【個人情報の悪用（フィッシング・不正アクセス）】

通信販売、金融機関等から不審なＥメール（SMS）が届いた

よくある相談内容

○　Ｅメールの URL から誘導されたサイトで個人情報をだまし取られた
○　ネットバンキングの預金が不正に送金された・・
○　利用した覚えのない請求（キャリア決済）がきた・・
○　今まで使えていたアプリにログインできなくなった・・　etc

上記でお困りの方は、フィッシング被害に遭われている可能性があります。
一般的な手口や対処法を紹介しますので、以下をご確認ください。
※ フィッシング…実在する組織を偽って、ID・パスワード、クレジットカード番号等の個人情報を詐取すること

フィッシングの一般的手口

犯人が、実在する企業を装い、
○　「ログインアラート、アカウント情報を確認してください」
○　「お支払い方法に問題があります」
○　「登録情報を確認してください」　等の Ｅメール（SMS）を送信

メールの文中には URL リンクが張られており、受信者が「URL からログイン」「ここをクリック」などの文言に誘導され、偽のサイトへアクセスし、アカウント情報等を入力することで個人情報がだまし取られる。

フィッシング被害による影響

各種サービスの不正アクセス（不正利用）被害など、個人情報が悪用される可能性がある。

フィッシング被害に遭った場合の対処法（一例）

【入力項目別対処要領】

○　ID・パスワード等のアカウント情報を入力した場合
・　対象サービスの公式サイト又は公式アプリからパスワードを変更する。
・　同じ ID・パスワードで設定しているサービスや SNS アカウントがある場合は、併せて変更する。

○　**銀行口座の情報を入力した場合**

・　インターネットバンキングに関する ID･パスワードを入力した場合は、当該金融機関のサービスを停止するとともに、パスワードを変更する。

・　預貯金口座に関する口座番号、暗証番号等を入力した場合は、当該金融機関の口座を停止又は暗証番号を変更する。

○　**クレジットカード情報を入力した場合**

カード番号、カード名義人、セキュリティコード等を入力した場合は、クレジットカード会社へ連絡して利用を停止し、不正利用を確認する。

○　**電話番号やメールアドレスを入力した場合**

別の迷惑メール（SMS）を受信する可能性があるため、必要に応じて電話番号やメールアドレスを変更する。

【警察への相談】

身に覚えのない決済や引き落としがある場合、アカウントにログインできなくなった場合など、被害が疑われる場合は、メールや SMS が確認できる端末や引き落とし状況が分かる資料等、関係資料を持参し、住居地を管轄する警察署に事前連絡の上、相談する。

被害に遭わないための対策

★　メール（ＳＭＳ）の URL リンクには**安易にアクセスしない。**

○　**ブックマークした公式サイトや公式アプリからの利用を基本**とし、パスワードや認証コード等を安易に入力しない。

○　「アカウント停止」「支払いの未納」等、不安を煽るメールは疑う。

○　迷惑メール等の受信拒否について携帯電話会社に相談する。

○　端末の OS は常に最新の状態にアップデートする。

【被害軽減策】

○　パスワード対策

・　できるだけ「長く」、「複雑」なものに設定し、使い回さない。

・　多要素認証が提供されている場合は利用する。

○　キャリア決済限度額の低価格設定

参考サイト

前ページ「参考リンク集」を参照。

○　フィッシング対策協議会

○　迷惑メール相談センター（日本データ通信協会）