F－CSNET NEWS

Fukuoka small and medium sized enterprises
Cyber security Support NETwork

第３号

【作成】 福岡県警察本部
サイバー犯罪対策課

あなたの会社の情報（企業情報や大切なパスワード等）が狙われている
フィッシング詐欺に注意しましょう

現在、マイクロソフトやＡｍａｚｏｎ等の有名企業を騙った偽メールが出回っています。これは偽サイトに誘導してあなたの会社の企業情報等を入力させ、あなたの会社の資産等を盗もうとしているフィッシング詐欺です。

フィッシング詐欺とは？

実在する金融機関や企業の名前をかたり、本物そっくりの偽メール（フィッシングメール）や偽ＷｅｂサイトをＷｅｂを使いユーザーを騙して、IDやパスワード、クレジットカード番号等の情報を盗みとる詐欺のことです。

このような被害が考えられます（例）

偽サイトでインターネットバンキングのID・パスワード・暗証番号等を入力してしまった・・

⇒　口座の預金がいつの間にかカラに

⇒　手形の支払期日に資金がない！

⇒　不渡り、倒産へ・・・

お金がない？！

平成29年になって確認された手口

事例１　マイクロソフトを騙ったフィッシングメール

使用している「Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅ」のプロダクトキーが違法コピーされた可能性があると偽り、偽サイトに誘導し、個人情報やクレジットカード情報を入力させる。

※プロダクトキー・・違法コピーを防ぐためソフトのインストール時に入力を求められる購入者ごとに付される番号。

事例２　Ａｍａｚｏｎを騙ったフィッシングメール

アカウントが更新できなかったと偽り、偽サイトに誘導し、Ｅメールアドレス・パスワード、クレジットカード情報等を入力させる。

事例３　ＬＩＮＥを騙ったフィッシングメール

メールやトークで、アカウントに異常なログインがあったと偽り、偽サイトに誘導し、ＩＤやパスワードを入力させる。

被害を防ぐために。フィッシング詐欺対策の心得。

メールにあるＵＲＬに、安易に接続（クリック）しない。

金融機関（銀行、保険、カード会社等）がメールで口座番号や暗証番号等の法人・個人情報を問い合わせることはありません！該当URLを金融機関の請求書や利用者カード等で、正しいものか確認しましょう。

フィッシング詐欺については「フィッシング対策協議会」へ

フィッシング対策協議会　検索

https:// www.antiphishing.jp/

サイバー犯罪対策課のページでは「サイバー妖怪」のマンガでフィッシング詐欺の手口等を紹介しています。（フィッシング妖怪　カッパル）

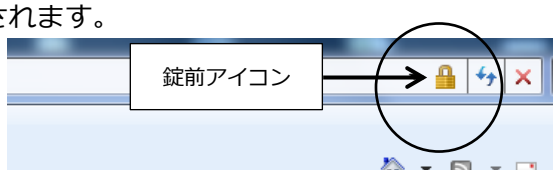
サイバー妖怪の情報はこちらへ

福岡県警察　サイバー犯罪対策課　検索

http://www.police.pref.fukuoka.jp

「錠前」マークは出ていますか？証明書の確認

重要な情報を入力する際は、入力画面を表示すると「錠前」アイコンが、画面上部のアドレスバー（URL等が表示されるバー）右側等に表示されます。



この「錠前」アイコンは暗号化通信（SSL/TLS通信）を採用していることの証明であり、アイコンをクリックすることで証明書の情報を見ることができます。証明書で証明書の発行元や該当の金融機関等の名称を確認しましょう。

（例）Ｗｅｂサイトの認証（中略）○○でこのサイトを次のように認証しました。○○ＢＡＮＫＩＮＧ　ＣＯＰＲＯＲＡＴＩＯＮ（○○銀行）・・・