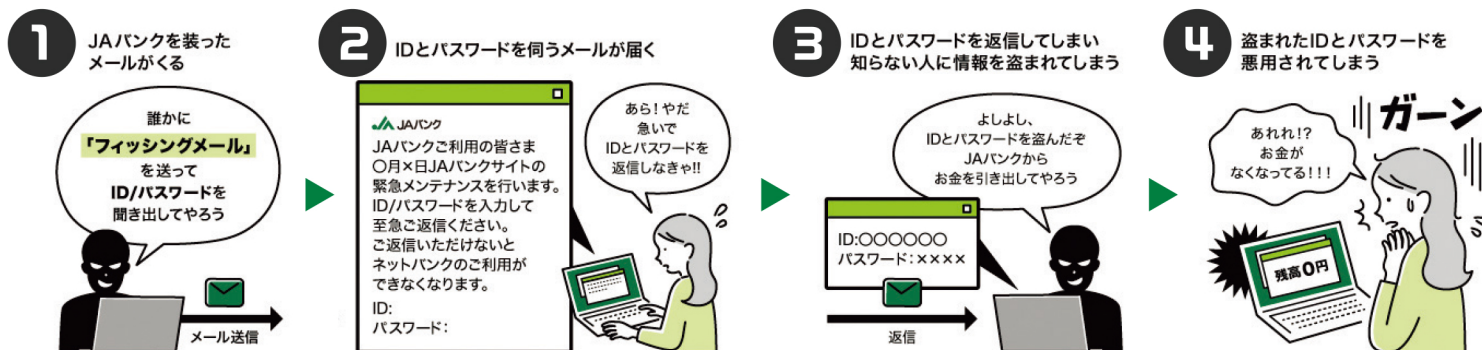


市内でも
急増中!

詐欺は身近に起こっています

フィッシング詐欺にご注意

フィッシング詐欺とは銀行等の企業を装ってメールを送り、メールの受信者に、実在する企業の偽ホームページにアクセスさせて、そのページにおいてクレジットカード番号やID・パスワード等を入力させるなどして、不正に個人情報等を入手する行為をいいます。不正に入手した個人情報を悪用し、他人になりすまして買物をしたり、インターネットバンキングからお金を引き出したりするなど、大きな問題となっています。



フィッシングメールの件名例

「セキュリティ設定未完了の方へ」
「本人確認未完了による一部機能停止」
「振込サービスのご利用に制限がかかる可能性があります」
「取引目的等の定期的なご確認にご協力ください」
「本人確認手続きのお願い」 "対応しないと制限がかかる" など不安を煽るものも

電子メールや JA ネットバンクを経由してお取引目的・お客様情報を確認することはありません！
口座番号・暗証番号などを電子メール等でお尋ねすることもしません！

▼ 実際送られてきたフィッシングメールの一例



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いたします。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 →

ご不明な点がある場合は、JAネットバンクサポートセンターまでご連絡いただくか、公式サイト内の「よくあるご質問」をご確認ください。

お客様の資産保護と健全な金融取引環境の維持にご理解とご協力をお願い申し上げます。

注意①
不審なメールアドレスからの発信
アドレス@の後ろのドメイン名に注意

注意②
ロゴを転用している場合もある
ロゴだけで判断しないこと

注意③
対応しないと口座機能に制限がかかるなど不安を煽る文章

注意④
URL から偽サイトへ誘導させる
メールに記載された URL から直接ネットバンクへログインすることは危険です

現金の振り込み指示やATMでの還付金の連絡、不審なメールの受信等がありましたら、
ご家族やご親戚、支店の窓口、警察等にご相談ください

