サイバーセキュリティ通信【第19号】

令和元年6月
大分県警察本部生活安全部
サイバー犯罪対策課

スミッシングによる被害が急増中！

本年４月から５月にかけて、通信事業者を装った偽ショートメール（SMS）を利用したフィッシング詐欺（下線部の手口を「**スミッシング**」と呼びます。）に関する相談が急増しています！

届いた偽SMSの内容に従って、アカウントのIDやパスワードを入力した人は、通話料金にサービス利用料を上乗せして支払う「キャリア決済」を不正に利用されるという被害も多数報告されています。

偽SMSの内容は非常に巧妙ですので、被害防止対策には十分な注意が必要です。

偽SMSの内容は非常に巧妙！！

【偽SMSを使った犯行手口】

1　アカウントやキャリア決済の不正使用の可能性を通知する通信事業者を装ったＳＭＳが届く。

2　ＳＭＳに記載されたＵＲＬにアクセスすると、正規ログイン画面とそっくりな偽サイト（フィッシングサイト）が表示されて、ＩＤとパスワードの入力を求められる。

3　アカウントのIDとパスワードを入力すると、IDとパスワードが盗み取られ、キャリア決済により電子マネーや商品を不正に購入される。

偽SMSの内容の特徴

偽SMSの内容には、次のような特徴があります。

お客様のアカウントに異常ログインの可能性がございます。下記URLにて検証お願いします。

http://www.事業者名-xxx.com

【今までに確認されている文言】

- アカウントが異常ログインされているので検証をして下さい。
- お客様がご利用のキャリア決済が不正利用の可能性があります。ウェブページで二段階認証をお願いします。

など

URLがhttp **s** で始まっていない。

URLに通信事業者名が含まれるなど、一見本物に見える。

スミッシングから身を守るためには

① SMSの受信設定で「**海外SMSの受信拒否**」ができる場合には、なるべく設定しておいてください。

② 「海外SMSの受信拒否」を設定した場合、海外のソーシャルネットワークサービスなどの本人確認用SMSが届かなくなる可能性がありますので、受信の予定がある場合には、その設定を解除するなど、こまめな設定変更をしてください。

③ SMSを受信し、通信事業者が送信元となっていたとしても、**メッセージに記載されたURLには安易に接続しない**ようにしてください。

④ メールやSMSに記載されているURLが、**正規の通信事業者のサイトであるか**、公式ホームページなどで**確認**してください。

⑤ 万一、偽サイトでIDやパスワードを入力してしまった場合には、直ちに契約している通信事業者に連絡してください。

あなたの会社や団体で研修の一環として、サイバーセキュリティセミナーを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。
大分県警察本部生活安全部サイバー犯罪対策課
企画・指導・サイバーセキュリティ係　Tel:097－536－2131