

スマートフォンの乗っ取りを目的とした偽アプリによる不正送金にご注意ください

最近、スマートフォンの遠隔操作により、お客さまの口座から不正送金された可能性のある事案が、全国で発生しております。

報道された事例では、以下の流れで被害に遭っています。お客さまご自身で、十分な注意をしてください。

不正利用の流れ

1. SNS 広告やメールから誘導される

- ・SNS 広告やメールなどからの URL により、ダウンロードサイトに誘導されます。
- ・リンク先には、アプリストアのような偽のページが用意され、アプリをインストールするよう誘導されます。
- ・本人は特に意識していなくても、ダウンロードサイトへ誘導されるケースもあります。

2. 偽アプリを入れてしまう

- ・有名な SNS を装い、見慣れたサービス名・アイコンを表示させて、本物だと思わせるようなものであるため、特に不振と思わずダウンロードしてしまいます。
- ・ダウンロード後、様々な設定変更を求める画面が表示されますが、すべてを許可してしまいます。

3. 乗っ取られたスマホから不正に操作されてしまう

- ・偽アプリをダウンロードすると、遠隔操作が可能となるような設定となってしまいます。

どうやって防ぐか

1. アプリのダウンロードは、正規のストアから探す

- ・広告やメールのリンク先から、そのままインストールすることはやめてください。

2. 警告メッセージが表示されたら、操作を止める

- ・最新のスマートフォンであれば、不審なアプリの操作は警告メッセージを表示してくれる場合があります。

・上記メッセージが表示されたら、いったん立ち止まり、本当に必要なアプリであれば、正規のストアからインストールし直してください。

・「この設定を解除してください」「警告が出ても続けてください」のようなメッセージは危険です。

3. 許可を求めるようなメッセージが表示された場合は特に注意する

・インストール作業を続けると、特に下記のメッセージが表示されることがあります。これは、遠隔操作を可能とするよう許可を求めるものであり、許可をすると不正利用される可能性があります。

✓「ユーザー補助を有効にする」

✓「接続リクエスト」

通常時の対策

1. 不審なメール・サイトを開かない

- ・差出人や内容に心当たりのないメール・SMS のリンクや添付ファイルは開かない
- ・正規のアプリストア以外からアプリをインストールしない

2. OS やアプリを最新に保つ

- ・スマートフォンの OS を最新の状態にアップデートする
- ・しまぎんアプリを含む各アプリは、公式ストアから最新バージョンに更新する

3. ウイルス対策ソフトを利用する

- ・信頼できるセキュリティソフトをインストールし、定期的にウイルスチェックを行う

■ ウイルス感染・不正利用された際に見受けられる主な兆候

次のような場合は、スマートフォンのウイルス感染や不正送金の疑いがあります。

- ・身に覚えのないメールや SMS、通知が急に増えた
- ・インストールした記憶のないアプリが表示されている
- ・端末の動作が急に重くなる
- ・劣化ではないのにバッテリーの減りが異常に早い
- ・しまぎんアプリやほかの決済アプリの明細に、身に覚えのない送金・支払いがある

■ 不審に感じたときは

少しでも「おかしい」と感じたら、次の対応をお願いします。

- ・しまぎんアプリでの操作をいったん中止し、スマートフォンの電源を切るか、機内モードに設定するなどして、通信を遮断してください（機内モードに設定した場合は、Wi-Fi がオフになっていることをご確認ください）
- ・他の端末や電話から、窓口・コールセンターへ連絡し、状況をご相談ください
- ・身に覚えのない送金・請求がある場合は、警察へもご相談ください

お客さまの大切なご資産をお守りするため、日頃の対策と、異常に気付いたときの早めのご相談をお願いいたします。

以上