

サイバーだより



令和6年12月23日第34号

長野県警察本部
サイバー捜査課
026-233-0110

フィッシング被害が多発！！

フィッシングによるインターネットバンキングやクレジットカードの不正利用が後を絶ちません。

日頃からサービスへログインする際は、メールやSMS内のリンクではなく、公式アプリやブックマークなどからアクセスするように心がけてください。

フィッシングメールの例

【●●銀行】振込(出金)、ATMのご利用(出金)利用停止のお知らせ
●●銀行をご利用いただき、誠にありがとうございます。

本メールは、お客様の生体情報を登録することをご利用され、ログイン異常により、振込(出金)、ATMのご利用(出金)が一時停止されました。

提携企業サービス商品のご案内を配信登録されているお客様にお送りしています。

~~~~~略~~~~~

▼解除はこちら

【重要なお知らせ】お客様の●●カードがロックされています。-ご対応ください。  
会員様

平素より●●カードをご利用いただき、誠にありがとうございます。

この度、会員様の●●カードに関する3Dセキュア認証方式の変更を実施しましたが、システムにより不正利用の可能性が確認されたため、誠に勝手ながら会員様のアカウントおよび●●カードの利用を一時停止させていただきました。

~~~~~略~~~~~

会員様専用の再認証リンク

参考：フィッシング対策協議会(<https://www.antiphishing.jp>)

フィッシングサイトは、本物のサイトをコピーして作成しているため、**見た目で判断することは極めて困難です。**

被害に遭わないためには

○メール、SMSのURLリンクからアクセスしない。

ことが重要です。

被害に気がついたら、**金融機関やカード会社に連絡し、警察に相談してください。**



長野県警察公式ホームページの「サイバーセキュリティ対策」には、サイバー事案等の手口や被害に遭わないための情報が掲載されています。是非ご覧ください。