AWAJI POLICE STATION NEWS

淡路警察署だより　２月号

サイバーセキュリティに関する普及啓発強化
～サイバー犯罪対策の推進～　　～サイバー攻撃の脅威～

２月１日～３月 18 日は「サイバーセキュリティ月間」です

フィッシングやサポート詐欺、ランサムウェアなど、皆さんの生活をおびやかす犯罪も身近となっています。

家庭や職場でセキュリティについて話し合い、一人一人が日頃から対策することが何よりも重要です。

政府では、毎年２月１日から３月 18 日を「サイバーセキュリティ月間」と定め、国家サイバー統括室（ＮＣＯ）を中心に、産官学民が連携して、サイバーセキュリティに関する取組を集中的に行っています。

フィッシングメールについて

フィッシングとは、実在するサービスや企業をかたりＩＤやパスワードなどの情報を盗んだり、マルウェアに感染させたりする手口です。

電子メールやＳＭＳのＵＲＬから偽サイト（フィッシングサイト）に誘導し、そこで個人情報を入力させる手口が一般的に使われています。

フィッシングメールには、官公庁や金融機関、宅配業者、通信事業者などの生活に密着した事業者などを装うものから、知人や取引先に成りすましたものなど様々なものが確認されています。

「支払情報が変更された」「１年以上利用がないためアカウントを停止する」などといって確認や再設定を促すものや「セキュリティ上の理由でブロックされている」と不安をあおるもの「お荷物をお届けにあがりましたが不在のため持ち帰りました」と日常生活で利用する宅配業者を装うものなど、信用してもおかしくない内容で届きます。

フィッシングメールやフィッシングサイトは非常に精巧に作られており、本物のメールやサイトと見分けがつかないことが多く、判別は困難です。

【対策】

○　メッセージに記載されたＵＲＬをクリックしない
○　事業者などからの連絡は公式アプリやブックマークした公式ページから確認する
○　パソコンＯＳやソフト、アプリのアップデートを行う
○　ＩＤやパスワードの使い回しはしない
○　身に覚えの無い通信料やアプリのインストールがないかを確認する

偽サイト・詐欺サイトについて

インターネットショッピングにおいて「代金を支払ったが商品が届かない」「別の商品が届いた」など、偽サイトや詐欺サイトによる相談も多く寄せられています。

これらの相談は「商品名で検索をかけた結果、偽サイトや詐欺サイトにたどり着いた」というケースが多くみられます。

さらに、商品が届かないことを連絡すると、担当者から「商品が欠品している。キャッシュレス決済サービス（〇〇Pay など）を使って返金する」と言われ、指示通りにスマートフォンを操作すると、返金を受けるはずのお金を送金させられてしまうという手口が急増しています。

返金名目の詐欺にも注意してください。

【対策】

○　価格の安さや入手困難な商品に惑わされず、信頼できるお店を利用する

○　会社名やサイト名などを検索し、正規サイトが別に存在しないか確認する

○　検索エンジンから直接ショッピングサイトに移動するのではなく、正規サイトのＵＲＬからショッピングサイトに移動する

○　決済方法を確認する

（例）　決済方法が「口座振り込みのみ」になっていないか

（例）　決済方法を「口座振り込み」に変更するよう依頼されていないか

（例）　振込先は法人名かどうか

個人名の場合は、代表者や責任者、運営者以外の個人名になっていないか

上の（例）に該当しない場合でも、偽サイトや詐欺サイトである場合がありますので十分に注意してください。

アカウントの乗っ取り、なりすましについて

ＳＮＳアカウントの乗っ取り、なりすましについても多数の相談が寄せられています。

ＳＮＳには個人情報が多く載せられており非常に大切なものなので、アカウントが乗っ取られることがないよう、ＩＤやパスワードなどの取扱いには気を付けましょう。

●アカウントの乗っ取りの例●

知人を装ってＳＮＳのＤＭ（ダイレクトメッセージ）が届き、

①　「オンラインアンバサダーの座を争っています。投票いただけませんか」などと電話番号を聞かれる

②　電話番号を教えると「あなたの投票を確認したいので、送られてくる６桁の番号を教えて」などといって、ＳＭＳで送られた６桁のコードを聞かれる

③　自分の携帯電話番号宛に届いた６桁の認証コードを伝える（絶対に他人には教えない）

④　自分のアカウントのパスワードが変更され、アカウントが乗っ取られて、さらに自分になりすまして詐欺などのＤＭを送られる

というものになります。

【対策】

○　個人情報を安易に教えない

（「認証コードを教えて」は詐欺と思いましょう）

○　ＩＤやパスワードの使い回しはやめましょう

○　２段階認証など、更なるセキュリティ対策をしましょう

●アカウントのなりすまし●

著名人を装ったなりすましアカウントも増えています。

著名人からのＤＭ（ダイレクトメッセージ）で「お世話になっております。ご注目とご支援ありがとうございます。感謝の気持ちを込めて、今月から新しいＳＮＳグループを開設しました。投資知識や株式知識などを無料で共有します。参加費や条件は一切ありません」などと送られ、投資詐欺に誘導するものやＩＤ・パスワードを窃取して不正ログインや不正取引、情報漏洩を目的としているものなど、さまざまなものがあります。

【対策】

○　著名人や会ったことがない人からのＤＭは疑う

○　十分な説明がないままグループチャットに誘われたら疑う

○　「投資テクニックを教えます」「無料」などの文言があれば疑う

○　著名人からのＤＭや広告であれば、本人が詐欺に関する注意喚起を行っている場合があるので調べてみる

子どもを守るために

インターネットは、子どもたちにとっても日常生活に欠かせないアイテムになっています。

そのような中、ＳＮＳやオンラインゲームを通じて知り合った相手に呼び出され被害に遭うケースや裸の写真や動画を送信させられる「自画撮り被害」が発生しています。

どのような危険があるか、安全に使うためにはどうしたら良いかを知り、家庭や学校でルールを作り、守っていきましょう。

また、子どもが困ったときにためらわず相談できるよう、日頃のコミュニケーションを大切にするとともに、信頼できる公的機関に相談してください。

話合いのきっかけに、ぜひサイバー防犯標語「あひルのおやコ」をご活用ください。