偽物サイトは見た目で違いはわからないから。

メールやSMSのURLリンクは危ない!!

いつものサイトはいつもの方法で入る「正規アクセス」が効く!

ブックマークやアプリなどを使った正しいログインならフィッシング被害に遭わない!

公式サイトをブックマーク

ウェブブラウザでよく見るページを登録しておいて、すぐ開けるようにする機能のことです。検索エンジンで正規サイトにアクセスしたらブックマークを心がけましょう。

公式アプリ

正規のアプリストアで配布されているアプリは開発元が明記されていて信頼できるものです。アプリをインストールする際は正規のアプリストアからインストールしましょう。

そのほか金融機関ではさまざまな対策を講じています

フィッシングサイトの検知・閉鎖活動の強化

フィッシングサイトの立ち上がりを監視し、検知したフィッシングサイトの閉鎖。

メールの送信ドメイン認証

なりすまされているメールは受け取らないと受信側に対してメールの受信拒否を要求するDMARCという技術。

メールを送信した企業のブランドアイコンが受信メールフォルダに表示されるBIMIという技術。

ウェブサイトトップだけでなく、アプリ内通知や定期メール、ログイン時に閲覧しなければ先に進めないなどの方法により、必ず注意喚起に目を通すような措置を講じています。
金融機関では送信ドメイン認証技術の導入やフィッシングサイトの速やかな閉鎖など、フィッシング対策を講じていますが、完全に防ぐことはできません。利用者も自身の身を守るために注意することが必要です。

そのために! 金融機関名のメールであっても偽物の場合があります!送信アドレスやリンクを注意して確認!ブックマークした公式サイトや公式アプリからアクセス!

ご自身でできる7つの対策

対策①　不審なリンクは開かない

不審なメールまたはSMSや添付ファイル、リンクを開かないこと。

対策②　パスワードは使いまわさない

パスワードは推測が容易な単純なものを用いず、また、同じパスワードを使いまわさないこと。

対策③　強力な認証方式を利用する

金融機関から強力な認証方式が提供されている場合は積極的に利用すること。

対策④　適切な上限を設定する

金融サービスにおける取引や振込の上限は取引の実態に合わせて適切な金額を設定する。

対策⑤　公式サイトの利用を徹底する

ソフトウェアは必ず公式サイトや正規のアプリストアからダウンロードすること。

対策⑥　不自然な画面に注意する

普段と違うログイン画面、不自然なポップアップ、追加の個人情報入力要求などが出た場合は閉じること。

対策⑦　通常と違う入力指示には警戒する

ブラウザから通常行わないキーボード操作、特にCtrl+V等のショートカット実行などを求められても実行しないこと。

大切な資産は、奪わせない。

金融庁 Financial Services Agency　警察庁 National Police Agency

一般社団法人 全国銀行協会　一般社団法人 全国信用金庫協会　一般社団法人 全国信用組合中央協会　一般社団法人 全国労働金庫協会　日本証券業協会

金融犯罪者はなりすましが得意だから

従来のパスワード対策では危険です!!

フィッシングに耐性のある「多要素認証」が効く!

昨今、証券口座への不正アクセスが発生しています。その手口は、メールやSMSなどで実在する金融機関のウェブサイトを装い、フィッシングサイトへ誘導するものです。誘導先のサイトでIDやパスワードなどを入力してしまうと、これらの情報が盗み取られ、証券口座に不正アクセスされるおそれがあります。他にも金融犯罪者があなたのスマホやパソコンなどをマルウェアに感染させ、リアルタイムでそれらの端末を監視するとともに操作し、個人情報を窃取するなどの犯罪がひろがっています。

パスワードを入力する必要がない、安全性の高い仕組みでなりすましを防ぐ!

パスキーによる認証

パスワードの代わりに生体認証(指紋認証や顔認証)、PINコードなどを使ってログインする、より安全で簡単な次世代認証方式です。パスワードを覚える手間もなくセキュリティと利便性を両立できます。

PKI(公開鍵基盤)による認証

公開鍵と秘密鍵のキーペアからなる技術で、信頼できる第三者(認証局)を通じて、本人であることを電子的に証明する仕組みです。マイナンバーカードを認証に利用することもできます。

メールやSMSに届くワンタイムパスワードを利用した多要素認証は、リアルタイムフィッシングに脆弱なほか、中間者攻撃、マルウェアによる窃取等により突破される場合があります。

リアルタイムフィッシングとは…金融犯罪者が利用者から入力された認証情報を即座に盗み取り、リアルタイムに正規サイトへ不正ログインする手口

パスキーやPKIには以下のメリットがあります。

メリット01 パスワードレスでより安全

端末に保存された秘密鍵や電子証明書を使用し認証するため、パスワードの入力が不要

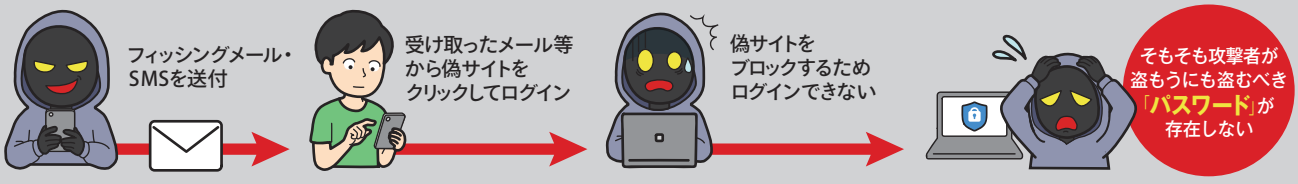
メリット02 フィッシングサイトをブロック

端末側で本物サイトか確認するため、人間に代わってフィッシングサイトをブロック

秘密鍵や電子証明書とは…いずれも数千桁のランダムな数列で複製や口伝が困難なもの

金融機関から強力な認証方式が提供されている場合は積極的に利用しましょう。

つまり! もしもフィッシングサイトに誘導されても、パスキー・PKI認証があなたを守る!



大切な資産は、奪わせない。

金融庁 Financial Services Agency
警察庁 National Police Agency

一般社団法人 全国銀行協会
一般社団法人 全国信用金庫協会
一般社団法人 全国信用組合中央協会
一般社団法人 全国労働金庫協会
日本証券業協会 Japan Securities Dealers Association