サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和4年
5月17日
Vol.75

携帯電話会社を装ったメール・SMSに注意

携帯電話会社が提供する、電子決済サービスのIDとパスワードが**フィッシング**によって盗み取られ、**電子マネー等を不正利用される被害が多発**しています。

フィッシングとは、**実在する企業を装ったメールやSMS**を送り付け、フィッシングサイトに誘導し、**IDやパスワード等**を入力させて盗み取る手口です。

特徴１　不安をあおる内容で、メール本文に記載されたURLにアクセスさせようとする

＜メールの例＞

件名：重要なお知らせ【データ通信量の通信速度制限】

お客様

いつもご利用いただき誠にありがとうございます。
お客様の月間のデータ通信量がご利用中のプランの上限を超過したため、通信速度を低速に制限しております。
通信速度制限中にそのまま使い続けた場合、超過料金は発生しますので、早めに解除手続きの程よろしくお願いいたします。予めご了承ください。

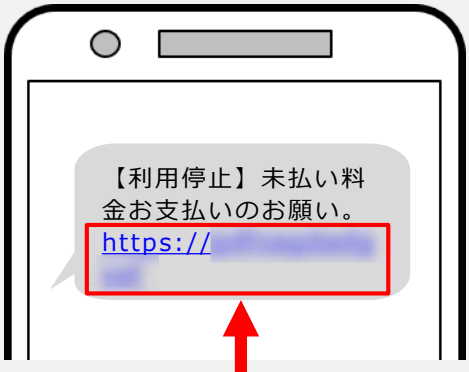
▼アカウントを更新してください

https://[redacted]

ご迷惑をおかけいたしますが、何卒ご理解いただきますようお願い申し上げます。

■発行者■
[redacted]株式会社
〒[redacted]

＜SMSの例＞



フィッシングサイトの可能性が高いので、絶対にアクセスしないでください！

特徴２　本物とそっくりのフィッシングサイトに誘導して、IDやパスワードを盗み取る

＜フィッシングサイトの例＞

メール本文中のURLにアクセスすると実在する企業のサイトとそっくりのログイン画面が表示されます。

何の疑いもなくIDとパスワードを入力すると、アカウント情報等が盗まれ、被害に遭う可能性があります！
メール本文中のURLからアクセスした場合は、絶対に入力しないでください！

実在する企業を名乗るメールやSMSが届いても、本文中のURLにはアクセスせず、企業が配布している公式アプリや、検索サイト経由で公式サイトを確認しましょう。

ID・パスワードを入力してしまった場合や、被害に遭った場合は、最寄りの警察署に相談してください。

相談窓口　愛媛県警察本部サイバー犯罪対策課 TEL089-934-0110(代)