



フィッシング詐欺SMS

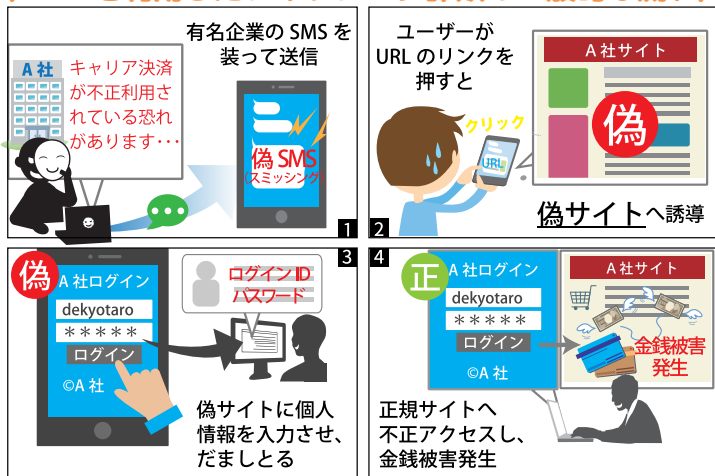
最近、本人確認の2段階認証や企業・自治体からの情報配信用としてなど、さまざまなシーンでSMSが利用されるようになりました。

SMSは電話番号を利用してメッセージをやりとりするサービスで、一般的に受信者がメッセージに気づきやすく、開封率が高いといわれています。便利になった反面、こうしたSMSの特徴を悪用した詐欺が最近急増しているため注意が必要です。

有名企業・ブランドになりすます

SMSを利用したフィッシング詐欺の事例が急増しています。よくある手口としては、宅配便業者、携帯電話事業者、通販会社などの有名企業になりすましてSMSを送るものです。このSMSにより、偽サイトへ誘導した上で、ID・パスワードなどの個人情報盗み取り、最終的に金銭をだまし取るものです。

<SMSを利用したフィッシング詐欺の一般的な流れ>



●新しい手口にも注意が必要です

スマートフォンの中にはアプリのログイン情報、ショッピングサイトやオンラインバンクのアカウント情報など、重要な情報が大量に保存されています。

そして、こうした情報は悪意のある攻撃者にとっての格好のターゲットとなっています。

ID・パスワードなどの個人情報を盗み取る手口だけではなく、不正なアプリをインストールさせ、そのスマートフォンから同じ内容のSMSを他の宛先に多数送信させる悪質な手口も報告されています。

不審なSMSにも十分注意するようにしましょう。



迷惑メール・詐欺
メールの手口を知る

