２０２６年6月５日

お客さま　各位

株式会社 富山銀行

ボイスフィッシング詐欺についての注意喚起

現在、銀行員や公的機関職員を名乗り、お客様の個人情報や金銭を騙し取ろうとする「ボイスフィッシング詐欺」の被害が全国的に報告されています。被害に遭われることがないよう、下記のような手口に十分ご注意ください。

記

【詐欺手口の例】

- 犯人が銀行担当者等を装い電話をかけ、通話の中でメールアドレスなどの情報を聞き出す。（自動音声の場合あり）
- 犯人が聞き出したメールアドレス宛にメールを送信し、フィッシングサイト（入力した情報が盗み取られる Web サイト）に誘導する。
- フィッシングサイト画面でインターネットバンキングの情報や認証情報を入力させて、情報を盗み取る。
- 犯人が盗み取った情報を使い、犯人が口座から資金を不正に送金する。

【被害にあわないために】

- **知らない電話番号や国際電話（＋で始まる電話番号）からの着信は信用しない**
- **不審な電話には対応しない**
- **メールや SMS に記載されたリンクからアクセスしない**
- **電話やメール等でインターネットバンキングの契約者番号やパスワード等の入力を求められても、絶対に入力・回答しない（銀行担当者がパスワード等の情報をお尋ねすることはありません）**

以　上

本対応に関しご不明な点等がございましたら、以下にお問い合わせください。

本件に関するお問い合わせ先
富山銀行　事務センター
（フリーダイヤル）0120-089-789
受付時間　銀行営業日　9:00～17:00

サイバー警察局便り

Cyber Police Agency Letter 2026 Vol.6 (R8.6)

巧妙化する「ボイスフィッシング」被害に注意

遠隔操作ソフトを悪用した手口が新たに発生

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手口を変えて再発

※ 架電イメージ

犯人

※発信元は国際電話番号

①電話（自動音声）

○○銀行です。ネットバンキングを利用している方は
■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）

PC環境の更新が必要です。手続きのため、
メールアドレスと携帯電話番号を教えてください。

企業担当者

I. 偽メールのリンクをクリックさせ、「セキュリティ強化のためのソフト」と称する**遠隔操作ソフトをインストール**、企業側の端末を遠隔操作

II. SMSのリンクをクリックさせて偽サイトに誘導、ネットバンキングのID・パスワードを窃取

III. Ⅰの遠隔操作している企業端末に偽の画面（「システム更新中」等）を表示その間にⅡのID・パスワードを悪用して不正送金を実行

被害を未然に防ぐために社内で徹底！

- **銀行をかたるメールやSMSに記載のリンク等へのアクセスは禁止**
- **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**

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/soudan.html

一般社団法人 全国銀行協会　金融庁 Financial Services Agency　警察庁 National Police Agency　JC3 日本サイバー犯罪対策センター