サイバーニュース

2026年6月
第12号

巧妙化する「ボイスフィッシング」被害に注意
遠隔操作ソフトを悪用した手口が新たに発生

ボイスフィッシングとは、電話で金融・公的機関等を装い、ネットバンキング等のＩＤ・パスワードを聞き出して、不正利用する手口です。

※ 犯行イメージ

（発信元は国際電話番号）

① 電話（自動音声）
○○銀行です。ネットバンキングを利用している方は■番を押してください

② 自動音声に従い番号押下

③ 電話（犯人の声）

③　「PC環境の更新が必要です。手続きのため、**メールアドレスと携帯電話番号**を教えてください。」等と誘導

④　偽メールのリンクをクリックさせ、「セキュリティ強化のためのソフト」と称する**遠隔操作ソフトをインストール**させ、企業側の端末を**遠隔操作可能な状態**に

⑤　SMSのリンクをクリックさせて**偽サイト**に誘導、**ネットバンキングのID・パスワードを窃取**

⑥　④の遠隔操作している企業端末に**偽の画面（「システム更新中」等）を表示**その間に⑤のID・パスワードを悪用して**犯人側が管理する口座に送金を実行**

被害を未然に防ぐために社内で徹底！

- 銀行をかたるメールやSMSに記載のリンク等へのアクセスは禁止
- 銀行から電話があれば、営業店・代表電話に折り返し、本物か確認

詐欺電話対策として“国際電話着信ブロック”もあります

みんなでとめよう!!国際電話詐欺 → https://www.npa.go.jp/bureau/safetylife/sos47/case/international-phone/

被害に遭ってしまったら警察に通報・相談を！

一般社団法人 全国銀行協会　金融庁 Financial Services Agency　警察庁 National Police Agency　JC3 日本サイバー犯罪対策センター