お客さま各位

金融犯罪にご注意ください！

平素は格別のお引き立てを賜り厚く御礼申しあげます。

最近、インターネットバンキングを悪用した様々な金融犯罪が発生しています。下記の手口などを確認いただき、詐欺被害にあうことのないようご注意ください。

・電話を使った「ボイスフィッシング」

【詐欺の主な手口】

犯人は、銀行等を名乗り、電話でインターネットバンキングのパスワード等を聞き出したり、聞き出したメールアドレスにフィッシングサイト（入力した情報が抜き取られるWebサイト）のURLを送りつけたりするという手口により、インターネットバンキングから不正に送金を行うものです。

※不審な電話には応じないでください。
※不審なメールのURLは開かないでください。
※銀行員や警察官、県市町村の職員等が、お客さまのパスワード、暗証番号等をお尋ねすることはございません。絶対に他人には伝えないでください。
※不審に思われた際は、最寄りの警察までご相談ください。

詳しくはこちら

・インターネットバンキングを悪用した還付金詐欺

【詐欺の主な手口】

犯人は、金融機関、税務署・市役所など公的機関、保険会社等を騙って、「○○の還付金があります。」と電話をかけてきます。

※口座番号およびキャッシュカードの暗証番号を絶対に教えないでください。
名古屋銀行、税務署、市役所など公的機関、保険会社からキャッシュカードの暗証番号をお尋ねすることはありません。

※インターネットバンキングを契約いただいていないお客さまでも、キャッシュカードの暗証番号を教えてしまったことで被害にあいますのでご注意ください。

詳しくはこちら

・ウイルス感染を装った「サポート詐欺」

【詐欺の主な手口】

犯人は、インターネット利用時に、「偽のセキュリティ警告音が流れる」「ウイルス感染を装う偽の警告画面が表示される」ことでお客さまの不安をあおり、偽のサポート窓口に電話させ、ウイルス除去などの費用をインターネットバンキング経由で振込させてだましとろうとします。

名古屋銀行
Bank of NAGOYA

※偽のセキュリティ警告音が流れたり、警告画面が表示された場合は、ブラウザを強制終了もしくは端末を再起動してください。

※偽のセキュリティ警告画面に表示された電話番号には、絶対に電話をしないでください。また、パスワード等の入力を求められても、絶対に入力をしないでください。

詳しくはこちら

・名古屋銀行を装ったメール／SMS や SNS、偽サイト

【詐欺の主な手口】
犯人は、当行を装ったメールやＳＭＳ、あるいはフリーローンなどの偽の Web サイト広告から「当行を騙る偽サイト」に誘導し、ログインパスワードやキャッシュカードの暗証番号などのお客さま情報をだまし取ろうとします。
※名古屋銀行は、電子メールや SMS などで「ログインパスワードやキャッシュカード暗証番号の入力画面」をご案内することはありません。
※名古屋銀行は LINE の公式アカウントを使用していません。
※ローンお申込みの際、LINE で友だち登録を求めることはありません。

bankstage のログインは、普段より以下の方法でのアクセスをお勧めします。

【パソコンでの利用】
bankstage のログインページを「お気に入り（ブックマーク）」として登録し、以降は「お気に入り（ブックマーク）」からログインする

【スマートフォンでの利用】
「名古屋銀行アプリ」から利用する

詳しくはこちら

以上