2026年10月20日

お客さま 各位

湖東信用金庫

悪質なウェブサイトや偽アプリにご注意ください！

①　検索サイトで表示される悪質なウェブサイトについて

Google等の検索サイトにおいて、「湖東信用金庫　インターネットバンキング」等で検索した場合、正規の当金庫ウェブサイトのほか、サポート詐欺などの可能性がある不審なリンクが表示される悪質なウェブサイトが確認されております。

検索結果に表示されるURLが不審なものである場合には、絶対にアクセスしないようご注意ください。

当金庫のインターネットバンキングをご利用の際は、当金庫ウェブサイト（以下のURL）のトップページに掲載しているリンクからご利用くださいますようお願い申し上げます。

当金庫のウェブサイト　https://www.shinkin.co.jp/kotoshin/

②　偽アプリによるフィッシング詐欺について

国税庁や楽天等になりすましてメールを送り、偽のアプリをインストールさせた上で、金融機関のアプリを模したログイン画面を表示することにより、正規アプリやインターネットバンキングのID・パスワード等を窃取するフィッシング詐欺や遠隔操作による不正送金などが発生しております。

「しんきんバンキングアプリ」など金融機関のアプリをインストールする際は、公式ストア（Google Play、App Store）よりインストールをしていただきますようお願い申し上げます。

以上

滋賀県警察
サイバーセキュリティ滋賀
サイバー犯罪からあなたを守るセキュリティ情報をお届けします。
R８年度 No.29

偽ポイントアプリに注意！（Androidスマホ）

１．案内メールが届く



２．アプリストアが開く



３．インストール中に何度も確認が求められる



一般的な公式アプリのインストールでこのような確認画面が出てくることはありません！

偽アプリをインストールしてしまう…と<u>スマホが乗っ取られ</u>、
・遠隔操作で決済アプリを勝手に使われる
・個人情報が外部に送信される　　などの被害につながります。

Point

・アプリは公式のアプリストアからインストールする
（メールやSMSで届いたリンクからストアを開かない）
・偽アプリをインストールしてしまった場合は、ネット接続を切り、アプリを削除、アカウントのパスワード変更をしてください。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）

滋賀県警察

サイバーセキュリティ滋賀

サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

R８年度 No.32

不正アプリによる不正送金被害が発生

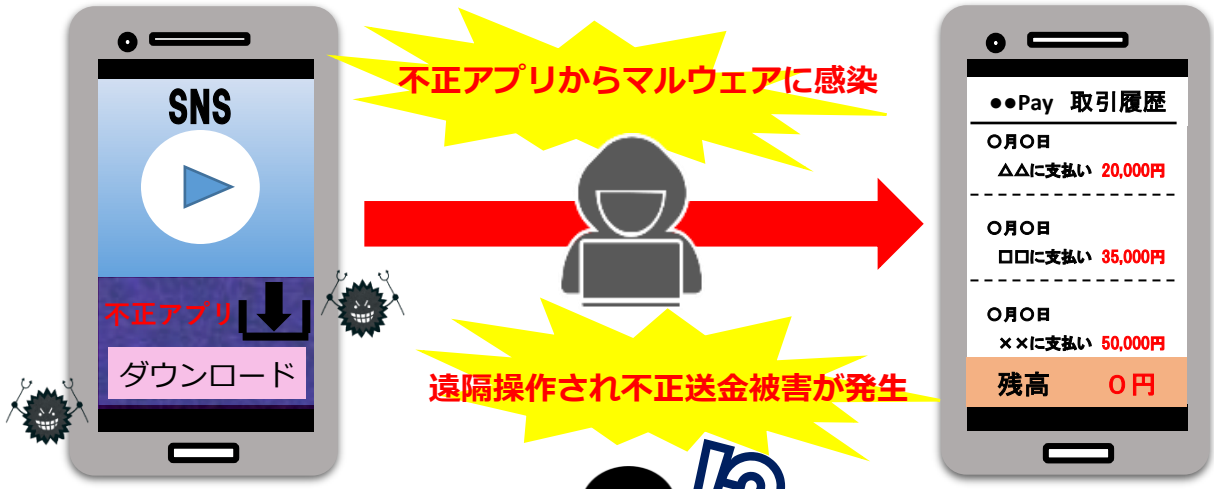


不正アプリをインストールしたことでキャッシュレス決済サービスが遠隔操作され、**不正送金される被害**が発生しています！

Case１_**SNSに掲載された広告**から
Case２_**メールやSMSのリンク**から
Case３_**SNSで知り合った相手**から

不正アプリをインストール

※有名なSNSやアプリを装っています！





アプリをインストールしたらスマホが操作できなくなった！

勝手にチャージされて送金された！
身に覚えのない送金がある！

被害にあわないために

- ☑ SNS広告やメールリンクから誘導されたアプリを、安易にインストールしない
- ☑ 公式アプリストアでも、提供元や内容をよく確認する
- ☑ 不正アプリは、直ちに削除する
- ☑ スマホにもウイルス対策ソフトを導入し、ＯＳを最新の状態にする

☑ **警察に通報・相談する**

▶ 最寄りの警察署又はサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）