サイバーセキュリティ通信【R5-7】

令和5年5月
大分県警察本部生活安全部
サイバー犯罪対策課

フィッシングを起因とした不正送金事犯が急増中！

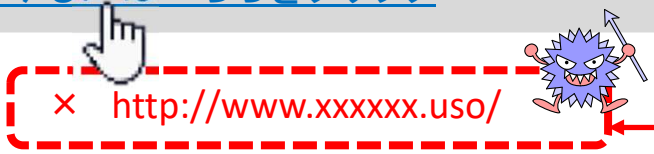
今年２月ころから、フィッシングを起因としたインターネットバンキングの不正送金事犯が被害が全国的に急増しています！

大分県下においては、昨年１年間で３件の被害にとどまっていましたが、今年は既に７件の被害を確認しており、被害が急拡大している状況です。

このようなメールは要注意です！

当社では、犯罪収益移転防止法基づき、お取引を行う目的等を確認させていただいております。
また、この度のご案内は、当社ご利用規約第〇条〇項〇に基づくご依頼となります。
お客様の直近の取引についていくつかのご質問がございます、下記のリンクをアクセスし、ご回答ください。
→続けるにはこちらをクリック

【フィッシングメール本文の一例】

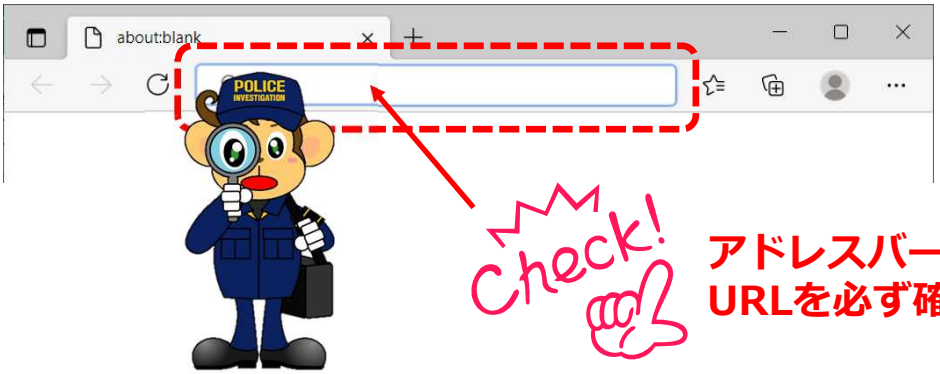


実際にアクセスするURL

フィッシングサイトを見抜くためには

認証情報を入力するときは、正しいインターネットバンキングサービスのURLにアクセスしているかを必ず確認してください。

また、メール中のURLをクリックして直接アクセスすることなく、正規サイトのURLを検索・入力してからアクセスするように心がけて下さい。



アドレスバーからサイトのURLを必ず確かめてください

フィッシングによる不正送金被害の**恐怖**

○　認証情報を入力した利用権者にも一定の過失があるとし、従来のように**全額補償を行わないという銀行もでてきています**

○　被害金が海外に送金されている事実も確認されており、**一度被害に遭うと、取り返すことは困難**であり、個人が重大な財産的被害をうける可能性があります

○　フィッシング被害に遭う可能性は、

全ての人にあります。

多額の預金を失わないように、
自らの預金をしっかりと守ってください！！！

フィッシングから身を守るには

●　インターネットバンキングを使う端末は
○　可能な限りインターネットバンキング専用端末を用意する（メールを閲覧する端末でインターネットバンキングにログインしない）
○　メールの内容について不安を感じたときは、銀行に電話で問い合わせる等し、インターネットという単経路の通信のみに頼らない
○　フィッシング対策ソフトやアンチマルウェアソフトを導入する
などの諸対策を確実にとるようにお願いします。

✍　銀行等各サービス提供者やフィッシング対策協議会のウェブサイトでは典型的事例や最新事例が紹介されていますので、ウェブサイトを閲覧して犯人の手口を学ぶことも大事です。
　また、トークン等のワンタイムパスワードや乱数表の数字入力については、送金時のみに追加入力が必要な情報ということにも注意してください。

※　送金手続きをしていないときに、送金手続きのみに必要となる

・　ワンタイムパスワード
・　乱数表（認証番号表など）の数字　等

の入力を求められたときは不正送金

を疑ってください！！

　フィッシングを見抜き、あなたの大切な預金を守ることができるのは、

あなた自身だけ

です。