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！

本年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2件の被害にとどまっていましたが、本年は2月から現在までの３か月間で既に7件の被害を確認しており、被害が急拡大しています。

手口は非常に狡猾です！

【フィッシングによる不正送金の犯行手口】

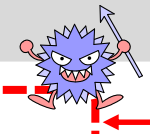
1　犯罪収益移転防止法の取引目的の確認等を騙り、フィッシングサイトにアクセスさせようとします。

2　メールに正規のインターネットバンキングサイトのURL表示や「アクセスはこちら」等の文言がありますが、実際にアクセスするとフィッシングサイトにアクセスさせられ、正規ログイン画面とそっくりなフィッシングサイトが表示されて、口座番号、暗証番号、ワンタイムパスワードや乱数表の数字等の入力を順次求められます。

3　同時にその裏側で、犯人はインターネットバンキングサービスに不正アクセスを行っており、必要となる情報を順次得ながら送金手続きをします。

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

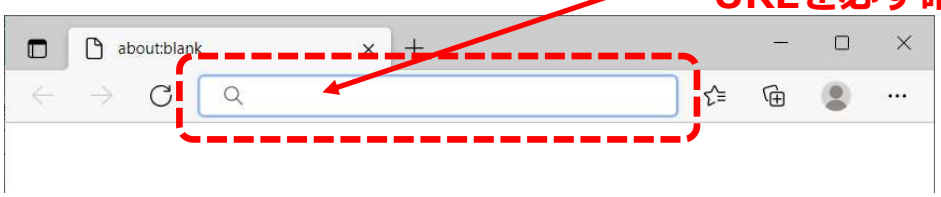
【フィッシングメール本文の例】



× http://www.xxxxxx.uso/ ← 実際にアクセスするURL

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**

フィッシングによる不正送金の被害は、従来のインターネットバンキング不正送金の被害と異なり、

○　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いるため、**一度被害に遭うと、被害金を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覚えたときは、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、トークンによる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です。

※　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。