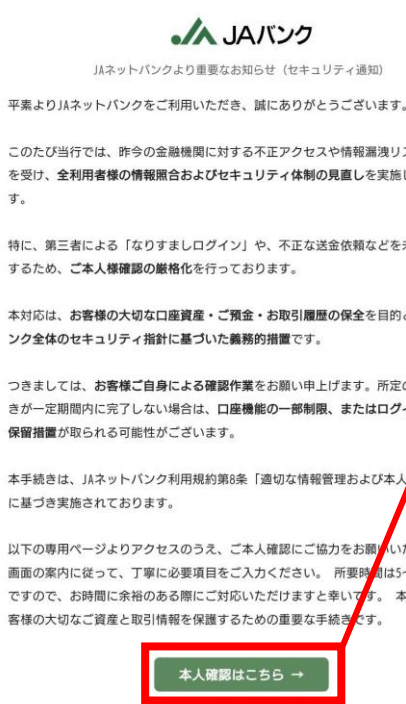


「JAバンク」や「JAネットバンク」を装った フィッシングメールによる被害が急増中！

本物とそっくりに作りこまれています！



平素よりJAネットバンクをご利用いただき、誠にありがとうございます。

このたびは、昨今の金融機関に対する不正アクセスや情報漏洩リスクの増加を受け、全利用者様の情報照会およびセキュリティ体制の見直しを実施しております。

特に、第三者による「なりすましログイン」や、不正な送金依頼などを未然に防止するため、ご本人様確認の厳格化を行っております。

本対応は、お客様の大切な口座資産・預金・お取引履歴の保全を目的とし、JAバンク全体のセキュリティ指針に基づいた義務的措置です。

つきましては、お客様ご自身による確認作業をお願い申し上げます。所定の確認手続きが一定期間内に完了しない場合は、口座機能の一部制限、またはログイン機能の保留措置が取られる可能性があります。

本手続きは、JAネットバンク利用規約第8条「適切な情報管理および本人確認義務」に基づき実施されております。

以下の専用ページよりアクセスのうえ、ご本人確認にご協力をお願いします。画面の案内に従って、丁寧に必要項目をご入力ください。所要時間は5～10分程度ですので、お時間に余裕のある際にご対応いただけますと幸いです。本確認は、お客様の大切なご資産と取引情報を保護するための重要な手続きです。

[本人確認はこちら →](#)



偽

偽

クリックすると
ログイン画面に
進み...

ログインID、口座情報、ログインパスワード等の入力情報が盗まれ、口座から

全財産

が奪われます！！

フィッシングに騙されるとどうなるの？

JAバンクを装ったメールやSMSから偽のウェブサイトに誘導し、金融情報や個人情報を不正に入手する手口、それがフィッシングです！



- アカウントを乗っ取られる
- JAネットバンクを開設される
- 銀行口座を操作されて勝手に送金される

フィッシングに対してできること



- メールやSMSに記載されたリンクをクリックしない
→ 内容の確認は、公式サイトやアプリを利用する
- 携帯電話会社等の迷惑メッセージブロック機能を活用する
- 生体認証を活用する（パスワードを利用しない。）