滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R４年度 No.２２
今、注目のサイバーセキュリティに関する情報をお届けします。

社長！年末商戦異常アリです！

自社の住所・企業名・責任者・連絡先などが勝手に使われていませんか？

社長：Ａ君、年末商戦真っ只中だが、わが社のＥＣサイトの売れ行きはどうかね？
Ａ君：社長！そのＥＣサイトで問題発生です！
社長：何かあったの？
Ａ君：お客様から、「お前のところのショッピングサイトで時計を注文して金を振り込んだのに、商品をまったく送ってこないやないか！」という苦情がありました。
社長：え？入金確認してないの？
Ａ君：当社では注文を受けていませんし、入金もありませんでした。そのお客様からよくよく話を聞くと、うちで扱っていない商品でした。
社長：お客様の振込先間違いじゃないの？
Ａ君：もしやと思って、お客様がアクセスしたＵＲＬや先方とやりとりされたメールの内容を伺うと、当社が使っているものと全く違うものでした。
お客様がアクセスしたWebページを見てみると、内容は当社のＥＣサイトではないですが、会社概要はまるっぽ当社のものでした。これが俗に言う「偽サイト」かと。
社長、どうしたらよいですか？
社長：うーーん、どうしよう？

１２月に入り、こういった相談が増加しています。

偽サイトの対応要領について

１．被害者(お客様)への対応
- ○ 被害者から商品を購入したサイトのＵＲＬを聞き取り、実際に確認する。
- ○ 被害者が注文したサイトは、自社とは無関係であることを説明する。
- ○ 被害者に、被害者の居住地を管轄する警察などに相談するよう依頼する。

２．自組織の対応
- ○ 自社のWebサイトに「当社を騙るショッピングサイトに注意！」などの注意喚起文を掲載する。
- ○ 偽のショッピングサイトが使用しているドメインやサーバの管理会社に、該サイトの削除を依頼する。(サーバの管理会社は、該当のＵＲＬやドメインをWhois検索すれば調べられます。)
- ○ 偽のショッピングサイトが検索サイトに表示されないように、検索サイトの運営会社に通報する。

３．警察への情報提供
- ○ 偽のショッピングサイトのＵＲＬ
- ○ 偽のショッピングサイトが代金の振込先として指定した銀行口座情報(番号や名義人など)

偽のショッピングサイトの多くは、海外に所在するサーバで運営されており、該当サイトの削除に時間を要するケースが多いため、警察では、そういったサイトのＵＲＬ情報を収集し、ブロッキング対策（偽のショッピングサイトにアクセスすると「このサイトは詐欺サイトです。」といった警告画面を表示して、利用者に注意を促す対策）に活用しています。利用者からこういった相談があれば、警察への情報提供もお願いします。

«CS情報SHIG@»偽のショッピングサイトにだまされないようにしましょう！

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）　詳細は県警webページで　→