

法人インターネットバンキングを狙った詐欺にご注意ください

全国で法人インターネットバンキングを狙った被害が急増しております。

【手口の概要】

1. 犯人が銀行を騙り自動音声や担当者を名乗り、被害者（企業）に電話をかけ、法人インターネットバンキングの利用に関し、「電子証明書の更新が必要」、「更新手続きが完了していない」などと言葉巧みにメールアドレスを聞き出す。
2. 犯人が被害者（企業）にフィッシングメールを送付し、被害者をフィッシングサイトに誘導。（電話による指示がある場合もある）
そして、インターネットバンキングのアカウント情報等を入力させて、盗み取り、フィッシングサイトに入力させたアカウント情報等を使って、犯人が法人口座から資産を不正に送金する。
3. パソコンでサイトを閲覧しクリックしたところ、警告音がなり、右下にマイクロソフト社等のシステム会社の電話番号が表示され、電話したところ片言の外国人が受電しパソコンをリモートで操作される。

【注意喚起】

- ・銀行や第三者（マイクロソフト社等のシステム会社）から法人顧客に対して、電話やメールで、①法人インターネットバンキングのIDやパスワードを確認すること、②電子証明書の更新等を依頼することは一切ありません。
- ・不審な電話やメールがあった場合には、ご回答やお手続き等は絶対に行わず、直ちに銀行にお問い合わせください。
- ・万が一、不審なサイトにアクセスし、ID・パスワードや法人・個人情報を入力してしまった場合には、銀行及び最寄りの警察署にご連絡をお願いします。

法人インターネットバンキングへログインする際は、メール等のリンクではなく、銀行ホームページやブラウザのブックマークなどからアクセスするよう心がけていただくとともに、インターネットバンキングへのログインを誘導する不審なメールを受け取った場合は、メール本文中のURLから絶対にアクセスを行わないようにご注意ください。

また、ID・パスワード・暗証番号等の管理には十分にご留意ください。

本件に関するお問合せ先
佐賀銀行
E B サポートセンター
0120-74-2525