

3分で分かる!

知らないうちに損する情報セキュリティ対策レポート①

インターネット倉敷の「お客様のネットワークの安全・安心を見直す運動」

「お客様のネットワークの安全・安心を見直す運動」とは…
これから増えると予測されているインターネットセキュリティ被害からお客様をお守りするために立ち上げられた、インターネット倉敷の社内プロジェクトです。
みなさまの会社の大切な情報を、巧妙な手口で攻撃してくるフリのハッカーや情報詐欺師、ウィルスなどのあらゆる脅威からお守りする有益な情報をお届けします!



被害多発① インターネットバンキングをご利用の方はフィッシング詐欺に注意!

(1) フィッシング詐欺とは??

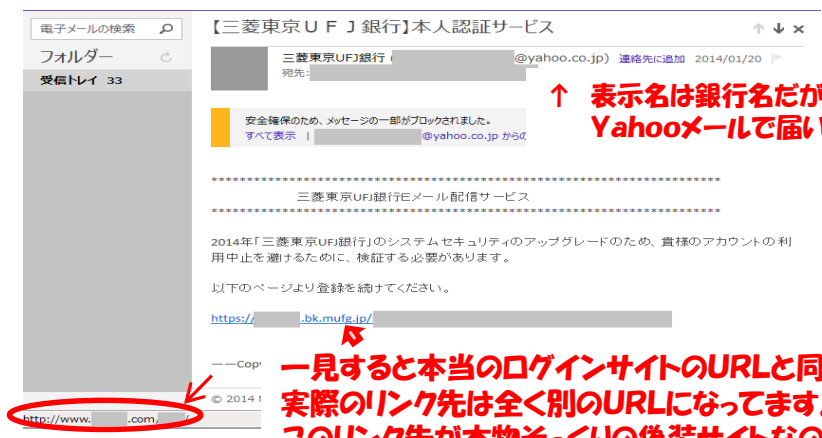
フィッシング詐欺とは、ハッカーがメールを利用して、本物そっくりにした金融機関のサイトやショッピングサイトに誘導し、パスワードやクレジットカードなどの個人情報盗み出す行為のことです。盗み出した情報は、売却して利益を得たり、あなたに成りすまして買い物やポイントを勝手に使われたり…現金を不正に送金されてしまうなどの可能性があります。

(2) 実際に届いたメールがこちらです。

表示名	件名	並べ替え
三菱東京UFJ銀行	【三菱東京UFJ銀行】本人認証サービス	2014/01/20
三菱東京UFJ銀行	【三菱東京UFJ銀行】本人認証サービス	2014/01/15
三菱東京UFJ銀行	【三菱東京UFJ銀行】本人認証サービス	2014/01/15
三菱東京UFJ銀行	【三菱東京UFJ銀行】本人認証サービス	2014/01/15

三菱東京UFJ銀行からのメールと見せかけたメールです。これらのメールは悪意のある第三者より、不特定多数に送信されています。
三菱東京UFJ銀行でも注意喚起を行っております。
<http://www.bk.mufg.jp/info/phishing/20131118.html>

開くと…



↑ 表示名は銀行名だが、Yahooメールで届いていました。

アクセスすると…

一見すると本当のログインサイトのURLと同じでしたが、実際のリンク先は全く別のURLになってます。このリンク先が本物そっくりの偽装サイトなのです。

本物そっくりの偽装サイトにアクセスしてしまい、契約者番号やパスワードを入力すると、ハッカーにその情報を盗まれてしまうのです。また、アクセスしただけで、ウィルス感染する場合もあります。会社の大切な情報やお金そのものを盗られてしまったら、大変ですよ…! 汗

(3) では、どうすればいいの?

不審なメールのリンクはクリックせず、メールを削除して下さい! でも、メールを開かないように社員全員を統制するのは難しいですよ! 実は、入口でブロックする方法があるのです! (次回に続く)