



巧妙化するボイスフィッシング詐欺 被害に注意!

犯人が銀行関係者をかたって企業に架電し、メールアドレスや電話番号等を聞き出してフィッシングサイトに誘導する

ボイスフィッシング (ビッシング)

による法人口座を狙った不正送金被害が再発しています。



〇〇銀行です。
更新手続きのため
連絡先を教えてください。

ボイスフィッシング(ビッシング)とは・・・

金融機関の担当者等をかたって電話をかけて個人情報聞き出し、偽サイトに誘導するフィッシングメールを送り付ける手口です。

新たな手口としては、ID・パスワードを窃取するだけでなく、**犯人が企業の端末を操作できるソフトをインストールさせる**ケースがあります。

ボイスフィッシングは
音声(Voice)
と
フィッシング(Phishing)
を掛け合わせた造語
です



ボイスフィッシングの新たな手口

1 電話 (自動音声) がかかってくる

【自動音声例】
〇〇銀行です
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



銀行員等をかたって接触がある
自動音声に従って番号を押すと肉声に変わる

発信元が国際電話番号である
ケースが多く見られます

2 連絡先を聞かれる

PC環境の更新が必要。
手続きのため
メールアドレスと
電話番号を
教えてください。



銀行担当者等をかたる相手が
「更新手続きのため」等と
言ってメールアドレスや電話
番号等を確認される

上司や取引先、官公庁や
弁護士を名乗る電話にも注意!!

3 犯人側から「罠」が届く



遠隔操作

ID・パスワード
窃取

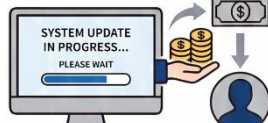
罠 メール

届いたメールのリンクをクリック
すると、「セキュリティソフト」を
装った「遠隔操作ソフト」の
インストールを指示される

罠 SMS

届いたSMSのリンクをクリック
すると偽サイトに誘導されて、
IDやパスワードが盗まれる

4 不正アクセス被害・不正送金被害に遭う



遠隔操作している企業端末に
二重の画面(「システム更新
中」等)が表示される
二重の画面が出ている間に、
犯人がID・パスワードを悪
用、遠隔操作等で預金を送金
される

国際電話番号に警戒!
警察庁推奨アプリ等で
国際電話ブロック!

下記詐欺電話対策を
チェック!

個人情報を伝える前に
営業店・代表電話に
折り返して確認!

心当たりのないソフトの
インストールは厳禁!
ログインが必要な場合は
公式サイトや公式アプリ
からアクセス!

被害に気づいたら
速やかに銀行や警察へ
連絡・通報を!

詐欺電話対策

固定電話にかかる国際電話を休止できます!

国際電話不取扱受付センター

☎ 0120-210-364

オペレーター案内(平日:9:00~17:00/通話料無料)
自動音声案内(平日・土日祝24時間/通話料無料)

WEBで申込みも可能!
詳細は二次元コードから



携帯電話の場合も
警察庁推奨アプリをご活用ください!



詐欺対策
by NTTタウンページ



詐欺バスター Lite
by TREND



詳しくはこちら!

