福岡県警察からのお願い

金融機関を装った電話に注意！

手口の流れを確認しよう！

#ボイスフィッシング
#ビッシング

1 犯人が銀行担当者を名乗り、被害者（企業）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。

○○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。

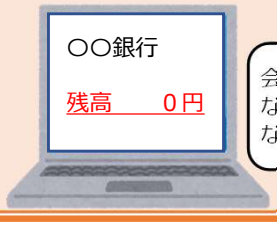
電話

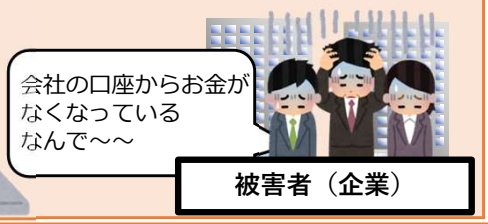
2 犯人がフィッシングメールを送信し、電話で指示をしながら、被害者をフィッシングサイトに誘導。インターネットバンキングのアカウント情報等を入力させて、盗み取る。

○○銀行です。
メールを送りましたのでリンクを開いて、アカウント情報を入力してください。

メール

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、犯人が法人口座から資産を不正に送金する。





被害に遭わないための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！

銀行担当者を名乗る者から連絡があった場合は、銀行の代表電話番号に連絡して確認するなど慎重に対応しましょう。

★メール記載のリンクにアクセスしない！

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。

福岡県警察本部サイバー犯罪対策課公式ホームページは下記QRコードから！

福岡県警察サイバー犯罪対策課