サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

今、企業の資産（法人口座）がねらわれている！

○○銀行です。
ネットバンクの電子証明書の更新手続きの案内で電話しました。
更新専用サイトのリンクをメールで送らせて頂きたいので、メールアドレスを教えてください。

犯人は、このように電話でメールアドレスを聞き出し、アポを取ってフィッシングメールを企業に送信し、フィッシングサイトに誘導します。
目的は、**インターネットバンキングのアカウント情報を盗むこと**です。
更に盗んだ情報を悪用して**預金を不正に送金する被害**が発生しています。

ボイスフィッシング被害に遭わないために！３つの対策

① 緊急の要件であっても落ち着いて対応する

緊急の要件で、ログインの要求の他、入金や個人情報を聞き出す等の連絡があっても慌てず、落ち着いて対応してください。

② 金融機関の代表電話番号・問い合わせ窓口で確認する

相手が金融機関の担当者と名乗っても、すぐに信用しないでください。

至急の要件であるからこそ、担当者の部署と氏名を確認し、金融機関の代表電話番号へ連絡し、確認してください。

③ メールに記載されているリンクからアクセスしない

メール本文にURLやリンクがあったとしても、アクセスしないようにしてください。

特にログインを行う場合は、必ず金融機関の公式サイトや公式アプリからアクセスするようにしてください。

もしも、被害に遭ってしまったら警察に通報・相談を！

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

その他サイバー犯罪対策に関する事は
大阪府警察ウェブサイトをご確認ください