十六銀行
16FG

２０２５年６月１６日

お知らせ

法人口座を狙ったボイスフィッシングによる不正送金にご注意ください

法人口座を狙い、電話やメールを組み合わせた巧妙な手口による不正送金が増えています。手口として、金融機関や銀行の担当者を騙る犯人がフィッシングサイトへ電話で誘導し、法人口座のログインパスワードなどの情報を入力させ、不正に送金する「ボイスフィッシング」の被害が急増しています。

お客さまのログインパスワード・ワンタイムパスワード等の入力を求めるメールは**詐欺メール**です。第三者からの指示で、お客さまのログインパスワード・ワンタイムパスワードを入力することは決して行わないようお願いいたします。

●確認されている手口

①犯人が銀行担当者を騙り、被害者（企業さま）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犯人はフィッシングサイトのＵＲＬや２次元コードを記載したメールを送信し、電話で指示しながら被害者を正当なサイトを模倣した偽サイト（フィッシングサイト）に誘導。
③当該偽サイトで、インターネットバンキングの情報等を入力させて本情報を盗み取る。
④偽サイトに入力させた情報を使い、犯人が被害者の口座から不正送金を行う。

●被害に遭わないために

・見覚えの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、担当部署や氏名等を聞き取りしたうえで、折り返し連絡するなど慎重に対応してください。
・不審なメールが届いたら、メールに記載されているＵＲＬや２次元コードにはアクセスしないようにしてください。

万一、被害に遭われた場合は、最寄りの警察署またはサイバー犯罪相談窓口へ通報・ご相談ください。

サイバー事案に関する相談窓口はこちら

以　上