまった場合は、すぐにカスタマーサービスに連絡してください。購入履歴の確認、キャンセルや、パスワードの変更などの措置が必要です。

本物のメッセージかを確認するには？（Amazonの場合）

本物のお知らせかどうか迷ったときは、「メッセージセンター」を確認しましょう。

確認するときは受信したメールのリンクからではなく、「検索」や「アプリ」からログインし、「アカウントサービス」→「メッセージセンター」を開くとメールで送られたすべての内容を確認することができます。

ログイン＞アカウントサービス＞メッセージセンター＞メッセージ＞すべてのメッセージ

パソコンでの表示

アプリの表示