偽メールや偽サイトに注意しよう!

スマートフォンやパソコンを使用していると、発信者を装った偽の電子メールやショートメッセージが送られてくることがあります。

多くの場合で偽サイトへ誘導され、個人情報（ID・パスワード、クレジットカード情報等）を盗まれたり、コンピュータウイルスに感染したりします。

被害に遭わないために対処法を身につけましょう！

1　実際に県内で相談があった事例

大手ショッピングサイトを装った偽メールが届き、記載されているリンクをクリックすると偽サイトへ誘導され、クレジットカードの番号などを要求される。

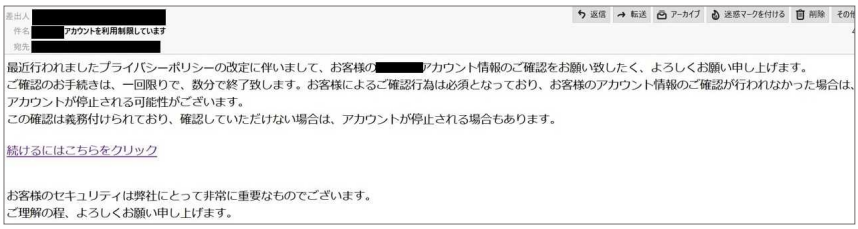

図１　大手ショッピングサイトを装った偽メール

図２　偽ログイン画面

図３　クレジットカード番号等要求画面

2　トラブルに巻き込まれないために

⑴　不審なメールは開かない、開いてもおかしいと感じた場合はリンクをクリックしない。

○　メールアドレスは簡単に偽装することができるため、アドレスが合っているからといって信じてしまうと危険です！

⑵　サイトを開いた場合はURL（ホームページアドレス）を確認する。

○　偽サイトを見た目で判断するのは困難です。URLの末尾が「co.jp」や「.com」ではなく、「.tk」や「.ga」等の普段使われないものが多いです。

⑶　個人情報の入力は慎重に！

○　おかしいと感じたらその企業の連絡先をインターネットで調べ、問合せしましょう。

⑷　２段階認証を導入する。

○　詳しくは「重要なパスワード管理！」のページを御覧ください。

警察の相談窓口

・警察本部警察安全相談窓口
　TEL 098-863-9110(又は、プッシュ回線等から#9110)
・各警察署の警察安全相談窓口