令和６年11月22日

関　係　各　位

警視庁サイバーセキュリティ対策本部

インターネットバンキング不正送金事犯の連続発生について（注意喚起）

最近、銀行を騙った犯人が、法人に対して電話をかけたり、メール等を送信して、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で不正送金する事案が連続発生しています。つきましては、下記のとおり、注意喚起させていただきます。

記

１　発生事例

(1)銀行を騙った、フィッシングサイトのQRコードが記載されたFAXやフィンシングサイトのURLが書かれたメールが届く事例

・　発生状況（FAXの場合）

①　銀行を騙り、「口座制限告知書」等と題したQRコード付きのFAXが会社に届く。

②　FAXには「(口座の）利用を一時制限させていただきました。スマートフォンでQRコードを読み取って、利用制限を解除してください」と書かれている。

③　QRコードを読み取ると、インターネットバンキングのIDやパスワードを入力する画面（フィッシングサイト）が表示される。

・　実害例

①　会社に、Ａ銀行を騙った上記FAXが届く。

②　QRコードを読み取ったが、サイトにアクセスできなかった（原因不明)。

③　同じ頃、Ａ銀行を騙った上記FAX内容と同様のメール（フィッシングメール）が届いていた。

④　そのメールに書かれたリンクをクリックすると、IDやパスワードを入力するログイン画面（フィッシングサイト）が表示された。

⑤　ID・パスワード等を入力すると、会社にＡ銀行を騙る者（流暢な日本語）から電話がかかってきた（直後であるか、時間を置いてであるかは不明)。

⑥　その者から「乱数表の内容を教えてもらいたい」と言われたので、内容を教えた。

⑦　その後、会社担当者がインターネットバンキングの残高を確認すると、資金が身に覚えのない銀行口座へ不正送金されていることが判明した。

(2)　会社宛てに、銀行を騙った者から電話があった後、フィッシングメールが送られてくる事例

・　実害例

①　会社にＢ銀行を騙った者から電話がかかってきた。

②　その者から「インターネットバンキングの電子証明の期限が切れているので更新してもらいたい。これからメールで URL を送信するので、メールアドレスを教えてほしい。」と言われたので、メールアドレスを教えた。

③　その後、会社宛てにリンクが書かれたメール（フィッシングメール）が届く（相手との通話は継続している状態）。

④　そのメールに書かれたリンクをクリックすると、ID やパスワードを入力する画面（フィッシングサイト）が表示された。

⑤　相手の指示に従い、契約者番号・ID・パスワードを入力すると、次に取引実行パスワードやワンタイムパスワードを入力する画面が表示された。

⑥　さらに相手の指示に従い、ワンタイムパスワードを入力すると、相手から「手続きは終了した。」と言われ、通話を終えた。

⑦　その後、会社担当者がインターネットバンキングの残高を確認すると、資金が身に覚えのない銀行口座へ不正送金されていることが判明した。

２　上記実害例を受けて皆様にご注意していただきたい事項

(1)　FAX やメールに記載されている、QR コードを読み取ったり、リンクをクリックしたりして、フィッシングサイトにアクセスしないでください。

(2)　銀行担当者を名乗る者から電話があった際は、担当者の部署・氏名等を聞いた上、銀行の代表番号から担当者に折り返し連絡するなど、慎重に対応してください。

(3)　被害が発生してしまった場合は、所在地の管轄の警察署にご相談ください。

以上