10.スマートフォンやパソコンのトラブルにご注意

※実在する事業者を装う偽の SMS（※）

事例 スマートフォンにクレジットカード会社を名乗り「カードを不正使用されている」という SMS が届いた。添付の URL をタップすると本物そっくりのフィッシングサイトにつながり、ID、パスワード、クレジットカード情報等を入力してしまった。

（※）SMS：電話番号を宛先に設定して送受信するショートメッセージサービス

○クレジットカード会社や宅配業者など、利用者が多い企業名を騙る手口が多発しています。**決してメール内の URL をクリックしたり連絡したりせず無視しましょう。**判断に迷うときは事業者の公式サイトなどで真偽を確認してください。

○フィッシングサイトに、パスワード、認証コード、クレジットカード情報などを入力してしまった場合は、すぐにパスワードを変更し、クレジットカード会社や携帯電話会社に不正な請求が発生していないか確認してください。

※ワンクリック請求

事例 スマートフォンで無料のアダルト動画を再生しようと年齢確認ボタンを押すと、画面に「登録完了、登録料 40 万円を支払ってください」と表示された。解約しようと電話をすると、名前や生年月日を聞かれ「一旦支払えば調査して全額返金する」と言われ、コンビニに行き電子マネーで支払った。

○ 有料の契約であることが事前にわかりやすく書かれていなければ、契約は成立しておらず、料金を支払う必要はありません。

○ **「退会はこちら」などのボタンがあってもタップせず決して連絡しないようにしましょう。**電話をしてしまうと相手に着信履歴が残ります。知らない電話番号からの電話には出ないでください。メールアドレスを知られてしまった場合はアドレスを変えるのも対策のひとつです。

※実在する事業者を装う偽の電話

事例 スマートフォンに電話会社を名乗り「料金未納」という自動音声の電話がかかってきた。自動音声に従い、ボタンを押すとオペレーターにつながった。個人情報を聞かれ「電子マネーでお金を支払うように。」と言われた。

○スマートフォンだけではなく固定電話に国際電話がかかってくる場合もあります。不在着信に折り返すと高額な電話料金が発生してしまいます。決して折り返したり、お金を支払ったりせず、無視しましょう。

※偽のセキュリティ警告

事例 パソコンでインターネットを利用中、突然画面に「ウイルスに感染」とメッセージが出て警報音が鳴った。あわてて表示された事業者連絡先に電話しオペレーターに指示されるままに遠隔操作ソフトをインストールした。サポート代金として 5 万円のプリペイドカードをコンビニで買って番号を連絡したが「無効コードだ」などと言われ、繰り返しカードを購入し 30 万円支払った。

○実際には異常がないにもかかわらず、パソコンにトラブルが起きているかのような表示をして不安をあおります。
○電子マネーを購入させて、そのコード番号を連絡させるのは、典型的な詐欺の手口です。絶対に応じないでください。
○遠隔操作中にインターネットバンキングの画面を開かせて、振込みに誘導する事例もあります。

スマートフォンやパソコンで被害が発生し、**不安があれば早急に消費生活センターに相談してください。**

下記のホームページも参考になります。

独立行政法人　情報処理推進機構（IPA）

https://www.ipa.go.jp/security/anshin

※契約している携帯電話会社やプロバイダ、パソコンメーカーに相談してもよいでしょう。