

# 今、大切な資産が狙われています！！

## 電話に注意！「ボイスフィッシング」による不正送金被害が急増

ボイスフィッシング（ビッシング）とは、音声（Voice）とフィッシング（Phishing）とを合わせた造語で、音声通話を利用して個人情報や金融情報などを窃取しようとする詐欺の手口です。**企業・個人問わず、詐欺の電話が確認されています**ので、注意しましょう。

### ▶ 手口の概要

1. 犯人が銀行担当者を騙り、被害者に電話をかけ、メールアドレスを聞き出す。
2. 犯人がフィッシングメールを送信し、電話で指示しながら、被害者をフィッシングサイトに誘導。そして、インターネットバンキングのアカウント情報等を入力させて、盗み取る。
3. フィッシングサイトに入力させたアカウント情報等を使って、犯人が被害者の口座から資産を不正に送金する。

※犯行イメージ

①



犯人



〇〇銀行です。  
ネットバンクの電子証明書の  
更新手続きが必要です。  
更新用のリンクを送りますので  
メールアドレスを教えてください。

電話



被害者

③



犯人

不正に入手した  
情報を基に  
不正送金を実行

②

フィッシングサイトに  
アカウント情報などを入力

応答



被害者

## ボイスフィッシング被害に遭わないために！3つの対策

- 知らない電話番号からの着信は信用しない！
- 銀行の代表電話番号・問い合わせ窓口で確認する！！  
銀行担当者を騙る者から連絡があった場合には、銀行の代表電話番号へ連絡して確認するなど、慎重に対応しましょう。
- メールに記載されているリンクからアクセスしない！！  
インターネットバンキングにログインする場合は、銀行公式サイトや公式アプリからアクセスしましょう。

もしも、被害に遭ってしまったら警察に通報・相談を！

サイバー事犯に関する通報等の窓口



<https://www.police-qa.jp/cyber/qa.html>



埼玉県警察 サイバーセキュリティレポート

R7. 3

サイバー局サイバー対策課