

2025 年 12 月 22 日

お客さま各位

法人インターネットバンキングを狙った「ボイスフィッシング」にご注意ください

平素は格別のご高配を賜り、厚く御礼申し上げます。

最近、実在する金融機関を装った「ボイスフィッシング」と呼ばれる巧妙な詐欺が、全国で多数確認されております。

●ボイスフィッシングとは

1. 金融機関の関係者を装い、インターネットバンキング契約者に自動音声などで電話を掛ける
2. 自動音声の指示通り進めるように仕向け、電話でメールアドレスなどを聞き出す
3. 犯人は偽メールを送信しインターネットバンキング契約者を偽サイトに誘導、インターネットバンキングの ID やパスワードを入力させて盗み取る
4. 偽サイトに入力させた ID やパスワード情報等を使って、犯人が口座から不正に送金する

●被害にあわないために

- ・ 知らない電話番号からの着信は信用しない
- ・ インターネットバンキングへログインする際は、メール等のリンクではなく愛知商銀のホームページからログインする
- ・ ログインを誘導する不審なメールを受け取った場合は、メールのリンクは開かない
- ・ 金融機関から電話があれば、取引の営業店や代表電話に折り返し、本物かどうか確認する

上記の手口以外でも全国でサポート詐欺などインターネットバンキングを狙った不正送金被害が急増しています。ご注意ください。

万が一、不審なサイトにアクセスし、ID・パスワード等の情報を入力してしまった場合は、早急に弊社窓口までご相談ください。



サイバー警察局便り

Cyber Police Agency Letter 2025 Vol.12 (R7.12)

その電話、本当に銀行からですか？

電話を利用する「ボイスフィッシング」被害が再び発生

ボイスフィッシングによる法人口座を狙った不正送金被害が**再発・急増**している。

企業の法人口座を狙う、その手口とは？

1. 犯人が銀行関係者をかたり、企業に**電話**をかけ、メールアドレスを聴取する
2. **メール**を送信して偽サイトに誘導し、ネットバンクの認証情報等を入力させる
3. 犯人は認証情報等を利用し、法人口座から企業の資産を**不正送金**する

※架電イメージ



犯人

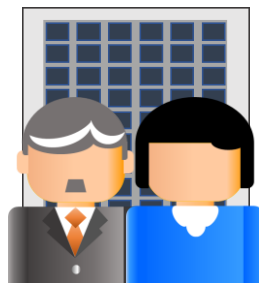
①電話（自動音声）

〇〇銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番を押してください

②自動音声に従い番号押下

③電話（犯人の声）

顧客情報の更新用リンクを送るので、メールアドレスを教えてください



被害企業
担当者

どう見分ける？こんな電話は偽物！

- 発信元番号が**国際電話**（+国番号）である（例：**+1 800 123 4567**）
- **自動音声ガイダンス**が流れたのち、人間の声に切り替わる
- 通話中に**メールアドレス**を聴取され、リンク付きメールが送られる

社内で徹底！被害を防ぐために

- 銀行から電話があれば、営業店・代表電話に折り返し、本物かどうか確認する
- インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスする



詐欺電話対策として“国際電話着信ブロック”もあります

みんなでとめよう!!国際電話詐欺



<https://www.npa.go.jp/bureau/safetylife/sos47/case/international-phone/>

もしも、被害に遭ってしまったら警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口



<https://www.npa.go.jp/bureau/cyber/boudan.html>



一般社団法人
全国銀行協会



警察庁
National Police Agency



日本サイバー犯罪対策センター