

もはや「見た目」だけでは判別不可能

フィッシングの脅威

「🔒」と「S」が見破るポイントだ!

サイバー瓦版

岡山県警察本部
サイバー犯罪
対策課発行
086(234)0110
phi.ghitech@pref.okayama.jp

フィッシングとは、住所・氏名・電話番号・クレジットカード番号などの重要な情報が偽のメールやサイトによって盗まれるという手口です。

具体的には、金融機関などになりすました精巧な偽メールが届き「あなたのアカウントがセキュリティ上の問題で閉鎖されます。至急手続きを行ってください」と記載されています。このメールの指示に従うと、本物サイトにそっくりなフィッシング（偽）サイトが表示され、ID・パスワード・個人情報やクレジッ



本物サイトとフィッシングサイトの比較（画像の一部を加工）

トカード番号の入力を求められます。うっかり入力するとこれらの情報が盗まれ、クレジットカードの不正利用などの被害に遭うのです。

上ではアマゾン为例に挙げていますが、実際にはアップル、楽天、LINE等になりすました手口も多発しているので注意が必要です。

専門相談員 アツコの解説員



今回はフィッシングね。と言っても魚を釣る「フィッシング」じゃないわ。期待した方、ごめんなさいね。ところで、フィッシングサイトへの誘導は、メールだけではなく、掲示板やSNS等にもフィッシングサイトへ誘導するURLが貼られていることがあるのよ。どこに潜んでいるかわからないフィッシングに引っかかるからため、今回も行くわよ。専門相談員アツコのおや・く・そ・く

☆クレジットカード番号など重要な情報を入力する際には、マークや「https」と「S」がついていることを必ず確認する

☆IDやパスワードの変更は送られてきたメールで対応するのではなく、必ず、公式サイトから行う
に注意してもらいたい。マークや「S」のURLは、やり取りする情報が暗号化されているという意味なんだけど、フィッシングサイトは、この方式に対応していないことが多いから、見分けるポイントになるの。上の偽物のログイン画面にもマークはついていないでしょ。マークと「S」に普段から注目して、絶対にフィッシングに引っかからないようにしましょう。約束ですよ!

課長のつぶやき



「一段階パスワードの設置」という件名のフィッシングメールが増加しています。ひっかかってIDやパスワードを入力しないようにしてください。また、ID・パスワードの使いまわしも危険です。それにしても最近、いろいろなフィッシングメールがくるなあ…

おら東京さ行ってきただ

サイバー課の機動戦士フミフミです。先日、久しぶりの東京出張で、スマホにやられました。出張のミッションをコンプリートし、地図アプリを使って意気揚々とホテルに向かったものの、案内されたのは全く違う場所。ホテルに電話して右往左往しながら、やっとのことで何とか到着。おいしい食事にあつこうとスマホ片手に外出したところ、??

りました。すると目の前には、閉店間際のスーパーが。半額シールが貼り付けられたハンバーグ弁当（300円相当）を迷わず購入したのです。スマホの地図アプリは確かに便利ですが、GPSの誤差で自分の位置が正しく表示されないという落とし穴があるので、技術に頼りすぎはよくないと痛感しました。とほほ…。



※サイバー瓦版5月号に、平成29年中のサイバー相談のうち架空請求の件数を536件としていましたが、正しくは487件でした。お詫びして訂正します。