



企業の皆様！

ボイスフィッシング対策を

ボイスフィッシングとは、銀行員などを装った犯人が電話(ボイス)で接触し、フィッシングサイトに誘導して、法人口座の認証情報を盗み取る手口です。



自動音声

「セキュリティ更新が必要です。
経理担当者の方は
1を押してください」



有人オペレーター

「手続きに必要なリンク
を送ります。
ご担当者様の
メールアドレスをお伺い
します」



メール

メールのリンク先は、
銀行のログイン画面を
模した偽サイトです。
ID・パスワード・ワン
タイムパスワードなどが
盗まれます。



「遠隔操作ソフト」をダウンロードさせて、企業側の端末を操作し不正送金を実行することもあります

対策はこちら

1 ルール作り

- ・ 電話は一旦切って、営業店や代表電話に折り返す ※【社長からの極秘・至急の指示】など役職者からの指示であっても例外なく行う
- ・ 振込データの「作成者」と「承認者」を分けるなど一人で完結できない体制を作る

2 システム導入

- ・ 特定のパソコンからしかログインできない制限をかけたり、多要素認証を導入する
- ・ ドメイン偽装を防ぐメール設定(DMARC等)を導入する

3 教育・研修

- ・ 社内教養で最新手口を周知する

サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX (旧Twitter) で、サイバー犯罪やサイバーセキュリティの情報をいち早くお届けしています。

https://x.com/HPP_c3division

