かごしまサイバー通信

Vol.11
令和８年６月９日
鹿児島県警察本部
サイバー犯罪対策課
Tel　099－206－0110

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による法人口座を狙った不正送金被害が手口を変えて再発しています。

※ 架電イメージ

犯人

※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）

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。

企業担当者

I. 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する。

II. SMSのリンクをクリックさせて偽サイトに誘導し、ネットバンキングのID・パスワードを窃取する。

III. Ⅰ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）を表示させ、その間にⅡのID・パスワードを悪用して不正送金を実行する。

といった手口が確認されています。

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、本物かどうか確認**

といった対策を講じてください。

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/

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

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　K.P. KAGOSHIMA POLICE