CyberNews

平成31年1月
宮城県警察本部
サイバー犯罪対策課

銀行をかたるショートメッセージに注意

昨年12月から、実在する銀行を装ったショートメッセージ（SMS）が大量送信され、フィッシングによる不正送金の被害が発生しています。

ショートメッセージの実例

＊銀行名・リンク先は加工しています。

＊第一暗証はワンタイムパスワードではございません。
www.XXXXX.pl　【〇〇▲▲銀行】
解除　http://●●▲▲/8N
12/31　10:00

注意：ダイレクトのパスワードが翌日に失効するのでwww.XXXXX.pl　により、更新をお願いします。　【〇〇▲▲銀行】
解除　http://●●▲▲/8N
14:00

フィッシングサイトは、銀行のインターネットバンキングのログイン画面を模倣した偽サイトであり、IDやパスワードを入力してしまうと、不正送金などの被害にあうおそれがあります。

被害を防ぐためのポイント

● ショートメッセージのリンクは絶対にクリックしない

通知されているURLをWebブラウザに直接入力するか、Webブラウザのブックマークに正しいURLを記録しておき、そこからアクセスすることを心がけましょう。

● 鵜呑みのせず、金融機関に確認する

正規のWebサイトで注意喚起している場合があるので、郵便物などで連絡先を調べて連絡してください。

※　万一ID・パスワードを入力してしまった場合は、すぐ銀行と警察に連絡してください。