

令和6年11月21日

不動産会社担当者 各位

警視庁生活安全部
サイバー犯罪対策課

不動産業を狙ったと思われるインターネットバンキング不正送金事犯について
(注意喚起)

当方は警視庁サイバー犯罪対策課となります。最近不動産業の法人口座にある資金を狙ったと思われるインターネットバンキング不正送金事犯の被害が数件立て続けに発生しているため、取り急ぎ、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（いずれもフィッシング（※）による被害）

※（フィッシング対策協議会サイトより引用）

フィッシング（Phishing）とは実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取することです。電子メールのリンクから偽サイト（フィッシングサイト）に誘導し、そこで個人情報を入力させる手口が一般的に使われています。

(1) 不動産会社宛てに、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 やフィッシングサイトの 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 が不動産会社に届く。
- 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 不動産会社に、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、不動産会社に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ください」と言われたので、内容を教えた。
- ⑦ その後、不動産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) 不動産会社宛てに、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 不動産会社に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ください。」と言われたので、メールアドレスを教えた。
- ③ その後、不動産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、不動産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、不動産会社所在地管轄の警察署にご相談ください。

以上