別添２

作品テーマ例

安全で安心なサイバー空間づくり

例

【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）

【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たり、サポートの名目で金銭を騙し取ろうとしたりするものです。

（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煽る。
・偽のサポート窓口に電話をかけると、遠隔操作ソフトのダウンロード・インストールへ誘導されたり、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、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、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。

【闇バイト対策】

いわゆる「闇バイト」は犯罪実行者の募集です。ＳＮＳやインターネット上の掲示板等で、仕事の内容を明らかにせず、短時間で高収入が得られる等の甘い言葉で犯罪の実行者を募集する投稿が掲載されています。応募してしまうと、詐欺の受け子や出し子、強盗の実行犯など、犯罪組織の手先として利用され、犯罪者になってしまいます。

（例）

・ＳＮＳに投稿されていた闇バイトに応募し、指示に従ってお年寄りからキャッシュカードを受け取り、ＡＴＭでお金を引き出していたところ、駆け付けた警察官に逮捕された。
・闇バイトに申し込み、自分名義で作った口座のキャッシュカードを指示された住所に送り、報酬をもらった。その後、警察官が自宅に来て逮捕された。その後、職場から解雇され、被害者から損害賠償請求された。
・ＳＮＳ上で目にとまった闇バイトの投稿に応募したところ、一定時間経過するとメッセージが消えるアプリを使うように指示された。指示役の要求に応じて運転免許証の写真を送ったところ、仕事の内容が強盗であると知らされた。やらなければ痛い目に遭わされると思い、強盗に加担してしまった。

（特徴）
・ＳＮＳ等の投稿には、「高額バイト」「即日入金」「書類を受け取るだけ」等と、好条件に見える情報が記載されている。
・申込時に匿名性が高いアプリのインストールや身分証明書の送付等を求められる。
・やめたいと思っても、応募の時に送った身分証明書から「家に行く」「周囲の人に危害を加える」等と犯罪組織から脅され、逮捕されるまで抜け出せない。
・逮捕されても犯罪組織は助けてくれない。

（対策）
・甘い言葉には騙されない
・楽をして大金を稼げるアルバイトは存在しないということを覚えておく
・怪しいと思ったら、家族や警察に相談する

【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
・薬物関連情報
・振り込め詐欺等関連情報
・不正アクセス関連情報

（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。