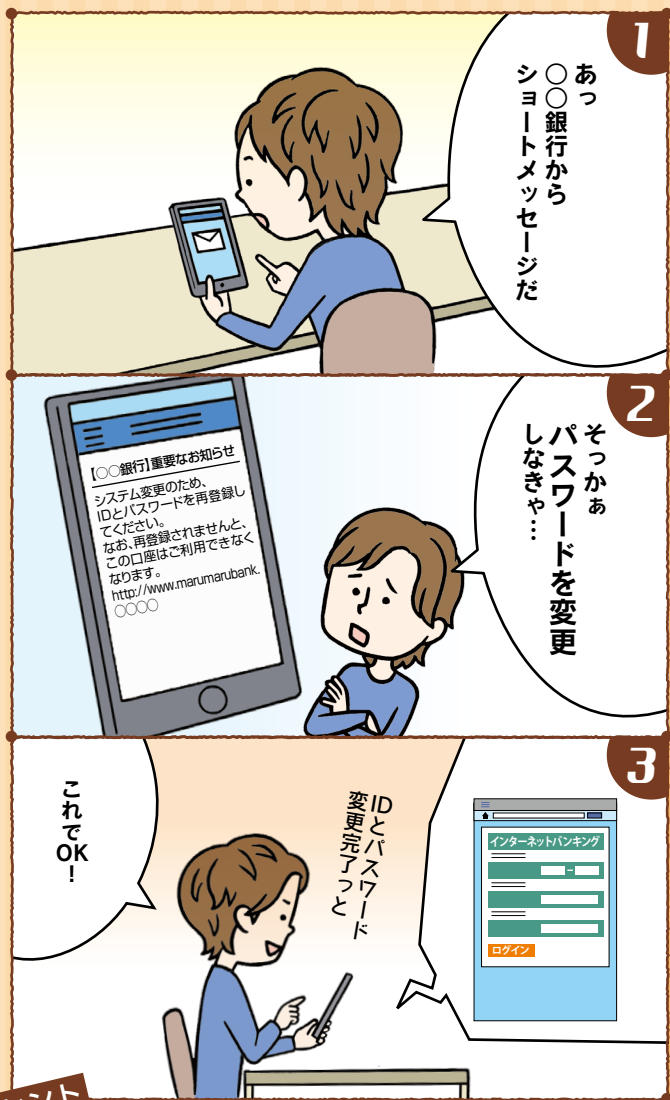


Q



「インターネット犯罪」 にご用心！②

ある日、銀行を名乗るショートメッセージ(SMS)が。次の対応のどこに問題があるのわかりますか？



ヒント

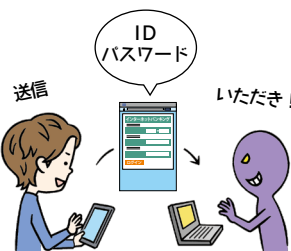
IDやパスワード変更に関する
ショートメッセージを簡単に信用して
しまってよかったですでしょうか？

A

これが 「フィッシング詐欺」 の手口です！



銀行を装ったショートメッセージやメール等でIDやパスワードを盗む



件名で「重要なお知らせ」などと危機感をあおり、銀行を装った二セのショートメッセージやメールを開かせます。URLから二セのサイトに誘導し、IDやパスワードを入力させ、それらの情報を盗みます。



用心する「ポイント」はココ！



1 パスワードの入力を求めるショートメッセージに注意。

銀行がショートメッセージやメールでパスワード等重要情報の入力をお願いすることはありません。また、心当たりのないショートメッセージやメールは開かないようにしましょう。

2 銀行の注意喚起の確認を。

銀行ではウェブサイト等を通じて最新の被害手口などについての注意喚起をしています。注意喚起を見て、怪しいと思った場合はパスワード等の重要情報の入力はしないようにしましょう。

3 銀行のウェブサイトを「お気に入り」に登録。

取引銀行のウェブサイトを、あらかじめウェブブラウザの「お気に入り」に登録し、そこからアクセスしましょう。取引銀行がアプリを提供している場合は、アプリから操作することも有効です。

さら
ここ
にも
ご用
心！

メールの添付ファイルや、誘導したウェブサイト等からマルウェアに感染させることも。日頃から注意し、スマートフォンやパソコンは安全に保ちましょう。