

作品テーマ例

【フィッシング】

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

【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
- ・パソコン内に保存していたネットバンキングのアプリから送金するよう指示をされ、送金画面になったところで送金金額を勝手に操作され高額な金銭を振り込んでしまった

(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
- ・偽のサポート窓口で電話をかけると、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
- ・ネットバンキングで送金するよう誘導された際、秘匿事項である旨を告げられ席を外すように告げられる

(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
- ・ネットバンキングを起動する指示が出たら詐欺を疑う、安易にIDやパスワードを教えない、入力しない

【偽情報・誤情報対策】

1 偽情報

意図的に作成・流布される虚偽の情報のことをいいます。

誰かを騙したり、誤解させたり、混乱させたりする目的で、意図的に虚偽の内容が作られ、広められるという特徴があります。

2 誤情報

意図的でなく、誤解や勘違いによって拡散した間違い情報のことを指します。

この場合、必ずしも悪意があるとは限りません。

(過去の例)

・令和6年1月1日に発生した能登半島地震の際、埼玉県内に居住する男性がSNS上に「倒壊した建物に親族が挟まれて重篤な容態に陥っている」等といった偽情報の書き込みをした。

・平成28年4月16日に発生した熊本地震の際、神奈川県内に居住する男性がSNS上に「動物園からライオンが逃げた」という書き込みとともに加工した写真を投稿した。

※上記投稿をした男性らはいずれも偽計業務妨害で逮捕された

(対策)

- ・信頼できる情報源（公的機関、報道機関、専門家など）からの情報かを確認する
- ・複数の情報源を比較する
- ・古い情報や更新されていない情報は現在の状況と異なる可能性があるため、常に最新の情報を確認する
- ・偽情報サイトには悪意ある広告やポップアップを利用してサポート詐欺に誘導するものもあるため、セキュリティ対策サービスを活用する

【誹謗中傷・SNSの適正利用】

・誹謗中傷

根拠のない嘘や悪口を言いふらし、他人の名誉や社会的評価を傷つける行為を指します。

SNSやネット掲示板への書き込みも対象となります。

・SNSの適正利用

ルールとモラルを守り、他者への配慮を欠かさずに安全なコミュニケーションを行うことです。

(注意点)

1 投稿者の特定

情報開示請求などの手続きにより、投稿者は匿名表示にしていた場合でも特定される。

2 拡散者の責任

自身が発信者でなくても、誹謗中傷の投稿をリポスト等して拡散させた場合も法的責任を問われる。

(対策)

1 画面の向こう側を意識

相手も自分と同じ人間であることを意識し、言葉遣いや表現に配慮する。

2 投稿内容

感情に任せた投稿は避ける。

また、個人情報につながる内容（住所、氏名、職場等）や肖像権や著作権（他人の写真や動画、作品等）に該当するデータ等は投稿しない。

3 SNSとの健全な付き合い

利用時間を決める、未成年者の利用においてはペアレンタルコントロールやフィルタリング機能を活用して安全を管理する。

【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ある。

パスワードが漏えいしてしまうと、悪意のあるユーザー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、事典掲載の単語等、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
- ・パスワードの使いまわしはしない
- ・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）

