

金融機関などを  
装った

# 偽SMSの



## リンクを開かないでください!

※SMS(ショートメッセージ サービス):携帯電話番号を用いて、短いメッセージを送受信する機能



**ID・パスワード、個人情報**は入力  
しないでください。



リンクを開いてしてしまうと、

**フィッシングサイトに**

**誘導されて**



ID・パスワードなどの  
情報が盗み取られ、

**不正送金の  
被害に...**



## 対策

① **リンクを不用意に開かない**



② リンクを開いてしまっても**ID・パスワード**  
などを**絶対に入力しない**



③ サイトへのログインは、**公式アプリ**や  
**公式サイト**からアクセスする



④ **迷惑SMSブロック機能**や  
**セキュリティ対策ソフト**を利用する



# スマホを安全に 使うには？

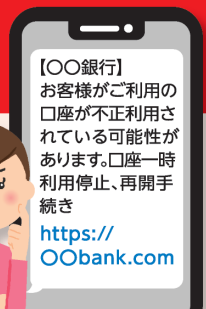


## スマホを使用する際には 以下に気をつけましょう



### メールやSMS内のリンクを 不用意に開かない

大手企業などをかたる偽メッセージから、フィッシング詐欺の被害にあわないよう、ブックマークに登録した正規サイトや公式アプリからアクセスしましょう。



### ご自身のアカウントを厳重に管理する

パスワードは、使いまわしせず、名前や誕生日など推測されやすいものは使わないようにしましょう。

※ワンタイムパスワードや指紋認証なども活用しましょう。



### セキュリティ対策ソフトを活用する

巧妙な詐欺サイトや不正なリンクの判別を行うセキュリティ対策ソフトを活用しましょう。

