アリコン通信

Vol.26
17年2月号

有田コンピュータの目的

有田コンピュータは「IT事業を通じ地域に貢献する事」
「顧客のパソコンによる業務改善を追求し、互いに利益を創り出し発展していく事」を目的として活動しています。

フィッシング詐欺に要注意!!

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って、文中にリンクを貼りその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、それを入手するという詐欺のことです。

フィッシング詐欺の特徴

その1 「送信者詐称」を使って、信頼できるメールアドレスを装う

フィッシング詐欺のメールの多くは、送信者を詐称しています。
たとえば、銀行のサイトを偽る手口が実際にあり、「info@○○bank.com」といったアドレスから「口座の更新期限が迫っています」のような文面でメールが送られ、ついついクリックをしてしまうわけです。

その2 ウイルス対策ソフトに検出されない

フィッシング詐欺のきっかけは、ごく普通のメールからです。添付ファイルなどもありません。悪質な添付ファイル等を使わないため、ウイルス対策ソフトは何もすることもありません。
もちろん、リンク先のサイトもただのWebページですので、ウイルス対策ソフトが検出できるような「悪質なプログラム」は何もありません。

その3 必ず「クレジットカード番号」や「パスワード」を入力するように求めてくる

これがフィッシング詐欺の最終目的です。
このような情報を安易に入力するのは、やめましょう。

フィッシング詐欺を防ぐために

その1 メールを信用しない、リンクをクリックしない

一人の悪意のある人間が何万通でも簡単にメールを送信する事が出来ます。しかも、送信者を偽る事も出来てしまいます。
「メールは信用出来ないもの」であることの認識が必要です。
もちろん、メール本文中のリンクはクリックしないようにしましょう。

その2 不審な点があるときは、自分から本物のサイトにアクセスしてみる

たとえば、○○bankから「口座の更新期限が迫っていいます」というメールがきたら、メールのリンクをクリックをするのではなく、銀行のサイトにアクセスしてそのような事実があるかどうかを確認する必要があります。

その3 アドレスバーで「本物のサイト」であるか確認する

もし、罠のサイトに誘導されてしまっても、「アドレスバー」をみれば罠のサイトかどうか確認することができます。
「http://○○○.co.jp」にアクセスしたのにアドレスバーが、「http://×××.△△」全く違う怪アドレス変わっていたら要注意です。

フィッシング詐欺の被害は近年急増しています。最近流行の「オレオレ詐欺」と同じように、自動的に検知して遮断することは困難です。
フィッシング詐欺に引っかからないためには、一人一人が注意して行動するという事が大切です。

編集者より：フィッシング詐欺もウイルスメールと同様に
まずは注意するという事が、大事ではないでしょうか。（タナカ）

■有田コンピュータ ◇TEL：0955-42-5133　FAX：0955-42-5166　Mail：support@aricom.jp　HP：http://www.aricom.jp
営業時間 9：00～18：00（土・日・祝日を除く）