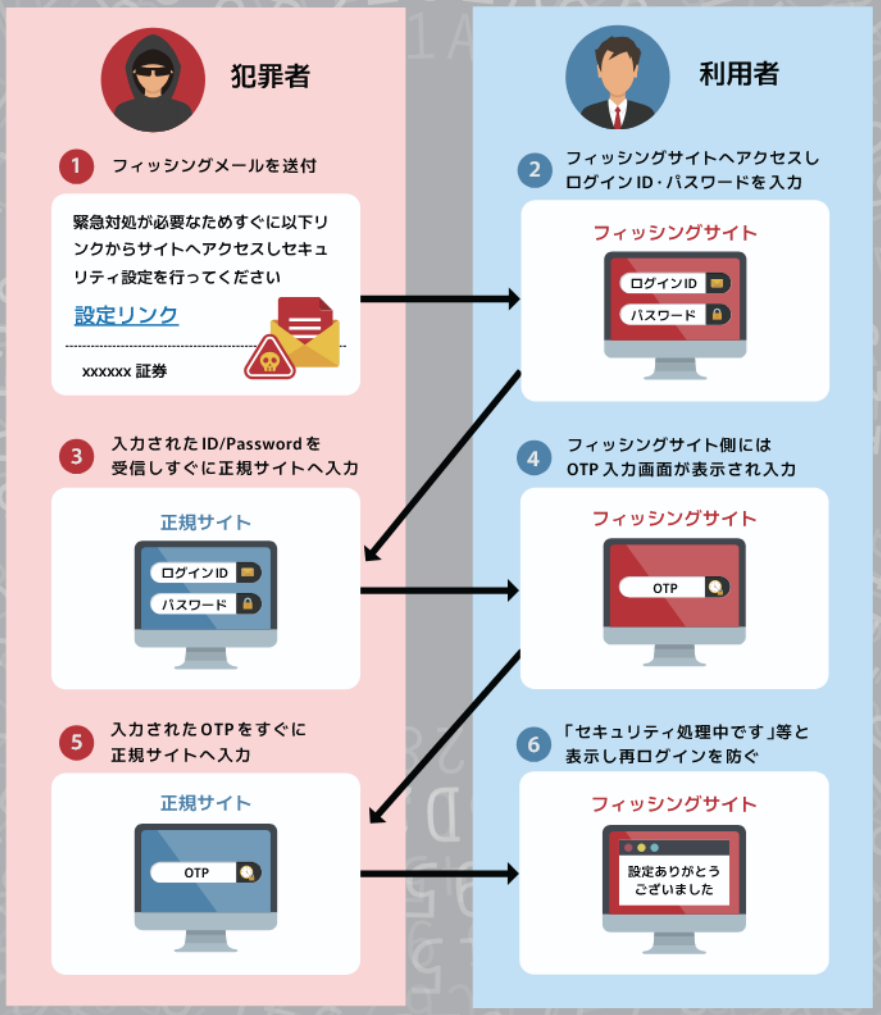
！多要素認証があっても油断厳禁

リアルタイムフィッシングに要注意

リアルタイムフィッシングとは…

近年、フィッシングサイトへの対策として普及してきた**多要素認証を突破可能なフィッシングサイト**です。
被害者がフィッシングサイトに入力した情報を犯罪者がその場で正規サイトにリアルタイムに中継し入力していきます。SMS やメール、アプリで受信する多要素認証のコードもフィッシングサイト上で入力させ、その**有効期限内に利用されることで犯罪者側が正規サイトへログイン可能となります。**

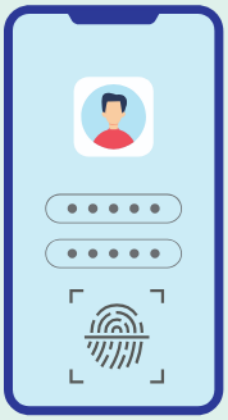


裏面を参照し対策・警戒をしてください。

特に**オンライン銀行、証券会社の利用者**は被害にあう可能性が高い手法です。

フィッシング被害防止に向けた3ポイント

1.可能ならすぐにパスキー認証を設定



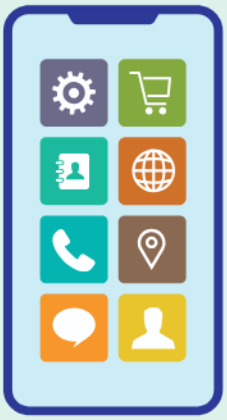
ご自身が利用する様々な Web サービスにおいて、パスキーが利用可能な場合はそれを設定しましょう。Google、Apple、Amazon、Yahoo、楽天、メルカリ、TikTok などの著名なサービスで利用が可能です。パスキーを設定していればフィッシングサイトで被害を受ける可能性が殆どなくなり、生体認証などとの組み合わせにより、ログイン操作も非常に簡単になるためぜひ設定をしてください。

2.多要素認証の設定

パスキーはすべての Web サービスで利用できるわけではありません。ご利用のサービスでパスキーによるログイン機能が提供されていない場合は、メール、SMS、アプリでコードを受け取るような従来の多要素認証でも良いのでそれを設定してください。リアルタイムフィッシングは防げませんが、それ以外の従来からあるフィッシング攻撃や ID・パスワード推測による不正アクセスを防御できます。

3.ブックマークやアプリからのアクセスを徹底

攻撃者は、様々な手口で偽サイトや偽ログイン画面にユーザーを誘導します。その中でも最も多い手口が、SMSやメールを使うことです。そのため、SMSやメールで送信されてくる URLにアクセスしなければ、フィッシング被害を受ける可能性を非常に少なくできます。



WEBサービスへのアクセス時はブラウザに URLをブックマークしておいて毎回そこからアクセスするか、公式から提供されているスマートフォンのアプリからアクセスするようにしましょう。
特に、緊急や利用停止など、焦りを誘うメールや、電話口で指示されたサイト、電話後に来た SMSには最大限警戒してください。

神奈川県警察　問い合わせ先　#9110　又は、最寄りの警察署までご相談ください　協力：株式会社マクニカ