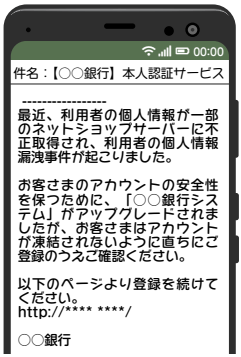
金融機関やクレジットカード会社になりすました偽メール

●あなたの預金やクレジットカード番号が狙われています



金融機関になりすまし、ネットバンキングやクレジットカード利用者へのお知らせメールを装ったフィッシング詐欺の事例もあります。

「安全性向上のためにパスワードを変更してください」「カードの利用確認」などと緊急性を強調して、本物そっくりの偽サイトへ誘導し、利用者のアカウント情報（口座番号、契約者番号、クレジットカード番号、暗証番号など）を入力させてだましとろうとする手口です。

犯罪者に、この方法でだましとったアカウント情報を使われて、正規のサイトにログインされ、銀行口座からの不正送金や不正なクレジットカード利用をされてしまうなどの被害が報告されています。

メールの特徴

・「不正に利用される懸念がある」「漏洩した名簿にあなたが含まれている」「セキュリティ強化に必要」「カードの利用確認」などと緊急を装う内容

対処法

✓金融機関やクレジットカード会社がメールで個人情報を求めることはありません。メールに記載されたリンクをタップ（クリック）したり、メールの問い合わせ先へ連絡したりするのはやめましょう。

✓偽サイトは本物そっくりに作成しているため、本物と見分けるのは困難です。本物かどうか確認する必要がある場合には、普段使用しているブックマークやアプリからアクセスするか、公式サイトから連絡するようにしましょう。

✓フィッシング詐欺の被害にあった時は、速やかにご利用の金融機関やクレジットカード会社の窓口に連絡してください。また、金銭被害にあった場合には、最寄りの警察署へ相談してください。

✓偽サイト対策には、「100%安心」といった対策を示すことは困難ですが、セキュリティ対策ソフトを最新の状態にアップデートして、「提供元不明のアプリ」のインストールを許可しないといった設定も有効です。

相談窓口

■ 警察相談ダイヤル

電話番号：＃9110（通話料有料）
受付時間：平日8：30～17：15（各都道府県警察本部で異なります）
（土日・祝日及び時間外は、一部の県警を除き、当直または音声案内での対応となります）

もっと知りたい

フィッシング対策協議会ではフィッシングに関する緊急情報やフィッシング事例の紹介を行っています。

■ フィッシング対策協議会
https://www.antiphishing.jp/