◇吉田町防犯だより◇　第156号　令和3年4月

セーフティよしだ

発　行
吉田町役場防災課 地域安全部門
電話　33－2134
※静岡県警察より情報提供を受けて発行しております。

インターネットバンキングを装った詐欺が巧妙化

インターネットバンキングを装った詐欺被害は従来、被害者の口座に不正ログイン（侵入）し、犯人側が管理する口座に預貯金を移すケースが大半を占めていました。

しかし、昨年ぐらいから被害者の口座の金をプリペイドカードに課金したり電子マネーなどの購入に充てたりする手口が増えています。これは、口座から不審な高額送金に対する監視が強まったためで、プリペイドカードへの課金の上限額が数万から10万円程度、電子マネーの購入も1口あたりが代金は数万円程度で設定されていることが多く、「被害が小口化」する手口に代わってきているとみられています。

「フィッシング」詐欺とは？

フィッシング（phishing）とは、「魚を釣る（fishing）」のフィッシングのことではなく、人をだまして情報を盗み、最終的に金銭的な利益を得ようとする不正行為を意味します。例えば、インターネットバンキングやショッピングサイトの登録情報（ID、パスワード等）が盗まれ、勝手にお金が引き出されたり、物品を購入されたりする恐れがあります。

メールの件名に【重要】【至急ご確認ください】等、緊急を装う言葉が使われ、「異常なログインがあったので、至急パスワードを変更してください」「不正を疑う取引がありましたので、アカウントの使用を制限します。再開するには画面に従って手続きをしてください」等、受け取った人を慌てさせるような文章が続きます。そこでうっかりメール内のリンク（URL）をクリックしてしまうと、偽サイトが開き、ID やログインパスワード、カード番号等を入力させようとします。

実際、県内の銀行を騙り不審な SMS が不特定多数に送信され、偽サイトへ誘導する事例が報告されています。沖縄では3,000万円、北海道では190万円等の送金被害が報告されています。

詐欺に遭わないために

☞ 金融機関は口座番号や暗証番号を電子メールで問い合わせることはありません。
　※金融機関が行わないことを確認しておく

☞ メールに書かれているリンク（http 等で始まる URL）を安易にクリックしない。
　※本物のサイトの URL によく似せている場合もあるので注意。

☞ カード番号、暗証番号等の個人情報を入力する前に URL を今一度確認する。

＜被害に遭ってしまった場合は…＞
① サービス事業者へ連絡→ID、パスワードの変更、カード再発行の依頼
② 静岡県警察へ相談（「フィッシング 110 番」）☏054-271-0110（代表）
③ フィッシング対策協議会へ情報提供（被害情報の共有）
　(https://www.antiphishing.jp/)