CyberNews

令和2年11月
宮城県警察本部
サイバー犯罪対策課

侮れないソーシャルエンジニアリング

ソーシャルエンジニアリングとは、ネットワークに侵入するために必要となるパスワードなどの重要な情報を、**インターネットなどの情報通信技術を使わず**、人間の心理的な隙や行動のミスなどにつけ込んで入手する方法です。

● ショルダーハッキング（覗き見する方法）

パスワードや暗証番号などの秘密の質問の入力画面を盗み見る、会話を盗み聞きするなど、記憶力があれば誰にでも実行できる手口です。過去には、消防局員が上司のパスワードを盗み見て人事情報を拡散した事案や、男子高校生がアルバイト先で買物客のカード番号や有効期限を盗み見て不正利用する事案などが発生しています。

● トラッシング（ゴミ箱をあさる方法）

ネットワークに侵入するため、サーバやルータなどの設定情報、IPアドレスの一覧、ユーザ名やパスワードが記載された資料（紙や記録媒体）をゴミ箱の中から探し出します。トラッシングと似た手法として、郵便ポストに入っている郵便物をそのまま持ち去って情報を盗むという「メールハント」という手法も存在します。

● 電話でパスワードを聞き出す方法

利用者のふりをして、ネットワーク管理者に電話をかけ、ID・パスワードを聞き出したり、パスワードの変更を依頼したりします。また、管理者になりすまして、直接利用者にパスワードを確認するといったケースもあります。

※ ソーシャルエンジニアリングへの対策 ※

＊ログイン情報やパスワードなどの情報取扱いの厳格化

電話では重要な情報を伝えないというルール作りや、本人確認の徹底はソーシャルエンジニアリング対策の基本です。

＊情報廃棄手順の明確化

紙媒体を廃棄する際には、必ずシュレッダーにかける、記録媒体のデータは確実に消去、物理的破壊を行うなど徹底し、情報を盗まれるリスクをなくしてください。

＊オフィスや公共交通機関などでの重要情報の取扱い

クレジットカード情報やID・パスワードなどを入力する時は、慣れた場所であっても周りに注意することが重要です。

決して人ごとではありません。基本を徹底して被害防止に努めましょう。