

フィッシング詐欺にご注意下さい！

金融機関であるかのように装った電子メールを不特定多数のお客さまに送付し、金融機関のものに似せたホームページ(偽サイト)へ誘導して利用者番号やパスワード等の重要情報を入力させ、取得するという詐欺事件が発生しております。

フィッシング詐欺とは

下記の方法で、お客さまの ID、パスワードを盗む犯罪です。

1. 金融機関を装った二セのメールを送るなど、さまざまな手口で二セのホームページへ誘導する。
2. 誘導した二セのホームページで、キャッシュカードの口座番号や暗証番号、インターネットバンキングの ID やパスワードなどを入力させる

これらの手口で入手した ID やパスワードなどを悪用して、犯人は口座から預金を引き出します。

フィッシング詐欺にあわないために

★心当たりのないメールは開かない

心当たりや取引のない金融機関のメールは開かないようにしてください。また、開いてしまった場合でも、そのようなメールの指示には従わないでください。

また、金融機関では、ID、パスワード、口座番号、暗証番号等の大切な情報に関して、電子メールでお問い合わせをすることはありません。

そのようなメールが来た場合には、直接金融機関に電話などで確認にしてください。

★『鍵アイコン』を確認する。

金融機関のインターネット・バンキングでは、ID とパスワードの入力画面に SSL 暗号化通信を使用しています。SSL 暗号化通信がおこなわれている場合は、Web のブラウザ右下に「鍵アイコン」が表示されます。取引をするにあたっては、まずこの「鍵アイコン」があることを確かめてください。

★取引のある金融機関のホームページを「お気に入り」に登録し、そこからアクセスする。

二セのメールから二セのホームページにアクセスしないように、取引のある金融機関のホームページを「お気に入り」に登録しておくことをお勧めします。ID やパスワードなどを入力する取引の場合は、「お気に入り」からアクセスすることでフィッシング詐欺にひっかかる心配がなくなります。

★誰でも利用できるパソコンで、インターネット・バンキングはおこなわない。

インターネットカフェなど、誰でも利用できるパソコンでインターネット・バンキングの取引はおこなわないでください。二セのホームページに誘導させられる可能性があります。

★通帳記入やインターネット・バンキングなどで、残高をこまめに確認する。

通帳記入やインターネット・バンキングなどをこまめにおこない、残高や不審な引き出しがないかを確認してください。

万一、身に覚えのない不審な取引をご確認された場合は

万一、当金庫のインターネットバンキングにおいて身に覚えのない不審な取引等をご確認された場合はすぐにお近くの営業店、もしくは新宮信用金庫業務部までご連絡ください。

お問合せ先

新宮信用金庫
業務部
TEL:0735-21-7924

