別添１

作品テーマ例

【ＳＮＳ型投資・ロマンス詐欺】

ＳＮＳ型投資詐欺は、著名人の名前・写真を無断で使用した嘘の投資広告や、「必ず儲かる投資方法を教えます」などのメッセージを送ることで投資話を持ち掛けます。

ロマンス詐欺は、ＳＮＳやマッチングアプリを通じて知り合った者に恋愛感情や親近感を抱かせ、結婚のための資金調達などと投資を勧めます。

その後、どちらもトークアプリに誘導し、投資に関するメッセージのやりとりを重ねて被害者を信用させ、投資名目で金銭等をだまし取る詐欺です。

(被害の例)

・ＳＮＳ上で著名人が投資を勧める広告を見つけてアクセスしたところ、著名人を名乗る者のＳＮＳアカウントに誘導され、「必ず儲かる投資グループ」を勧められグループチャットに加入した。
その後、グループチャット内で勧められた投資の運用サイトに登録し、指定の銀行口座に振り込むと運用利益が上昇。出金を試みるも「保証金」「税金」などの理由をつけて出金させてもらえず詐欺に遭った。

・ＳＮＳで知り合った異性に恋愛感情を抱くようになったところ、相手から「２人の将来のために投資でお金を貯めよう」と勧められた。相手に勧められるがまま投資専用アプリをインストールし、指定された銀行口座にお金を振り込むと相手と連絡が取れなくなった。

(特徴)

・著名人が投資の広告に悪用される
・マッチングアプリで知り合い、直接会ったことのない人から「会いたいから旅費を送ってほしい」「結婚するのにお金が必要」などと金銭を要求される
・ＳＮＳやマッチングアプリで知り合った人から投資の話を持ち掛けられ、投資に関するグループチャットに誘導される
・偽の投資サイトや投資アプリを登録し、入金すると利益が出たように見せかける
・出金しようとすると「出金するには税金がかかる」などの理由で、さらに送金を求められる

(対策)

・実際に会ったことがない人から「投資」の話をされたら詐欺を疑う
・「必ず儲かる」「確実に利益が出る」「あなたにだけ教える」という儲け話は詐欺
・勧められた投資アプリが正規の物かインターネットで確認する
・振込先の口座が個人名義、振込先が振込みのたびに変わるなど不審な口座へは振り込まない

【サポート詐欺対策】

インターネットを閲覧中に、突然、ウイルス感染したかのような嘘の画面を表示するなどして不安をあおり、画面に記載されたサポート窓口に電話をかけさせ、遠隔操作ソフトをダウンロードやインストールさせ、サポートの名目で金銭をだまし取ろうするものです。

(被害の例)

・警告画面に表示された連絡先に電話したら、ウイルスの除去費用を請求された。
・サポート料として、次々と料金を請求されるので、コンビニで電子マネーを購入し支払ってしまった。

(特徴)

・偽の警告画面に実在する企業のロゴ等が使われている場合がある。
・警告音を鳴らしたり、警告メッセージを音声で流したり、偽のセキュリティ警告画面を閉じられないようにして不安をあおる。
・偽のサポート窓口に電話を掛けると、遠隔操作ソフトをダウンロード・インストールするよう誘導されたり、有料のサポート契約を勧められたりする。
・支払いはクレジットカード決済や各種ギフトカード、コンビニ決済や電子マネー等が使われる。

(対策)
・偽のセキュリティ警告が表示されたら、「ESC」を長押ししてブラウザを終了する。
・ブラウザを終了できない場合は、強制的に終了する。
(Windows の場合 :「Ctrl」+「Alt」+「Delete」を同時に押してタスクマネージャを起動し、利用中のブラウザを選択、右クリックして「タスクの終了」を選択する。)
・偽のセキュリティ警告画面に表示されている電話番号に電話しない。
・電話先の相手の指示に従って、アプリやソフトウェア等をインストールしない。
・アプリやソフトウェアをインストールした場合は、ネットワークから切断してウイルスチェックを行い、ダウンロードしたものを削除、インストールしたものをアンインストールし、可能であれば初期化を行い、各種パスワードを変更する。

【フィッシング対策】

フィッシングとは、実在の企業・団体をかたり、メールやＳＭＳを送り、正規のＷｅｂページに酷似した偽サイトへ誘導し、ＩＤやパスワード等のアカウント情報、クレジットカード番号、暗証番号等の重要な情報を入力させて盗み取る犯罪行為です。

(被害の例)
・インターネットバンキングに不正アクセスされて、勝手に送金される。
・クレジットカードで身に覚えのない決済をされる。
・電子決済サービスにログインされて、電子マネーで買い物をされる。
・偽のアプリをインストールしてしまい、スマートフォンから勝手に知らない人にＳＭＳが送られる。

(対策)
・「緊急」「至急」等、何らかの行動を急かす文章であっても、メールに記載されたリンクを開かない。
・偽物のサイトを開いても、すぐに閉じる。
・公式Ｗｅｂサイトを事前にブックマークしたり、企業が提供する公式アプリをインストールしておき、そこから確認する習慣を作っておく。
・アカウント情報（ＩＤ、パスワード）やクレジットカード情報等の重要な情報、住所や氏名等の個人情報を入力しない。
・ウイルス対策ソフトやブラウザには、偽サイトへのアクセスを遮断する機能があるため、常に最新の状態を保っておく。

【ＩＤ・パスワードの適切な管理】

ＩＤ：個人を識別するための符号
パスワード：本人であることを示す認証情報
正しいパスワードを入力した人が本人であると認められるのは、「パスワードは本人しか知らない」という原則があるからです。パスワードが漏えいしてしまうと、悪意のあるユーザがパスワードを盗用し、その本人になりすまして不正アクセスを行います。

(対策)
・名前や誕生日、辞書掲載の単語等、他人が推測できるパスワードは設定しない。
・アルファベット、数字、記号、大文字・小文字を混ぜ、できるだけ長くする。
・パスワードの使い回しをしない。
・パスワードは絶対に人に教えない。
・二段階、多要素認証を活用する。(指紋等の生体認証やワンタイムパスワード等)
・パスワードは適切に保管・管理する。(ＩＤとパスワードは別々にメモする。不特定多数の人が使用する端末にはブラウザにパスワードを記憶させない等)

【違法・有害情報の通報等】

インターネット上には、児童ポルノ画像、違法薬物の販売広告や売春等の違法情報、犯罪の請負や集団自殺の呼び掛け等の有害情報が流通しています。

(違法情報)

・わいせつ関連情報（18 未満の児童を対象とした画像や動画の投稿、性器が明らかに確認できる無修正やそれに近い画像や動画の掲載など）
・薬物関連情報（違法な薬物の使用を示唆したり、販売を目的とした書込み）
・出会い系・売春情報（インターネット掲示板や SNS で性行や援助交際の相手を募集するなど）

(有害情報)

・情報自体から違法行為（拳銃等の譲渡、爆発物等の製造、児童ポルノの提供、公文書偽造、殺人、自殺関与、脅迫等）を直接的かつ明示的に請負・仲介・誘引等する情報
・人を自殺に誘引・勧誘する情報（集団自殺の呼び掛け等）
・人の殺人現場の画像等の残虐な情報のうちテロリズムに関するもの
・犯罪や違法行為に結び付く又はそのおそれの高い情報のうちテロリズムに関するもの（テロ実行の呼び掛け、テロの手法の教示、テロのための資金提供の呼び掛け等）を不特定の者をして掲載させることを助長する情報

(違法情報・有害情報を発見したら)

・違法情報・有害情報を発見した際は、警察又はインターネット・ホットラインセンター（https://www.internethotline.jp/ ）に情報提供をお願いします。

(緊急に対応が必要な情報を発見したら)

殺人・爆破予告、自殺予告等の人命に関わる事案は警察に通報（緊急を要するものは 110 番）してください。

(インターネット・ホットラインセンターとは)

通報を受けたインターネット上の情報をガイドラインに照らして判断し、警察への情報提供、プロバイダや電子掲示板の管理者等に対する送信防止措置等の対応依頼、関係機関等への情報提供等、フィルタリング事業者に対する情報提供を行う機関です。