道内の金融機関をかたる不審電話を多数確認

インターネットバンキングを利用している企業は、電話による「ボイスフィッシング」にご注意を！

- 11月ころから**道内の複数の金融機関**をかたる不審な電話（自動音声が多い）を多数確認。
- 全国的に被害が拡大しており、他の地域では１対象あたり**数千万～数億円規模**の被害も確認。

企業の資産を狙う手口「ボイスフィッシング」とは？

1. 犯人が金融機関の関係者をかたり、企業に電話をかけ、自動音声ガイダンスを流す。
2. 音声に従い番号を押すと、犯人に切り替わる（始めから犯人が電話することも）。
3. 担当者のメールアドレスを聞き出し、フィッシングメールを送信する。
4. メールに記載のリンクからフィッシングサイトに誘導し、インターネットバンキングのアカウント情報を入力させる。
5. 犯人がアカウント情報等を利用し、法人口座から資産を不正送金する。

※犯行の流れ（例）

犯人

①電話（自動音声）

○○銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番を押してください。

②自動音声に従い番号を押す

③電話（犯人の声）

顧客情報の更新用リンクを送るので、メールアドレスを教えてください。

被害企業担当者

どう見分ける？こんな電話は偽物の可能性大！

- 発信元番号が国際電話(+ 国番号)、または非通知となっている。
- 自動音声ガイダンスが流れたのち、人間の声に切り替わる。
- 通話中にメールアドレスを聞かれ、リンク付きのメールが送られる。

社内で徹底！被害を防ぐために

◆ **金融機関から電話があれば、本物かどうか確認する！**
上記に該当する特徴があったら、一旦切って、金融機関の問合せ先に確認してください。

◆ **メールに記載されているリンクからアクセスしない！！**
インターネットバンキング利用時は、公式サイト・アプリからアクセスしてください。

もしも、被害に遭ってしまったら、金融機関のコールセンターに連絡の上、警察に通報・相談を！

北海道警察公式HP
ｻｲﾊﾞｰｾｷｭﾘﾃｨひろば

北海道警察

YouTube動画
ｻｲﾊﾞｰｾｷｭﾘﾃｨ講座