

## 今、起きていることから学ぶ 将来必要なサイバー犯罪被害防止のための知識

### インターネットバンキングの不正送金被害

令和5年上半期の被害額 約30億円

※ネット銀行のID・パスワードが盗まれ、預金が他人の口座に送金されてしまうこと。

警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）より

あなたは、これを見て  
こう考えていませんか？



まだ銀行口座を持っていないし、  
今の自分には関係ないことだなあ。

関係あります

被害防止対策は  
今から使える知識

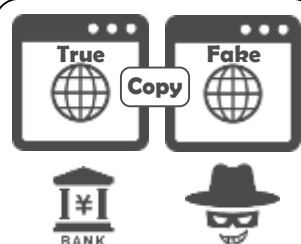


被害の多くは、フィッシングによるものとみられます。  
皆さんが利用するSNSやゲームなどのサービスで被害を受けることも。  
今から対策をしておくことで、将来のサイバー犯罪被害防止につながります。

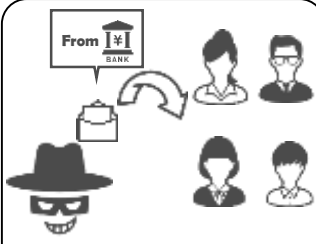
## フィッシングの手口と被害防止について学びましょう

### フィッシングとは

実在する企業のふりをして、IDやパスワードなどの個人情報を盗むこと。



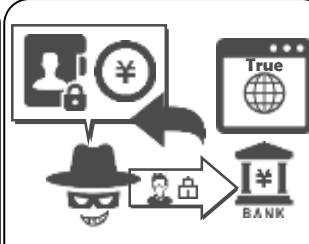
① 犯人は、あらかじめ  
実在する企業の公式  
サイトとそっくりな  
偽サイトを作る。



② 偽サイトにつながる  
リンク（URL）を  
記載したメールを  
様々な人にばらまく。



③ メールにだまされた  
人が、IDやパス  
ワードなどの情報を  
偽サイトに入力する。



④ だまされた人の情報  
を使ってアカウント  
にアクセスし、個人  
情報やお金を盗む。

偽サイトを開かないことが一番だけど、どのメールがフィッシングかわからない。  
そこで、サービスへのログインの習慣で被害を防止する！

日頃から、IDやパスワードを入力するサービスには  
公式アプリや公式サイト（ブックマーク）からログインする習慣  
をつけることで、怪しいメールが来ても偽サイトを開くことを防止できます。

怪しいメールが来たら、保護者や警察に相談しましょう。