ソーシャルエンジニアリング

～身近に潜むハッキングに御用心⚠～

情報窃取はマルウェアなどの高度な技術を使ったものだけではありません。人間の心理的な隙や行動のミスにつけ込み、個人情報や機密情報を盗み出す「ソーシャルエンジニアリング」にご注意ください！

ソーシャルエンジニアリングの主な手口と対策

なりすましのメール（スピアフィッシング）

〈手口〉
・会社や関連会社の社員、取引先等を装い特定の個人や組織にフィッシングメールを送り付ける

〈対策〉
・安易にメールの添付ファイル、リンクは開かない
・送金先変更等の重要な内容であっても、鵜呑みにせず電話等メール以外の手段で相手に確認する

なりすましの電話

〈手口〉
・システムの利用者や管理者等になりすまして担当者に電話をかけ、社員や顧客情報、パスワードなどを聞き出す

〈対策〉
・電話口ではパスワードや企業情報などを伝えない
・あらかじめ社内で電話対応のルールを決めておく

ＳＮＳを悪用

〈手口〉
・特定の人物になりすましてターゲットの情報を抜き取る

〈対策〉
・ＳＮＳの使い方について、社内で教育を行う
・SNSに職場の状況がわかる情報を投稿しない
・機密情報は、家族にも漏らさない

のぞき見（ショルダーハッキング）

〈手口〉
・モニター画面やキーボード操作をのぞき見し、ログイン情報などを不正取得する

〈対策〉
・人の目がある環境ではパスワードを入力しない
・パソコン、スマホから離れるときは必ずロックをかける

ゴミ箱を漁る（トラッシング）

〈手口〉
・捨てられたメモや書類を漁って機密情報やパスワードなどを不正取得する

〈対策〉
・紙媒体はシュレッダーにかける
・ＵＳＢなどの記録媒体は物理的に破壊する

人の恐怖心を利用する（スケアウェア）

〈手口〉
・偽の警告画面を表示させて使用者の不安を煽り、不正なソフトをインストールさせようとする

〈対策〉
・不審なリンクやポップアップは開かない、またはブラウザの設定でポップアップをブロックする
・慌てずに画面を閉じる