

企業・個人の資産（銀行口座）がねらわれている！！

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

【手口の概要】

1. 犯人が銀行担当者を騙り、被害者（企業や個人）に電話をかけ（自動音声の場合あり）、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、犯人が銀行口座から資産を不正に送金する。

※架電イメージ



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(企業や個人)

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真偽を確認するなど、慎重に対応してください。

◆ 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てください。

もしも、被害に遭ってしまったら警察に通報・相談を！



北海道警察公式HP
サイバ-セキュリティひろば

北海道警察
サイバ-
セキュリティ
対策本部



YouTube動画
サイバ-セキュリティ講座

