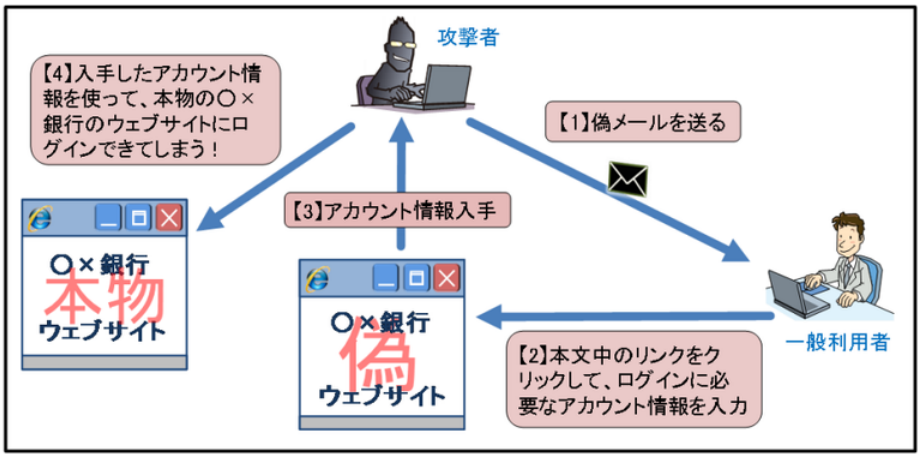
フィッシング詐欺

フィッシング（Phishing）詐欺とは、金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、受信者に偽のウェブサイトにアクセスするよう仕向け、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為のことをいいます。単にフィッシングと呼ばれることもあります。

Phishing という用語は、「餌を撒いて釣る」という類似性から、Fishing を語源として生まれた造語（同音別表記）です。f を ph に綴りを変えているのは両者を区別する（つまり異義語とする）ためです。

フィッシング詐欺被害の典型的な例は以下の通りです。（IPA 資料より引用）



【1】攻撃者が偽メールを送信
　攻撃者が、正規のウェブサービスや金融機関など実在する会社を装ったメールを無差別に送信します。
【2】利用者がメール本文中のリンクをクリック
　メール受信者が、そのメールを信用してメール本文中の URL をクリックすると、事前に用意された偽のウェブサイトに誘導されます。
【3】攻撃者がログイン情報を入手
　偽のウェブサイトと気付かずにログイン情報（ID やパスワードなど）を入力してしまうと、そのアカウント情報が攻撃者に渡ってしまいます。
【4】攻撃者が実際のウェブサイトにログイン
　攻撃者は、入手したログイン情報を使い、利用者になりすまして本物のウェブサイトにログインします。

フィッシング詐欺への対策

フィッシング攻撃者は、URL に使用される特殊な書式を利用してあたかも本物のドメインにリンクしているかのように見せたり、ポップアップウィンドウのアドレスバーを非表示にするなど、非常に巧妙な手口で攻撃を仕掛けてきます。そのため、「釣られる」被害者が続出している状況です。

そもそも金融機関などから、カード番号や暗証番号を入力するような依頼がメールで届くことはありません。そのような内容のメールであったならば、まずはフィッシング詐欺を疑いましょう。

フィッシング詐欺への対策として、最低限以下のことに留意しましょう。

・メールの真偽を確かめる
　送信者欄のメールアドレスは偽装されていることもありえます。
　差出人名称が騙られているかもしれません。
　差出人が誰であろうと、誰宛てと書かれていようと、「何をさせようとしているのか」だけに着目して、明らかにおかしいものを見つけましょう。
・メールに示されたリンク先に不用意にアクセスしない
　正規のサイトの URL と似たような URL の偽サイトかもしれません。
　金融機関などの場合は信頼できる方法（当該機関からの書類や、ネットでの検索）で正規サイトの URL を捉え、メール中の URL とドメインが同じであることを確認しましょう。
・メールに示された電話番号に不用意に電話をかけない
　偽サイトに誘導するのではなく、偽の電話番号に電話させるというフィッシング詐欺事例もあります。
　覚えのない電話番号にはできるだけ電話しない方が安全です。
　金融機関などの場合は信頼できる方法（当該機関からの書類や、ネットでの検索）で、電話番号が正規のものかどうか確認しましょう。

スピアフィッシング

スピアフィッシング（Spear Phishing）詐欺とは、特定の個人や団体を狙うフィッシング詐欺のことで、相手の素性を調べた上で、関係者を装うなど、ターゲットに合わせた手口で仕掛けてくるのが特徴です。
素潜りで銛（モリ）や水中銃で魚を突き刺す釣り方の Spear Fishing が語源です。

特定の個人や団体を狙ってフィッシングを仕掛けたり、ウィルスを送り込む攻撃を総称して、スピア型攻撃（標的型攻撃）といいますが、スピア型という表現の由来はこのスピアフィッシングです。

典型的なフィッシング詐欺が不特定多数のアドレスに同じ内容のメールを送り付けるのに対して、スピアフィッシングでは、攻撃相手のことをよく研究し、ごく自然に感じられる件名や本文、添付ファイル名などが付されています。そのため詐欺メールだと見分けにくく、日常業務をこなす意識で添付ファイルを開いたり、リンク先の URL をクリックしたりしてしまう危険性がより高いのです。

例えば、大企業の支店に勤務する社員に「本社の情報システム部の者だが調査に必要なのであなたのパスワードを教えてほしい」といったメールを送り、だまされた社員から聞き出したパスワードを使ってその企業のネットワークに不正侵入するといった手が使われた事例があります。他にも、上司や取引先に成りすまして業務上の機密情報や知的財産を詐取するといった事例が報告されています。

2015 年 5 月に発生した日本年金機構の 125 万件の個人情報漏洩事件は、特定の団体にウィルスを送り付けてくるスピア型攻撃によるものでした。学術機関の職員を装った電子メールに、セミナーの案内状と称したウィルス付きの文書ファイルが添付されており、これを開封した少なくとも 2 人の機構職員の端末が感染したことが発端とのことです。

ファーミング詐欺

ファーミング（Pharming）詐欺とは、ユーザーに気づかれないように、有名な金融機関やオンラインショップのサイトをそっくりに真似た偽の Web サイトに誘導し、不正に暗証番号やカード番号などを含む個人情報を得ようとする、ネット詐欺の手口のひとつで、フィッシング詐欺の進化型とも言われています。

フィッシング詐欺は偽の案内メールなどでユーザーを「一本釣り」にする手法ですが、ファーミング詐欺はユーザーが正しい URL を入力して正規のサイトにアクセスしようとした時に、DNS サーバの情報を不正に書き換えるなどの方法によって、ユーザーに気づかれずに偽のサイトに誘導するものです。

ユーザーを丸ごと偽サイトに誘導する手口は大規模農業を連想させるので、Farming をもじって Pharming と名付けられました。

ファーミング詐欺は、ユーザーの自発的な行動を利用するので、ユーザーが警戒心を抱きにくいという特徴があります。偽サイトが良くできているものであった場合には、一般の人にはなかなか詐欺だと見分けにくく、効果的な対処方法はいまのところありません。それ故、ファーミング詐欺はステルス型フィッシング詐欺とも呼ばれています。ステルス（Stealth）とは隠密とか、こっそりと行うことという意味です。