

JAバンクを装ったフィッシングメールにご注意ください！

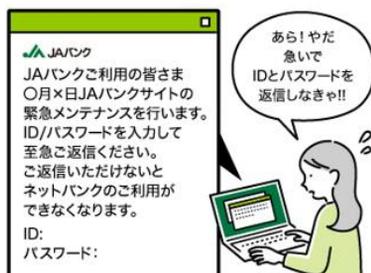


偽メールに気をつけてください

① JAバンクを装ったメールがくる



② IDとパスワードを伺うメールが届く



③ IDとパスワードを返信してしまい知らない人に情報を盗まれてしまう



④ 盗まれたIDとパスワードを悪用されてしまう



不特定多数の方へ複数回送られていることが確認されています。

操作を焦らされていませんか？

メールの件名や内容で慌てず、まずは公式サイトからログインし、あわせて身に覚えのない取引がないか確認しましょう。

<メールの件名> ※実際に確認されたもの

- ・【緊急情報】お客様情報・取引目的等のご確認
- ・【JAネットバンク】利用停止のお知らせ
- ・【JAネットバンク】緊急停止のご案内
- ・【JAネットバンク】お客さま情報等の確認について
- ・【件名なし】ご利用アカウントの確認手続きのお願い
- ※その他口座凍結や口座をブロックした等々の内容

JAネットバンク、JAバンクアプリから送付するメールのドメインは以下のみですので、不審なメールにはご注意ください。

「@webcenter.anser.or.jp」
「@otp-auth.net」 「@janetbank.jp」
「info@mailers.ja-apis.org」



偽サイトに気をつけてください

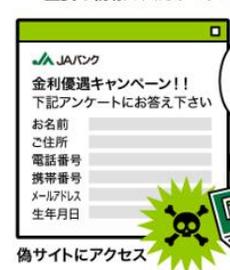
① JAバンクを装ったメールがくる



② 偽サイトにアクセスを促すメールが届く



③ 偽サイトにアクセスし重要な情報を入力してしまう



④ 知らない人に入力した情報が送られ、情報を悪用される



フィッシングメールなどに記載されているURLにはアクセスしない!

偽サイトにはID・口座番号・パスワード等は絶対に入力しないでください。

<要注意>

特にワンタイムパスワードを漏洩すると、犯人側で送金が可能となり、貯金残高の全額を不正送金されるリスクがあります。

JAネットバンクに定期的にログインし、身に覚えのない取引がないかをご確認ください

フィッシングメールの被害に遭われたと思ったら・・・JAネットバンクの緊急停止を実施してください。