◆ 「釣り」(fishing)ではありません。「Phishing」です

今回は、現在アメリカで急激に被害が増加しており、日本でも被害の増加が懸念される「フィッシング詐欺」をご紹介します。

フィッシングと言っても、魚釣り(fishing)ではなく、「Phishing」とつづります。
フィッ シング詐欺とは、実在の銀行・クレジットカード会社やショッピングサイトなどを装ったメールを送付し、そこにリンクを貼り付けて、その銀行・ショッピング サイトにそっくりな「罠のサイト」に呼び込み、クレジットカード番号やパスワードなどを入力させてそれを入手してしまうという詐欺です。

フィッシング詐欺は現在アメリカで被害が急増しており、フィッシング型の迷惑メールが 2003 年 9 月では 279 件しかなかったのに比べ、2004 年 3 月には 21 万 5643 件にまで達したとのことです。

◆ フィッシング詐欺を防ぐためには:「ユーザ側の正しい行動」が基本

フィッ シング詐欺は、昨今流行の「オレオレ詐欺」と似たところが多くあります。電話会社がオレオレ詐欺を検知して通話遮断することができないように、フィッシン グ詐欺を自動的に遮断することは困難です。
なので、フィッシング詐欺に引っかからないためには、ユーザ一人一人が正しく行動するということが大原則となります。
以下、どのような点に注意したらよいかを見ていきましょう。

1. メールを信用しない、リンクをクリックしない
   現在のメールシステムは信頼するに足るものとは言えません。送信者を偽ることは簡単にできるし、メールアドレスさえわかってしまえば、一人の悪意ある人間が何万通でも簡単にメールを送信できてしまいます。まず「メールは信用できないもの」であると頭に叩き込んでください。

   信用できないものであるということは当然、そこに書かれているリンクを安易にクリックしてはいけないということです。

2. 不審な点があるときは、“こちらから”本物のサイトにアクセスする

   「こちらから発信して相手を確認する」のは、オレオレ詐欺の基本的な防止法です。これと同じ手段でフィッシング詐欺も防げます。
   たとえば Citibank から「口座の更新期限が迫っています」というメールが来たならば、メールのリンクをクリックするのではなく、こちらで Web ブラウザを開いてブックマークなどから Citibank のサイトにアクセスし、そのような事実があるかどうか確認してください。必要であ

ればその「本物のサイト」で準備している問い合わせ窓口に問い合わせればよいでしょう。

3. メールヘッダを確認する

「メールヘッダ」とは、すべてのメールの先頭に付加されている各種の情報です。普段メールソフトを使っているとあまり目にすることはありませんが、メールヘッダを読むと「送信者詐称」を見破ることができる可能性があります。

メールヘッダには送信者名（自称）を示す「From:」項目のほかに、経由したSMTPサーバが何であるかを示す「Received from:」という項目があります。これも詐称可能ではありますが「From:」ほど簡単ではないので、安易なスパム・ウィルスメール・フィッシングメールであれば送信者詐称を見破ることができます。

これほど送信者詐称が横行している現在、メールヘッダをチェックするやり方はぜひ知っておくべきかと思います。

まずは、メールヘッダの表示方法を抑えておきましょう。

Outlook Expressであれば、ヘッダを見たいメールを右クリックして【プロパティ】を選択し、【詳細】タブをクリックするとメールヘッダが表示されます。

ずらずらと情報が表示されますが、とりあえず一番下（一番最初のサーバと思われるもの）を確認して、「From:」に示されているドメイン名と同じかどうか比べてみればよいでしょう。

4. アドレスバーで「本物のサイト」かどうかを確認する

もし罠のサイトに誘導されてしまった場合でも、ウィンドウ上部の「アドレスバー」を見れば罠のサイトかどうか確認できます。「http: //allabout.co.jp/」にアクセスしたはずなのに、アドレスバーが「http://123.123.123.xxx/…」のような怪しいアドレスになっていたら、それは罠のサイトである可能性が大です。

ただし、アドレスバーをJavaScriptによって偽装するというより巧妙な手口も開発されています。

このIT Proで紹介されている例の場合、偽のアドレスバーには「https://～」とSSL通信をしているかのようなURLが表示されますが、ウィンドウ最下部のステータスバーにはSSL通信をしていることを示す「鍵マーク」が表示されないため、それで区別することができるとあります。いずれにせよ、このように手を込んだ手法を使うフィッシング詐欺が既に存在するということは覚えておいたほうがよいでしょう。

事例:1

VERIFIED by VISA
VISA認証サービス

VISA カード保有者のみなさまへ

VISA カードをお持ちのお客様は自動的に VISA 認証サービス プログラム** にご加入いただいております。

VISA 認証サービスでは、お客様の個人パスワードでお持ちの VISA カードのセキュリティを強化します。オンライン ストアでのお支払い手続きの際に、ATM で暗証番号を入力するのと同じようにパスワードを入力していただきます。これで、実際にお店でカードを使用するときと同じように、VISA カードをオンラインで安全に使用することができます。

サービスの中断を避けるため、できる限り早急にカード情報を確認させていただく必要があります。

たいへんお手数ですが、次のカード情報確認ページ* へのリンクをクリックしてください

https://www.visa.co.jp/verified/

お手続きは、次の手順に従ってください。
・上記のリンクをクリックして、カード情報を確認してください。
・VISA カード情報を確認して、個人パスワードを作成してください。
・これでアカウントが更新され、サービスが中断されることなく引き続きカードをご使用いただけます。

このサービスにより引き起こされるご不便に関しては、深くお詫び申し上げます。

VISA 社員一同

* ご注意: VISA カードの更新に失敗した場合、一時的にカードが使用できなくなります。
* クレジット カードを 2 枚以上お持ちの場合は、フォームを再送信してください。
* クレジット カードを 2 枚以上お持ちの場合は、カードに別々のパスワードを設定することができます。

VISA
All it takes.

このお知らせは 2004 年 10 月 30 日まで有効です。

事例:2

「入金お知らせ」メールに注意 – イーバンク銀行を騙るフィッシング詐欺

イーバンク銀行を装ったメールを使い、ログインパスワードや暗証番号などを盗もうとするフィッシング詐欺メールが確認され、イーバンク銀行が利用者に注意を促している。同銀行を装ったフィッシング詐欺メールが確認されたのは初めて。

今回のメールは、件名が「イーバンク銀行からのお知らせ[入金がありました]」となっており、テキスト形式で送信される。同銀行では、メールアドレ スを登録している利用者に対し、入金時や出金時などに通知メールを送信しているが、今回のフィッシング詐欺メールは実際に入金時に送られるメールと同じ件名が使われていた。メール内には URL が記載されており、そこにアクセスするとログイン画面が表示され、支店番号・口座番号・ログインパスワードの入力が促され、さら に「システム上の確認」と称して暗証番号を入力させようとする。メールアドレスやメール記載の URL がイー

バンク銀行のものではなかったほか、同銀行は メールからログインパスワード・暗証番号を入力させるようなことはしていないという。現在、記載された URL にはアクセスできなくなっているそうだ。