オンライン上での識別情報の盗難：
フィッシングの技術、難点、および対抗策

(Online Identity Theft: Technology, Chokepoints and Countermeasures)

Radix Labs
アーロン・エイミー（Aaron Emigh）
ate@radixlabs.com

2005年10月3日

謝辞

本書への財政援助について、国土安全保障省の科学技術部門（DHS S&T）に感謝する。本書に含まれる見解は著者のものであり、必ずしも国土安全保障省または科学技術部門の公式な姿勢を示すものではない。本報告書の内容は、DHS S&T、SRI International、Anti-Phishing Working Group（APWG）、民間産業などの官民の連携によるIdentity Theft Technology Councilのメンバーによってまとめられた。本書に貢献いただいたDan Boneh氏、Drew Dean氏、Louie Gasparini氏、Ulf Lindqvist氏、John Mitchell氏、Peter Neumann氏、Robert Rodriguez氏、Jim Roskind氏、Don Wilborn氏に特に感謝の意を表明する。

対象とする読者

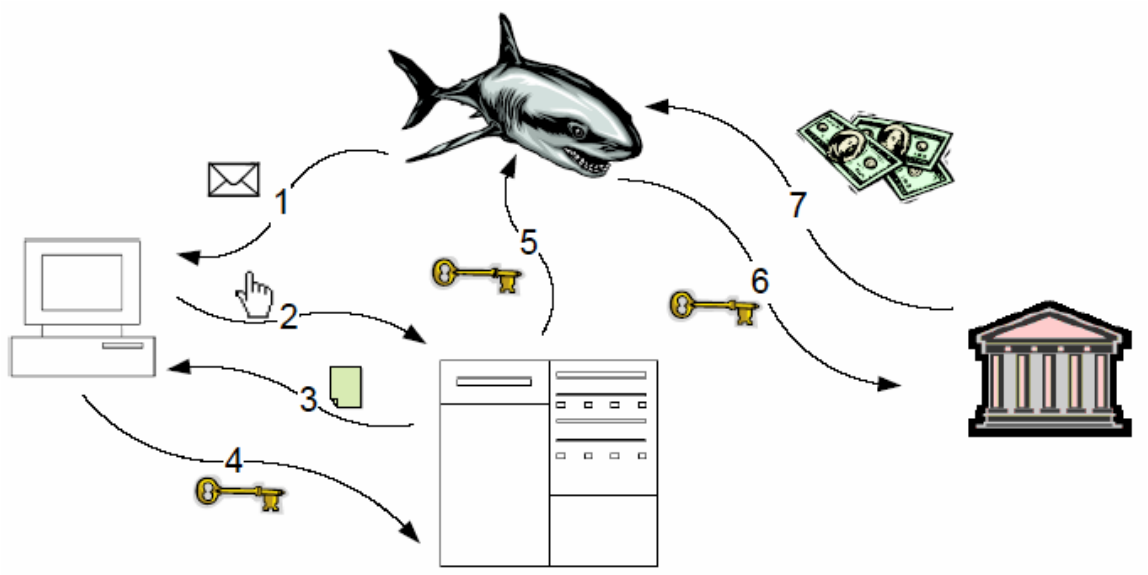
本報告書は、セキュリティ担当者、エグゼクティブ、研究者、オンライン上での識別情報の盗難者が使用する手法やそのような犯罪を防ぐための対抗策を理解したい人々など、技術に精通した読者を対象としている。

要旨

フィッシングとは、オンライン上での識別情報の盗難によって個人の機密情報が取得されることである。フィッシングには、不正なメッセージによってユーザを騙し、情報を提供させる詐欺攻撃、悪質なソフトウェアがデータの漏洩を招くマルウェア攻撃、ホスト名のルックアップを変更し、不正サーバにユーザを導くDNSベース攻撃などがある。

ガートナー・グループでは、米国の銀行およびクレジットカード発行会社でのフィッシング関連の直接的な損失は、2003年には12億ドルだったと推定している。間接的な損失はこれよりもはるかに大きく、顧客サービス費用、口座の書き換えコスト、さらにはオンラインでの金融取引の安全性に対する不安の広まりによる、オンライン・サービスの使用の減少を原因とする費用の増加などが生じている。不正な活動によって傷つけられた信用の修復は困難なため、フィッシングは被害に遭った消費者にもかなりの苦難をもたらす。

本報告書では、あらゆるタイプのフィッシング攻撃における情報の流れを検証する。フィッシャーが使用する技術とともに、適用できる対抗策についても説明する。フィッシングを防ぐために導入できる技術に主に注目する。現在利用可能な対抗策と研究段階にある技術の両方を紹介する。



フィッシング攻撃のステップ

フィッシング攻撃は、いずれも同じ一般的な情報の流れに従っている。流れの各ステップにおいて、異なる対抗策の適用により、フィッシングを防ぐことができる。ステップは次の通りである。

0. フィッシャーが攻撃の準備をする。ステップ0の対抗策としては、フィッシング攻撃を開始前に検出するための、悪意のある活動の監視などがある。
1. 悪質なペイロードが何らかの伝搬媒介(ベクトル)を通じて届く。ステップ1の対抗策は、フィッシング・メッセージまたはセキュリティの弱点への攻撃が届くのを防ぐことである。
2. 情報漏洩に対し脆弱となるような行動をユーザがとる。ステップ2の対抗策では、フィッシング戦術を検出し、フィッシング・メッセージをより騙されにくいものにする。
3. ユーザが、リモートWebサイトまたはローカルでWeb上のトロイの木馬によって機密情報を要求される。ステップ3の対抗策では、フィッシング内容がユーザに届くのを防ぐことに重点を置く。
4. ユーザが機密情報を漏洩する。ステップ4の対抗策では、情報の漏洩を防ぐことに集中する。
5. 機密情報がフィッシング・サーバからフィッシャーに送信される。ステップ5の対抗策では、情報の送信を追跡する。
6. 機密情報がユーザになりすますために使われる。ステップ6の対抗策では、情報をフィッシャーにとって役に立たないものにすることに重点を置く。
7. フィッシャーが漏洩情報を使用して不正行為を行う。ステップ7の対抗策では、フィッシャーが金銭を受け取るのを防ぐことに重点を置く。

フィッシングは、社会的要因だけでなく技術も関与する複雑な現象である。すべてのフィッシングを防げるような単一の「特効薬」はない。しかし、技術を適切に適用すれば、識別情報の盗難のリスクを大幅に軽減できる。このような技術を適用する機会は多数ある。たとえば次のようなものである。

- Webサイトの使用やドメイン登録など、悪質な可能性のある活動を監視し、フィッシング攻撃を開始前に検出してフィッシャーの準備を妨害する（ステップ0）。
- 非認証メッセージを廃棄できるよう、電子メール・メッセージの認証を行う（ステップ1）。
- 商標、ロゴ、およびその他の専有画像の不正使用を検出する（ステップ1）。

- マルウェアへの耐性を強化するために、セキュリティ・パッチのインフラストラクチャーを改善する（ステップ1）。
- 個人情報を使用し、ユーザに対して電子メールの認証を直接行う（ステップ2）。
- 不正なWebサイトを検出し、ユーザに警告する（ステップ4）。
- 相互認証プロトコルを使用する（ステップ4）。
- 情報が対象とする受信者によってのみ使われるよう、ユーザとWebサイトの間に信頼できるパスを確立する（ステップ4および6）。
- 二要素認証を使用する（ステップ6）。
- パスワードをサイト別にするよう強制する（ステップ6）。
- 公開鍵暗号を使用して証明書をエンコードし、妥当性に制限を設ける（ステップ6）。

はじめに

フィッシングとは、オンライン上での識別情報の盗難によって個人の機密情報が取得されることである。カード・スキミングや「ダンプスター・ダイビング（ゴミ箱漁り）」などのオフラインでの識別情報の盗難や、多数の個人の情報が一度に取得されるような大規模なデータ漏洩とは区別される。フィッシングには、次のようにいくつものタイプの攻撃がある。

- 不正なメッセージによってユーザを騙し、情報を提供させる詐欺攻撃
- 悪質なソフトウェアによりデータの漏洩を招くマルウェア攻撃
- ホスト名のルックアップを変更し、不正サーバにユーザを導くDNSベース攻撃

フィッシングでは、ユーザ名とパスワード、ソーシャル・セキュリティ・ナンバー、クレジット・カード番号、銀行口座番号、さらには誕生日や母親の旧姓をはじめとする個人情報など、さまざまな機密情報が狙われる。
ガートナー・グループでは、米国の銀行およびクレジット・カード発行会社でのフィッシング関連の直接的な損失は、2003年には12億ドルだったと推定している。間接的な損失はこれよりもはるかに大きく、顧客サービス費用、口座の書き換えコスト、さらにはオンラインでの金融取引の安全性に対する不安の広まりによる、オンライン・サービスの使用の減少を原因とする費用の増加などが生じている。不正な活動によって傷つけられた信用の修復は困難なため、フィッシングは被害に遭った消費者にもかなりの苦難をもたらす。
フィッシング攻撃の頻度とその巧妙さは、いずれも劇的に向上している。最近のフィッシング攻撃や関連統計については、http://www.antiphishing.orgで紹介されている。
フィッシングは複数の国に及ぶことが多く、組織犯罪として行われるのが一般的である。影響を受ける機関は法的措置の追求が可能であり、追求をすべきだが、長期的な解決策においてはフィッシングを防ぐための技術的な措置が不可欠な要素となる。
本報告書ではフィッシャーが使用する技術を検証し、技術的な対抗策について市販のものと提案段階のものの両方を評価する。

フィッシング攻撃のタイプ

フィッシングはさまざまな方法で行われる。フィッシャーは技術的に革新的であり、技術に投資する余裕がある。フィッシャーが素人であるという考えは、よくある誤解である。専門的な組織犯罪として行われるような、最も危険なフィッシング攻撃にはこれは当てはまらない。金融機関がオンライン上での存在感を増すのに伴い、口座情報の漏洩の経済的価値は劇的に拡大してきた。フィッシャーなどの犯罪者は、犯罪によって不法に得た利益に比例して技術への投資が可能になっている。
現在のフィッシング攻撃の巧妙さと急速な発展を考えると、フィッシャーが採用する技術の包括的な目録作りは不可能である。以下では、いくつかのタイプの攻撃について説明する。攻撃のタイプ間の区別は明確なものではない。フィッシング攻撃の多くは複数の技術を採用したハイブリッド攻撃だからである。たとえば、フィッシン

グ目的の詐欺電子メールでは、コンテンツインジェクションを受けたサイトにユーザを誘導し、そこでユーザのhostsファイルを攻撃するマルウェアをインストールする。その後正規のWebサイトにアクセスしようとするとフィッシング・サイトに転送され、中間者攻撃によって機密情報が漏洩される。

詐欺フィッシング

「フィッシング」という用語は、インスタント・メッセージによるAOLのアカウントの盗難が起源だが、今日最も一般的な詐欺フィッシングの媒介は電子メールである。代表的なシナリオでは、フィッシャーは受信者にリンクをクリックするよう求める「行動要請」の詐欺電子メールを大量に送信する。「行動要請」の例としては、次のようなものがある。

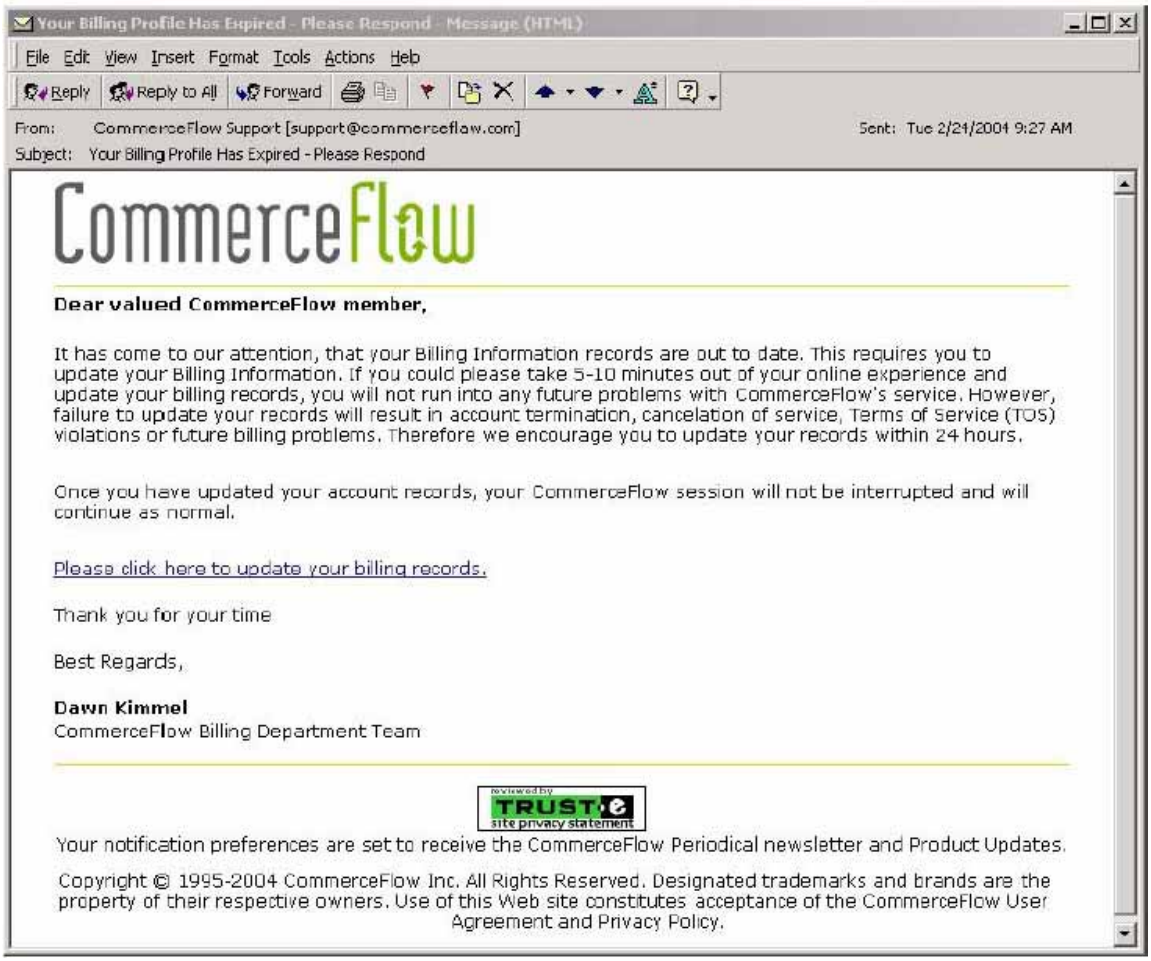
- 金融機関またはその他のビジネスにおいて受信者の口座に問題があるというメッセージ。電子メールでは、電子メール内の詐欺リンクを使用してWebサイトにアクセスし、問題を解決するよう受信者に求める。
- 受信者の口座が危険にさらされているとし、受信者に詐欺防止プログラムへの加入を勧めるメッセージ。
- 受信者が注文していない架空の商品（不快感を与えるような商品が多い）に関する請求書と、その偽の注文を「取り消す」ためのリンク。
- ユーザのアカウントへの好ましくない変更が行われたことを知らせる不正な通知と、その不正な変更に「異議を唱える」ためのリンク。
- 金融機関で新しいサービスが導入され、既存のメンバーである受信者に対し期間限定でサービスを無料で提供するという知らせ。

いずれの場合も、ユーザが誘導される先のWebサイトでユーザの機密情報が集められる。受信者が不正なWebサイトに機密情報を入力すると、フィッシャーは後に被害者になりすまして被害者の口座からの送金、商品の購入、被害者の住宅に対する2つ目のローンの申し込み、失業手当の申請などを被害者の名前で行ったり、その他の被害を及ぼす。

多くの場合、フィッシャーは経済的な損害を直接生じさせるのではなく、不法に取得した情報を二次市場に転売する。犯罪者たちは、このような情報が売買されるさまざまなオンライン・ブローカリング・フォーラムやチャット・チャネルに参加している。

詐欺ベースのフィッシング方式には多種多様なものがある。HTMLで電子メールを受信している人にはログイン・ページの複製を直接電子メールで提供できるため、リンクをクリックし、ユーザのWebブラウザーを起動する必要がない。

フィッシング・サイトへのリンクでは、ホスト名の代わりに数字のIPアドレスが使われる場合がある。そのような場合、Javascriptによってブラウザーのアドレスバーに取って代わったり、その他の方法で正規のサイトと通信しているとユーザを信じさせることが可能である。*類似ドメイン攻撃(cousin domain attack)*では、正規のドメイン・ネームと一見同じに見えるような、フィッシャーによって制御されたドメイン・ネームを使用するため、このような複雑さを回避できる。たとえば、www.commerceflow.comの代わりにwww.commerceflowsecurity.comが使われる。ユーザが悪質なサイトを訪問すると、最初の詐欺ベースのメッセージが、マルウェアのインストールへと発展することもある。



代表的な詐欺フィッシング・メッセージ

マルウェア・ベース・フィッシング

マルウェア・ベース・フィッシングとは、一般的に、ユーザのマシン上で悪質なソフトウェアを実行するあらゆるタイプのフィッシングを意味する。マルウェア・ベース・フィッシングにはいくつもの形のものがある。最も蔓延しているものを以下で紹介する。

一般的に、マルウェアはソーシャル・エンジニアリングまたはセキュリティの脆弱性の悪用のいずれかによって広まる。ソーシャル・エンジニアリング攻撃の典型的なものでは、電子メールの添付を開いたりファイルをWebサイトからダウンロードするようユーザを説得し、添付がポルノ、有名人のわいせつな写真や噂話などに関するものだとする場合が多い。ダウンロード可能なソフトウェアにもマルウェアを含むものがある。マルウェアは、セキュリティの脆弱性につけ込んでマルウェアをインストールするワームまたはウィルスの伝搬、またはセキュリティの脆弱性につけ込んだWebサイトからのマルウェアの提供のいずれかのセキュリティ攻撃によって広まることもある。サイト上に何らかの魅力的なコンテンツがあることを約束するスパム・メッセージなどのソーシャル・エンジニアリングや、クロスサイトスクリプティング脆弱性などのサイト上のセキュリティの弱点につけ込み悪質なコンテンツを正規のWebサイトに注入することなどによって、トラフィックが悪質なWebサイトに導かれることもある。

キーロガーとスクリーンロガー

キーロガーとは、自らをWebブラウザーにインストール、またはデバイス・ドライバーとしてインストールし、入力されたデータを監視して関連データをフィッシング・サーバに送信するプログラムである。キーロガーではいくつかの異なる技術が使われ、次のようなさまざまな方法で実装される。

- URLの変化を検出し、URLが指定された認証情報収集サイトになった際に情報をログに記録するブラウザーのヘルパー・オブジェクト
- キーボードとマウスからの入力とともにユーザの活動を監視するデバイス・ドライバー
- ユーザの入力と画面の両方を監視し、他のオンスクリーン入力セキュリティ対策を阻止する*スクリーンロガー*

キーロガーは、さまざまなサイトの認証情報を収集できる。キーロガーは通常、ユーザの位置を監視し、特定のサイトの認証情報のみを送信するようパッケージ化されている。金融機関、情報ポータル、企業のVPNなど、何百ものサイトが標的とされていることが多い。キーロガーの被害を受けた後には、さまざまな二次的被害が生じる可能性がある。実際に起きた例として、ポルノのスパムによってキーロガーが広まり、ある信用調査機関が巻き込まれたことで、この機関にアクセスできる50のアカウントが被害に遭い、それにより最終的に310,000組を超す個人情報が信用調査機関のデータベースから漏洩した。

セッション・ハイジャッカー

セッション・ハイジャッキングとは、主として悪質なブラウザー・コンポーネントによってユーザの活動が監視される攻撃である。ユーザが自らのアカウントにログインもしくは取引を開始すると、ユーザが正当に認証を確立した段階で悪質なソフトウェアがセッションを「ハイジャック」し、悪質な行為を行う。

セッション・ハイジャッキングは、マルウェアによってユーザのローカル・コンピュータで行われることもあれば、後に説明する中間者攻撃の一環としてリモートで行われることもある。マルウェアによってローカルに行われる場合、ユーザの自宅のコンピュータから開始されるため、セッション・ハイジャッキングは標的サイトからは正規ユーザとの対話とまったく同じに見える。

Web上のトロイの木馬

Web上のトロイの木馬は、認証情報を集めるためにログイン画面でポップアップする悪質なプログラムである。ユーザはWebサイトに情報を入力していると信じているが、実際には情報はローカルに入力され、フィッシャーに送信されて悪用される。

Hostsファイル・ポイゾニング

ユーザがURLバーにwww.company.comとタイプするか、またはブックマークを使用した場合、ユーザのコンピュータはサイトを訪問する前にそのアドレスを数値アドレスに変換する必要がある。Windowsなどの多くのオペレーティング・システムには、DNS（ドメイン・ネーム・システム）ルックアップを実行する前にホスト名をルックアップするためのショートカット用の「hosts」ファイルがある。このファイルを変更すれば、www.company.comが悪質なアドレスを参照するようにできる。ユーザがそこにアクセスすると正規のようなサイトが表示され、ユーザは機密情報を入力し、その情報は実際には意図した正規のサイトではなくフィッシャーに送られる。

システム再構成攻撃

システム再構成攻撃は、ユーザのコンピュータ上での設定を変更し、情報を漏洩させる。

あるタイプのシステム再構成攻撃では、ユーザのDNSサーバを変更し、下記のように誤ったDNS情報をユーザに提供する。

また別のタイプのシステム再構成攻撃では、Webプロキシーをインストールし、それを通じてユーザのトラフィックを受け渡す。これは別途説明する中間者攻撃の一種である。

データの盗難
悪質なコードがユーザのコンピュータ上で実行されると、コンピュータに保管されている機密情報を直接盗めるようになる。このような情報には、パスワード、ソフトウェアのライセンスキー、重要な電子メール、被害者のコンピュータに保管されているその他のあらゆるデータなどが含まれる。ソーシャル・セキュリティ・ナンバーなどのようにあるパターンに当てはまる情報を探すためにデータを自動的にフィルタにかけることで、かなりの量のセンシティブな情報を取得できる。パーソナル・コンピュータにはより厳重に保護された企業用コンピュータに保管されているのと同じ機密情報が存在することが多いため、データの盗難は、企業スパイ活動を目的としたフィッシングにも広く使われている。雇われスパイに加え、機密メモまたは設計文書が公に漏洩し、経済的損害が生じたりきまりが悪くなることもある。

DNSベース・フィッシング（ファーミング）

DNSベース・フィッシングとは、ここではドメイン・ネームのルックアップ・プロセスの完全性を妨害するあらゆる形のフィッシングを意味するものとして使用する。hostsファイルは正しくはドメイン・ネーム・システムには含まれないものの、これにはhostsファイル・ポイゾニングも含まれる。hostsファイル・ポイゾニングはユーザのコンピュータ上のファイルを変更するものであるため、マルウェアのセクションで説明している。

もう1つのDNSベース・フィッシングの形として、ユーザを間違った位置に誘導するために使用する間違った情報による、ユーザのDNSキャッシュの汚染がある。ユーザのDNSキャッシュの構成が誤っている場合、これは直接行うことができる。また、正規のDNSサーバをハッキングし、ユーザのDNSサーバを不正サーバに変更するシステム再構成攻撃、または構成が誤っている正規のDNSサーバのキャッシュの汚染によって行うこともできる。

コンテンツインジェクションフィッシング

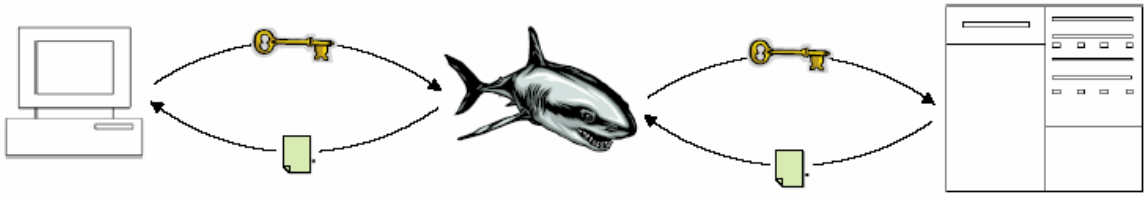
コンテンツインジェクションフィッシングとは、悪質なコンテンツを正規のサイトに注入することである。悪質なコンテンツは、他のサイトへの転送、ユーザのコンピュータへのマルウェアのインストール、またはフィッシング・サーバへのデータの転送を行うコンテンツのフレームの挿入を行う。
コンテンツインジェクションフィッシングには主に3つのタイプのものがあり、それぞれさまざまなものがある。

- ハッカーがセキュリティの脆弱性を通じてサーバを襲い、正規のコンテンツを悪質なコンテンツで置き換えまたは増補する。
- クロスサイトスクリプティング脆弱性を通じて悪質なコンテンツを挿入する。クロスサイトスクリプティング脆弱性とは、ブログ、電子商取引サイトの商品に関するユーザのレビュー、オークション、掲示板のメッセージ、検索語、Webベースの電子メールなどの外部ソースからのコンテンツに関するプログラミングの弱点のことである。このような外部から提供されるコンテンツは、悪質なスクリプトであったり、サイトのサーバでソフトウェアによって適切にフィルタで除去されていないその他のコンテンツであり、サイトの訪問者のWebブラウザー上で実行される。
- SQLインジェクション脆弱性を通じてサイトで悪質な行為が行われる。データベース・コマンドをリモート・サーバで実行し、情報漏洩を起こす方法である。クロスサイトスクリプティング脆弱性と同様に、SQLインジェクション脆弱性も不適切なフィルタリングによるものである。

クロスサイトスクリプティングとSQLインジェクションは、2つの異なる基本伝搬媒介を通じて伝搬する。1つの伝搬媒介では、悪質なコンテンツが、オークションのリスト、商品のレビュー、Webベースの電子メールなど、正規のWebサーバに保管されたデータへと注入される。もう1つの伝搬媒介では、ユーザがリンクをクリックした際に訪問するURLに悪質なコンテンツが埋め込まれる。これは、画面に表示されるURL、または検索関数の引数などのデータベース・クエリーの一部として使われるURLである場合が多い。

中間者フィッシング

中間者攻撃とは、フィッシャーがユーザと正規のサイトとの間に身を置くフィッシングの形式のことである。正規のサイトのためのメッセージは代わりにフィッシャーに送られ、フィッシャーは価値のある情報を保存してメッセージを正規のサイトに送り、応答をユーザに転送する。中間者攻撃は、漏洩させた認証情報を保管し、もしくは保管せずに、セッション・ハイジャッキングにも使用できる。中間者攻撃では、サイトは適切に機能し、何らかの問題があることを示す外的兆候がないこともあるため、ユーザに検出されにくい。



中間者攻撃

中間者攻撃はさまざまなタイプのフィッシングによって行われる。プロキシー攻撃などの一部のフィッシングの形式は本質的に中間者攻撃である。しかし、中間者攻撃は、DNSベース・フィッシング、詐欺ベース・フィッシングなど、この他の多くのタイプのフィッシングにも使われる。

通常、SSL Webトラフィックは中間者に対し脆弱ではない。SSLで使われるハンドシェークにより、サーバの証明書に記載された相手とセッションが確立され、攻撃者はセッション鍵を取得できない。また、SSLトラフィックはセッション鍵を使用して暗号化されるため、盗聴者にデコードされることもない。プロキシーはこのような暗号化されたトラフィックをトンネリングできる状態になっている。しかし、マルウェア・ベース攻撃によって新しい信頼された証明書をインストールするようシステム構成が変更されることもあり、その場合、中間者はあらゆるSSLで保護されたサイト用に独自に証明書を作成し、トラフィックを復号して機密情報を抽出し、反対側との通信のためにトラフィックを再度暗号化できる。実際には、ユーザはSSLの存在を確認しないことが多いため、中間者攻撃ではSSLをまったく使用しない。

中間者攻撃は、ハードウェア・デバイスによって生成されるワンタイム・パスコードまたは時変化パスコードなどの認証証明書を漏洩させることもある。このような盗まれた認証情報は、有効である限りフィッシャーによって認証に使われる可能性がある。

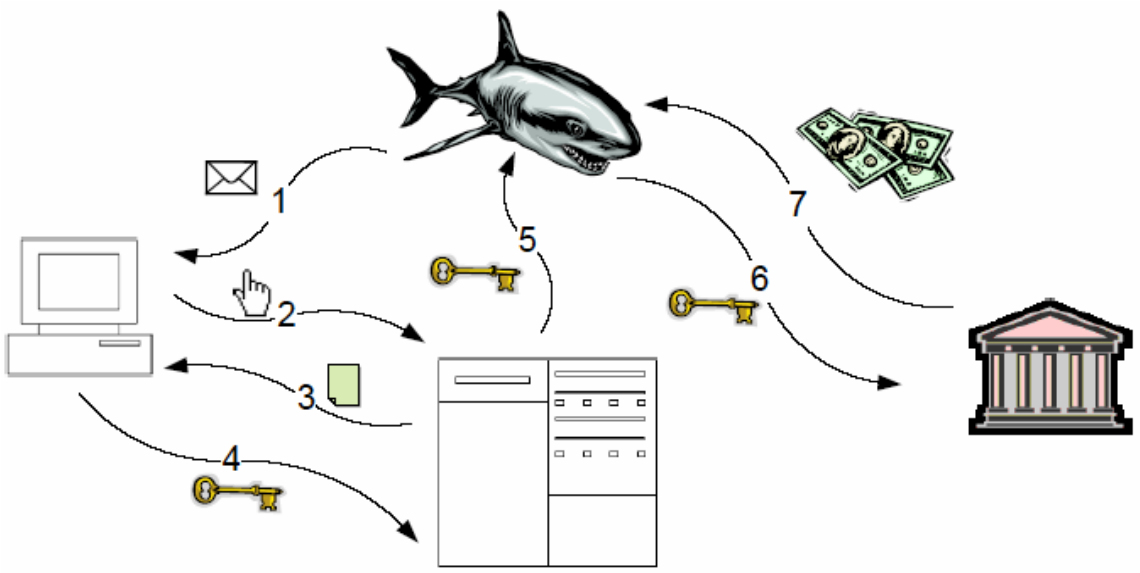
サーチエンジン・フィッシング

フィッシャーによるもう1つのアプローチとして、偽の商品のWebページを作成し、サーチエンジンにおいてそのページを索引付けし、ユーザが注文、登録、または残高の移動などの一環として機密情報を入力するのを待つ方法がある。このようなページでは、やや魅力的すぎる価格で商品を提供していることが多い。

とりわけ偽銀行による詐欺が拡大している。フィッシャーは、実在するどの銀行よりもやや高めの金利を宣伝するページを作成する。被害者たちはサーチエンジン経由でこのオンライン・バンクを発見し、新しい「口座」への「残高の移動」のために自らの銀行口座の認証情報を入力する。欲とは判断力を曇らせる強力な原動力である。「コロラド州ベッドロック」の「フリントストーン・ナショナル・バンク」にさえ銀行の口座番号を提供した被害者もいる。

技術、難点、および対抗策

技術の適用によって、フィッシング攻撃を複数の段階で防ぐことができる。技術的な対抗策については、フィッシング攻撃における下記の情報の流れの中でのステップを基準に説明する。



フィッシング攻撃のステップ

上の図でのフィッシング攻撃における情報の基本的な流れの各ステップは次の通りである。

0. フィッシャーが攻撃の準備をする。類似ドメインを使用した詐欺攻撃などでは、ドメインの登録が必要である。フィッシング・サーバが、フィッシャーが所有するものとして、または（より一般的には）ハッキングまたはマルウェアの被害に遭ったコンピュータが所有するものとして確立される。フィッシング・サーバは、Webベースのインターフェイスによってユーザから、または被害者のコンピュータのマルウェアから情報を受け取るよう構成される。
1. 悪質なペイロードが何らかの伝搬媒介を通じて届く。詐欺ベース・フィッシング攻撃では、ペイロードとは、通常、詐欺電子メールである。マルウェアまたはシステム再構成攻撃では、電子メールの添付、ダウンロードしたソフトウェアの意図せぬコンポーネント、またはセキュリティの脆弱性に対する攻撃によって届く悪質なコードがペイロードになる。DNSポイゾニング攻撃の場合、ペイロードは虚偽のIPアドレス情報である。サーチエンジン・フィッシングの場合、ペイロードは、不正なサイトを参照した検索結果である。クロスサイトスクリプティング攻撃の場合、ペイロードは、攻撃の詳細次第で、正規のサーバに保管される悪質なコードまたは電子メール内のURLに埋め込まれている悪質なコードのいずれかになる。
2. 情報漏洩に対し脆弱となるような行動をユーザがとる。詐欺ベース・フィッシング攻撃では、ユーザがリンクをクリックする。キーロガー攻撃では、ユーザは正規のWebサイトを訪問する。ホスト名のルックアップ攻撃では、ユーザは不正なサイトへと迂回する正規の名前のサイトを訪問する。
3. ユーザが、リモートWebサイトまたはローカルでWeb上のトロイの木馬によって機密情報を要求される。プロンプトを送信するリモートWebサイトは、正規のサイト（キーロガー攻撃の場合）、または悪質なサイト（詐欺ベース攻撃またはDNS攻撃の場合）、または悪質なコードを提供する正規のWebサイト（コンテンツインジェクション攻撃の場合）である。
4. ユーザが、認証情報などの機密情報を、悪質なサーバ、ローカルに実行されている悪質なソフトウェア、または正規の対話を盗聴しているソフトウェアに提供することで漏洩する。
5. 機密情報がフィッシャーに送信される。攻撃の性質次第で、この情報は悪質なサーバまたは被害に遭ったサーバ経由で送信され、キーロガーやWeb上のトロイの木馬などのローカルに実行されているマルウェアの場合は、情報は被害者のPCから送られることもある。
6. 機密情報がユーザになりすますために使われる。
7. 詐欺グループが機密情報を使用して不法な金銭収入を得る、またはその他の方法で詐欺行為を行う。

フィッシングの情報の流れの各ステップについて検証する。各ステップでは、その時点でフィッシングを防ぐために採用できる技術的な対抗策を評価する。

ステップ0：フィッシング攻撃を開始前に防ぐ

場合によっては、フィッシング攻撃を発生前に検出できることもある。また、企業は危機的状況に陥らないうちにフィッシング攻撃への対策を整えることで、対応を改善し、損失を軽減できる。

差し迫った攻撃の検出

類似ドメインを使用した詐欺攻撃などの何らかのフィッシング攻撃を実施するには、フィッシャーはフィッシング・データを受け取るためのドメインを設定する必要がある。考えられるなりすまし・ドメイン・ネームを対象に先制的にドメイン登録を行えば、最も騙されやすい名前のドメインの空きを減らすこともできる。

考えられるスプーフィング・ドメインは何百万もある可能性があるため、公式なものに見えるドメインとして考えられるものをすべて登録するのは現実的ではない。スプーフ・ドメインの可能性のあるものの登録を検出し、登録者に対処すると同時にサイトでの活動を監視する登録監視サービスを提供する企業もある。

新規のドメイン登録に「保留期間」を設け、付与される前に商標保持者が新規登録に反対できるようにするという案もあった。これは類似ドメインの問題には役立つかもしれないが、フィッシャーがサイトでなりすましができることへの対策にはならない。

フィッシング・サーバを設定する際には、なりすましの対象となる正規のサイトのコピーを保存する場合が多い。正規のサイトのWebログでアクセス・パターンを分析し、フィッシャーのダウンロード活動を検出できることもある。公開Webサイトのページは最終的にはフィッシャーから遠ざけておくことはできないものの、これは攻撃への応答のリードタイムを生み、使われているIPアドレスに基づき早くから分析をしておくことで、攻撃が始まったときに捜査を迅速化できる場合もある。

「ライブ」状態に移る前に、Webを検索して新しいフィッシング・サイトを特定しようと試みるサービスもある。このようなサービスでは、フィッシング・サイトをアクティブになる前に閉鎖することになる場合が多い。しかし、多くの場合、フィッシング・サイトは検索スパイダーからはアクセスできず、収益のほとんどを運用開始の初期に得られるため、長期間アクティブである必要はない。フィッシング・サイトがアクティブである期間は平均で2日以内であり、数時間のみのことも多いにもかかわらず、それでも多大な収益を獲得するのに十分である。

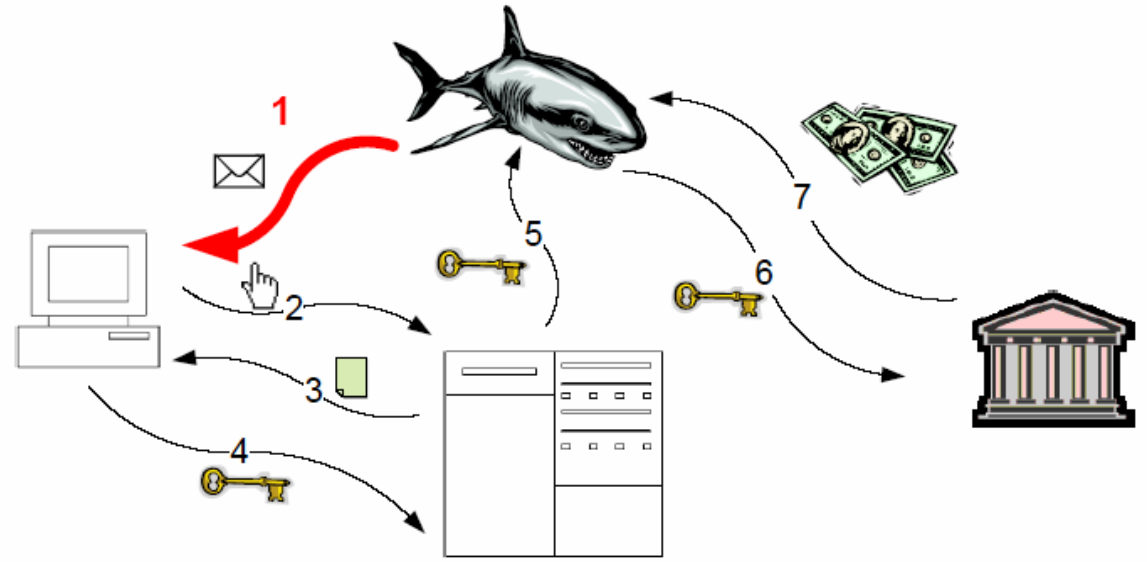
フィッシャーは、フィッシング・サーバをより長期間オンラインにしておくためにさまざまな技術を導入してきた。たとえば、フィッシャーが所有するドメインを使用したフィッシングは、フィッシング・ドメインのDNSサーバで情報を更新することで任意のIPアドレスに誘導できる。フィッシャーはカスタムDNSサーバをセットアップし、それらを交替で使用し、攻撃した多くのマシンにラウンドロビン方式でIPアドレスを提供してきた。あるフィッシング・サーバが撤去されると、そのサーバはローテーションから外され、別の攻撃したマシンが追加される。DNSサーバが撤去されると、登録情報が変更され、別のものと置き換えられる。そのため、ドメインの登録機関を通じて撤去する必要があり、ISPを通じてマシンを撤去するよりも厄介で時間のかかる作業になることがある。一部のフィッシャーは、被害者が回される先の攻撃済みのマシンにロード・バランサーとして機能するようポート・リダイレクターをセットアップし、フィッシング・サーバを撤去と同時に置き換えられるようにしている。

攻撃に備える

フィッシングの標的になる可能性の高い組織は、攻撃が発生する前に攻撃に備えることができる。このような準備によって、攻撃に対する組織の対応を劇的に改善し、損失を大幅に削減できる。準備には次のようなものが含まれる。

- 顧客がなりすまし電子メールを送信できるなりすまし報告用電子メール・アドレスを提供する。これにより、通信が正規のものかについて顧客にフィードバックを提供できると同時に、攻撃が発生した場合には警告を発することもできる。
- 「バウンス(不達)」電子メールの監視。多くのフィッシャーは、標的機関の返信用アドレスを使用して、実在しない電子メール・アドレスも含む大量のリスト宛に電子メールを送る。大量のバウンス電子メールは、フィッシング攻撃が発生している兆候である。
- 電話による問い合わせの件数や、顧客サービスへの質問の性質を監視する。パスワードが変更されたなどの特定のタイプの問い合わせの急増は、フィッシング攻撃の兆候である。
- 異常な数のログイン、パスワードの変更、送金、引き出しなど、異常な動きがないか口座の動きを監視する。
- 機関の企業ロゴや図を含む画像の使用を監視する。フィッシャーは標的企業を使用して顧客を騙すための図をホストする。これは、画像の「参照者」が空または異例のものであることによりWebサーバ上で検出できることがある。
- 「ハニーポット」を設置し、同機関からとする電子メールが届くか監視する。

これらの多くのサービスを実行できる請負業者もある。標的機関が手続き上の対抗策をとったり、捜査当局と捜査を開始したり、攻撃にタイムリーに対応できるようスタッフを増やせるため、攻撃が発生したことを知ることは有用である。



フィッシングにおける情報の流れ、ステップ1

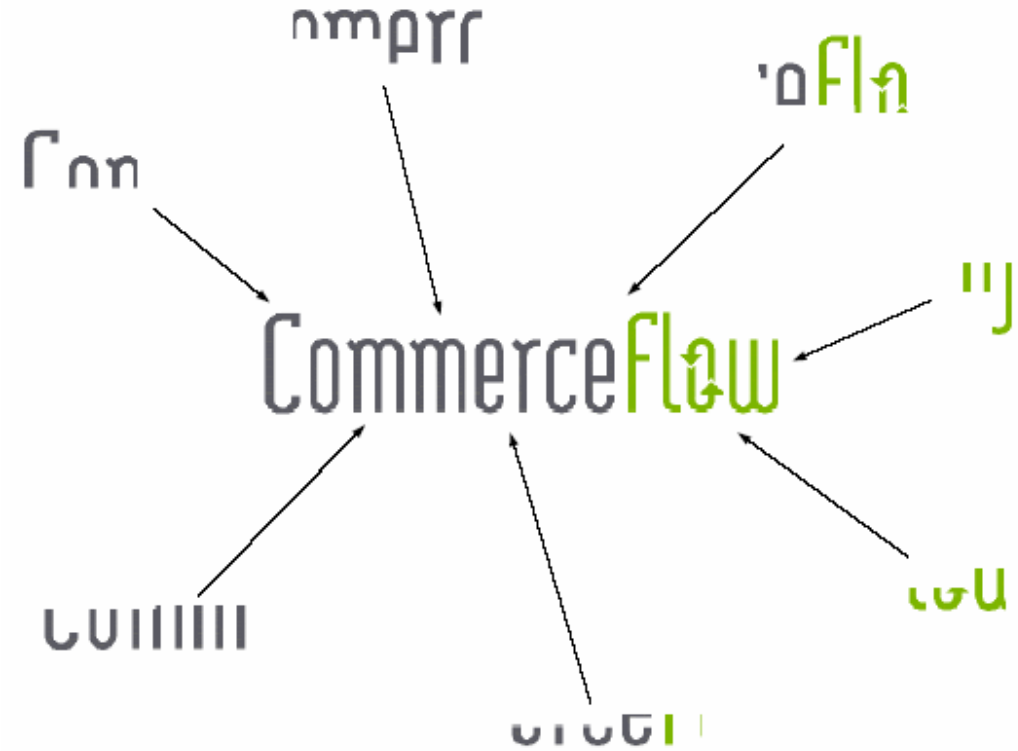
ステップ1：フィッシングのペイロードの配信を防ぐ

ひとたびフィッシング攻撃が始まると、電子メールやセキュリティ攻撃などのフィッシングのペイロードがユーザに届かないようにすることが、フィッシング攻撃を防ぐ最初の機会となる。これはフィッシングの情報の流れのステップ1の妨害を意味する。

ステップ1への対抗策：フィルタリング

スパム対策を目的とした電子メールのフィルタは、フィッシング対策にも有効な場合が多い。署名ベースのスパム防止フィルタは、特定の既知のフィッシング・メッセージを識別し、ユーザに届かないようにするために構成できる。統計またはヒューリスティックによるスパム防止は部分的にフィッシングに効果がある場合もあるが、

フィッシング・メッセージが正規メッセージに似ている場合、フィルタがフィッシングの電子メールを識別するのに足るだけセンシティブに構成されていると、正規の電子メールを誤ってブロックしてしまう危険性がある。効果的な詐欺ベース・フィッシングの電子メールや Web サイトは、まねようとしている機関と同じ外観でなければならない。カラー・スキームや画像は標的機関をまねしたものになる。そこで重要な側面となるのが企業ロゴの使用である。これにより、フィッシングの電子メールに騙される可能性が劇的に高まるからである。
対抗策の 1 つとして、電子メール内の不正なロゴの検出が考えられる。簡単な画像の比較に対抗してフィッシャーが採用し得る対抗策は多数ある。たとえば、小さなタイル状の画像を 1 つの大きな画像として表示したり、透明な画像を積み上げて複合画像を作成したりする。



複合ロゴタイプ・レンダリング

フィッシャーにこのような回避策をとらせないために、画像は分析前に完全にレンダリングする必要がある。全面的にレンダリングされた電子メールなど、大きな画像の中の変更された可能性のある商標またはその他の登録画像をいかに認識するかは、今後研究が進められる分野である。同様のアプローチをWebサイトに適用すれば、ユーザがリンクをクリックした際に役立つ可能性がある。

ステップ1への対抗策：電子メールの認証
フィッシングの電子メールは、信頼できるソースからだとされていることが多い。これには主に2つの方法がある。

- 返信用アドレスの偽造
- 類似ドメインの登録（たとえば、実際のドメインが「commerceflow.com」の企業をスプーフするための「commerceflow-security.com」）と、そのドメイン・ネームからの電子メールの送信

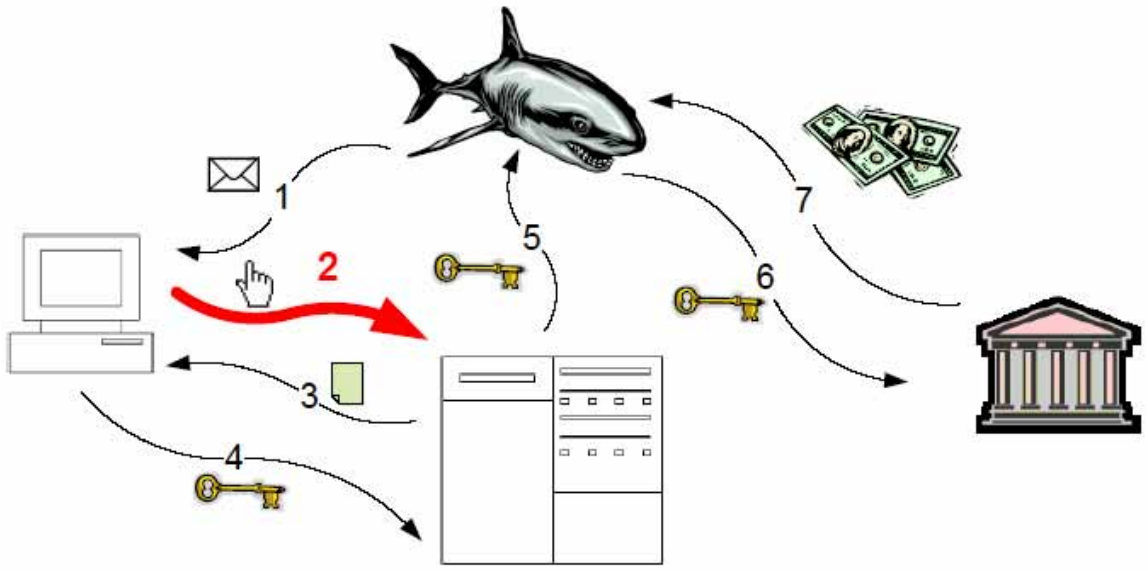
メッセージ認証技術は、フィッシング対策アプリケーションにおいて大いに期待されている。一般的に、メッセージ認証は、電子メールが送信者とされている相手から実際に送信されたものであることを保証する。幅広く展

開されれば、電子メール認証は返信用アドレスの偽造を防ぎ、不審な返信用アドレスの露呈、または公式なものに見えるドメイン・ネームの登録のいずれかをフィッシャーに強いる可能性がある。この利点としては、返信用アドレスが偽造されたアドレスよりも騙されにくいものになること、ドメイン登録がフィッシング攻撃の前に検出できること、フィッシャーをドメイン登録を通じて追跡できることなどがある。
電子メール認証技術は多数提案されている。Sender-IDとSPFは、DNSレコードを確認し、送信を行うメール転送エージェント（MTA）のIPアドレスが送信者のドメインからのメッセージの送信を許可されているかを判断することで、返信用アドレスの偽造を防ぐ。Domain KeysとInternet Identified Emailも、DNSレコードを通じて検証できるドメイン・レベルでの暗号署名を使用して、同様の認証を提供する。MTAの認可によるアプローチには実装が容易という利点があるのに対し、暗号アプローチではエンド・ツー・エンドの認証が提供される。
Sender-IDとSPFは現在IETF Experimental Standard（実験的標準）になっており、一方、MASSのワーキング・グループはDomain KeysとInternet Identified Emailの合併に取り組んでいる。この他にも、否認可能な暗号署名による電子メールや、権限者によって認定された認証トークンを受信者が解釈できるような権限ベースの電子メール認証のための提案などがある。
電子メール認証のためのもう1つのアプローチとして、送信者が受信者に電子メールを送信する権限の証明を提示する方法がある。このような方式には、送信者固有またはポリシー・ベースの電子メール・アドレスの自動生成と使用、メッセージの受信者によって発行され、送信者に送信を許可するトークンまたは証明書の使用などがある。このようなアプローチでは、追加のユーザ・インターフェイス（送信者固有の電子メール・アドレスを生成する場合）またはインフラストラクチャー（トークンの生成および／または証明書の署名および配布を行う場合）のいずれかが必要になる。
何らかの形の軽量なメッセージ認証が、将来フィッシング対策に非常に役立つ可能性がある。この潜在的な価値を実現するためには、認証されていないメッセージを即座に削除するか、またはその他の方法で不利に扱えるよう、電子メール認証技術が十分に広まり、Sender-IDなどのMTAの認可方式におけるメールの転送機能の使用に関するセキュリティの問題を解決する必要がある。
電子メールの暗号署名（S/MIME署名など）は、短期的には前向きで漸進的なステップであり、長期的に幅広く展開されれば効果的な措置となる。署名は、クライアントまたはゲートウェイのいずれかで実行できる。しかし、現在の電子メール・クライアントでは、電子メールが署名されているか否かが表示されるだけである。典型的なユーザは、電子メールが署名されていないことに気付かず、フィッシング攻撃を防げない可能性が高い。署名は、たとえばユーザが署名されていない電子メールのリンクにアクセスしようとした際に警告するなど、署名されていない電子メールの機能が制限されればより有効になる。しかし、これは、今日電子メール・メッセージの大半を占める署名されていないメッセージにとって負担となる。署名された電子メールが臨界点に達すれば、このような措置も実行可能になる可能性がある。

ステップ1への対抗策：セキュア・パッチ

マルウェアが関与するフィッシング攻撃は、セキュリティの脆弱性につけ込んでインストールされることが多い。パッチを当てていないオペレーティング・システムまたはブラウザーを実行しているユーザは、ブラウジングまたは単にインターネットに接続しているだけでもマルウェアに感染するリスクがある。
脆弱性につけ込む行為のほぼすべては、既知の脆弱性を対象にしたものである。あらかじめ知られていない脆弱性を対象とした「ゼロ・デイ」攻撃は、実際には非常にまれである。したがって、ファイアウォールの後ろに完全にパッチされたコンピュータを置くことが、脆弱性への攻撃によるマルウェアのインストールに対する最善の防御策である。
パッチは大きいことが多く、世界的な顧客ベースに配布するには長い時間を要することが多い。また、ユーザやIT部門はパッチを直ちに適用しないことも多い。パッチを適用する前に、バグが多く、コンピュータを不安定にさせる可能性のある最初のパッチが修正されるのを待つのがしばしば賢明であるという調査結果もある。
しかし、パッチの発表と配布は、パッチの対象となるセキュリティの脆弱性について犯罪者に情報を提供することを意味する。説明をあいまいにしても、パッチを分解し、それが置き換えることになるコードと比較できる。

新たに攻撃できる脆弱性が見つかると、マルウェアによる脆弱性の攻撃は事前に構築されたコンポーネントによって直ちに作成できる。パッチがリリースされてから悪質な攻撃が登場するまでの所要時間は、現在では3日未満、場合によってはわずか数時間となっている。この短い時間の後、ほとんどのコンピュータは依然として感染しやすい状態にある。
脆弱性に関する情報を漏らすことなく迅速にパッチを配布し、適用するための有望な提案の1つに、特定の脆弱性に関する集中的なセキュリティ・パッチを、パッチごとに異なる対称鍵を使用して暗号化して配布するというものがある。鍵はベンダーによって内密に保管される。パッチは暗号化された状態では適用できないが、脆弱性に関する情報を犯罪者に漏らすことなくすべての脆弱なコンピュータに配布することは可能である。パスによって修正された実際の脆弱性への攻撃が検出されると、その特定のパッチの複合鍵を直ちにインターネットですべてのコンピュータに配布し、自動的にパッチをインストールできる。脆弱性への攻撃は、パッチが修正する脆弱性への攻撃の試行を検出するハニーポット・マシンで実行されているパッチのバージョンによって検出できる。



フィッシングにおける情報の流れ、ステップ2

ステップ2：ユーザの行動の防止または妨害

フィッシングにおける情報の流れのステップ2は、ユーザを自らの機密情報が漏洩する可能性のある場所に移らせるユーザの行動に関するものである。このプロセスを妨害する対抗策にはいくつかのものがある。

ステップ2への対抗策：教育
ステップ2の対抗策として最も広く展開されているのは、ユーザ・ベースの「教育」である。具体的には、電子メールのリンクをクリックしない、SSLが使われていることを確認する、情報を提供する前にドメイン・ネームが正しいか確認するなどの手法についてユーザに指導する。
このような教育は効果的ではなく、フィッシング・メッセージへの回答率は正規の商売のための電子メールと同程度である。このような教育が効果的でなかった理由は少なくとも4つある。

- 電子メールの発信元、ページの場所、SSLの存在などの、ユーザに通常提示される情報がなりすまされる可能性がある。したがって、いかに教育されていようと、正規のメッセージとフィッシング攻撃の識別において、ユーザを頼りにすることには無理がある。

- SSLが使われていることの確認やドメイン・ネームの確認などの行動は、ユーザの通常のサイトとの対話と直接関係がないため、スキップされることが多い。
- 金融機関は、フィッシング・メッセージを正規の通信と区別するために広めてきたガイドラインから大幅に逸れてきたため、広めてきた教育のためのメッセージがむしばまれている。とりわけ、多くの金融機関は、フィッシャーが使うような意外なドメイン・ネームを使用したり、ログイン・ページでユーザが確認できるような形でSSLを使用しなかったり、電子メール通信にクリックできるリンクを含めたりしている。
- ユーザは欠陥や障害には慣れており、フィッシング関連の動きの解釈方法をよく知らないことが多い。ユーザはフィッシングの兆候をソフトウェアのバグやその他のエラーによるものだと正当化することが多い。

顧客が正規のサイトとの特定の対話のモードに慣れ、慣習から逸れたサイトを疑いやすくなるため、フィッシャーとは異なる一貫した慣習に従うことが、顧客を教育するためのおそらく最も効果的な方法である。金融機関は次のような慣習に従うことで、このような教育を促進できる。

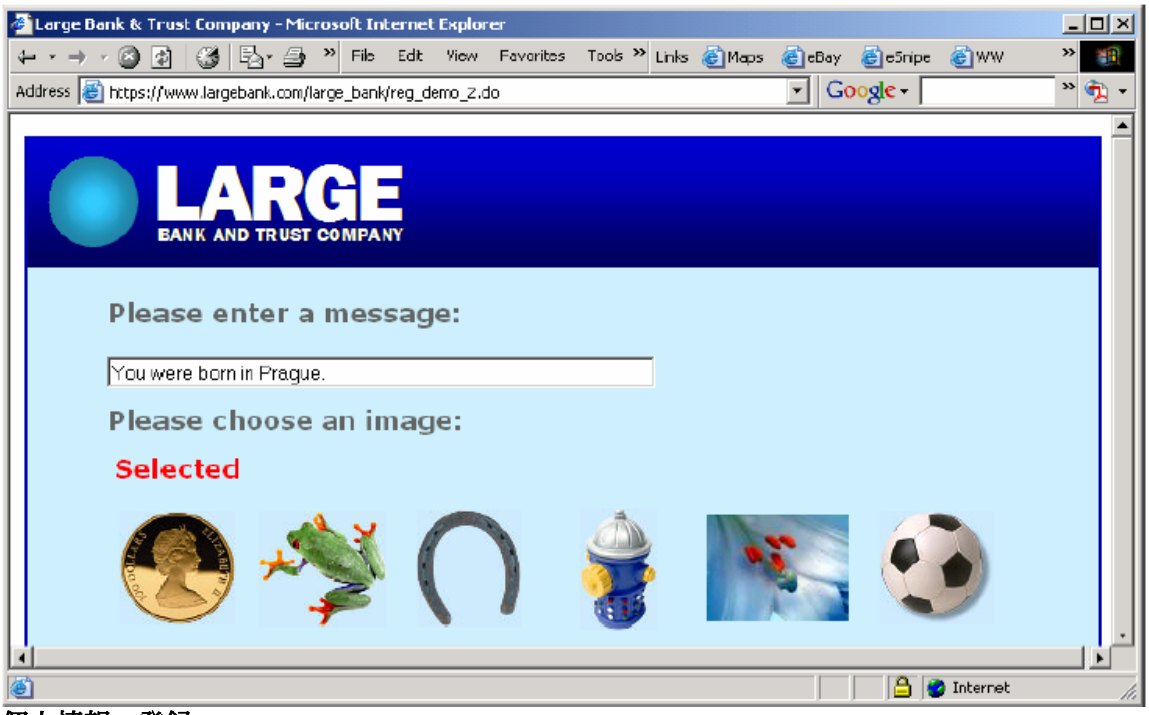
- クリック可能なリンクが実際にはマーケティングの貴重な形態となっている場合、クリック可能なリンクは決して使わないなどと顧客に言わない
- リンクにアクセスしない場合にマイナスの結果が生じると警告するような電子メールでは、「行動要請」は決して使わない
- 電子メール認証技術を使用する
- リンクを使用する場合、分かりやすい名前のリンクを使用する（虚偽的な名前のリンクは使わない）
- ログインには予想されるドメイン・ネームを必ず使用する
- ログイン・ページおよびその他のすべてのページで必ずSSLを使用する

ステップ2への対抗策：個人情報の使用

フィッシング・メッセージに騙されにくくする簡単な方法として、すべての正規の通信に個人情報を含める方法がある。たとえば、commerceflow.comからのすべての電子メールがユーザの名前で始まり、commerceflow.comがこの慣習についてユーザに教育していれば、ユーザの名前を含まない電子メールは疑わしいということになる。複数の事業部門間での連携の難しさ、提携企業によるマーケティング・プログラム、外部サービスに電子メールをアウトソーシングする慣習の拡大などにより、この慣習の導入は複雑なものになる可能性があるが、効果的な措置である。情報がパートナーと共有されたり、安全でないチャネル経由で送られることが多いため、使用する個人情報はいずれもセンシティブでないものにすべきである。

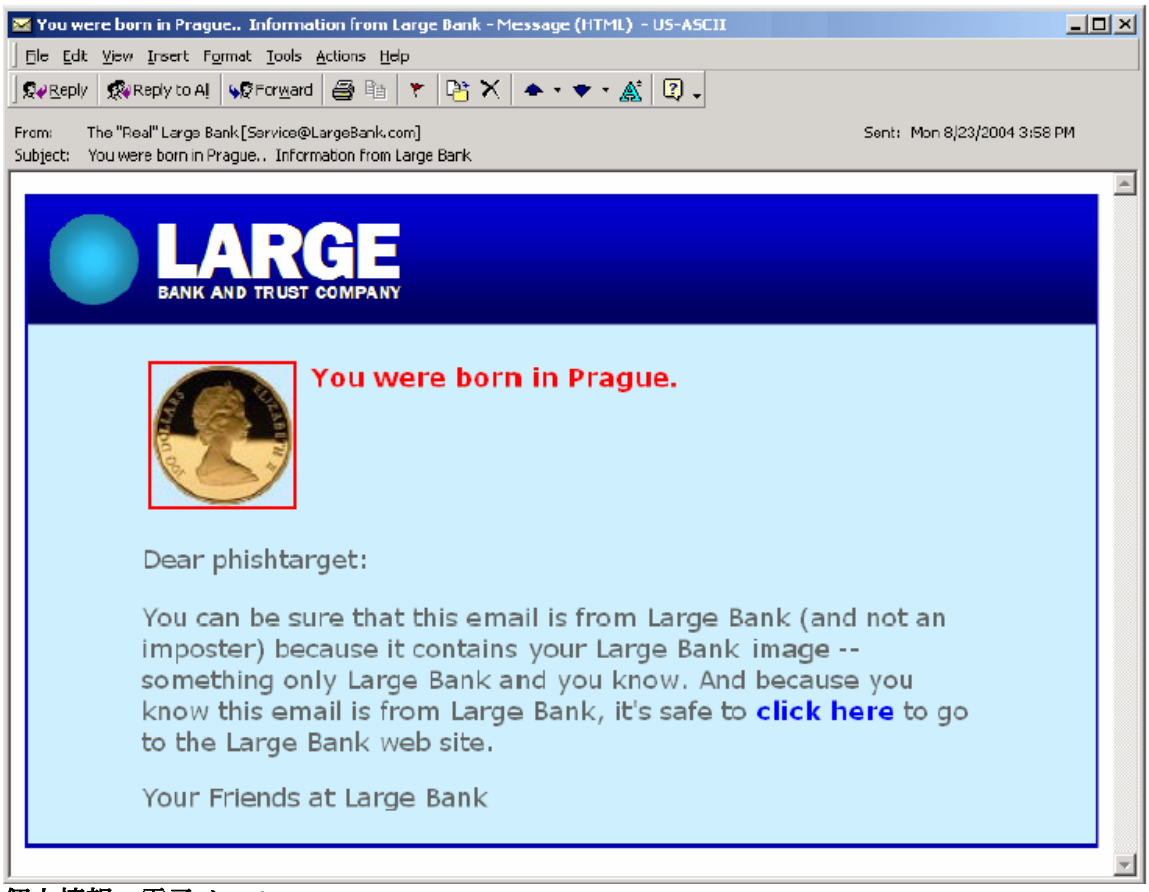
静的な識別情報以外にも、ユーザが使用を求めたテキストなどのより高度な個人情報も含むことができる。これによりユーザは、希望する情報が含まれていることを容易に確認できる。

個別の画像もメッセージの送信に使用できる。たとえば、ユーザがアカウント情報の作成または更新を行うと、そのユーザはその後個人情報として使われるテキストおよび／またはグラフィック情報の入力を許可（または要求）される。この例では、Large Bank and Trust Companyの顧客が個別テキストとして「You were born in Prague」とタイプし、カナダの1セント銅貨の画像を選択またはアップロードしている。



個人情報：登録

Large Bank and Trust Companyからのこれ以降の電子メールには、次のようにこの個人情報が含まれるようになる。



個人情報：電子メール

フィッシャーは、ユーザがどのような個人情報を選択したか知らないため、詐欺メールを偽造できなくなる。Webサイトでも、ユーザがユーザ名を入力した後、パスワードを入力する前に、同様のアプローチを使用できる。しかし、Webサイトではまず他の手段でユーザを認証する必要がある。中間者攻撃を防ぐために、二要素認証などの追加の認証を使用し、ユーザとコンピュータが正規のものであることを確認してから個人情報を表示すべきである。ユーザが確認できたら、個人用のテキストおよび／またはグラフィックが表示され、ユーザは個人情報が正しいことを確認してからパスワード情報を入力する。

このタイプのアプローチはユーザの教育に多少依存するものの、ロック・アイコンのチェック、署名のない電子メールの不信扱い、またはURLのタイプなどに関する忠告とは異なり、ユーザとメッセージまたはサイトとの間の対話に構造上の違いがある。これらの構造上の違いによって、ユーザはフィッシング攻撃と正規の対話との違いを見分けやすくなる可能性がある。

ステップ2への対抗策：詐欺コンテンツの正規表示

詐欺ベース・フィッシング電子メールでは、ユーザにリンクをクリックしてWebサイトを訪問するよう求めるものが多い。フィッシャーのWebサイトは、通常、正規の名前を持たないため、リンクの実際の宛先は偽装されていることが多い（類似ドメインを使用した攻撃、DNSのネーム解決への攻撃によるフィッシングサイトへの到達、国際化ドメイン名による同形異義語攻撃などはこの法則の例外である）。

現在では、コンテンツの作成者の指定方法に関係なくリンクを表示できる。これにより、フィッシングの電子メールで詐欺リンクが作りやすくなっている。フィッシャーはリンクの真の宛先を見えなくするために、多くの技術を採用している。たとえば次のようなものがある。

誤解を招くような名前のリンク－http://security.commerceflow.com と表示されているリンクが実際には http://phisher.com に結び付いている。
覆い隠されたリンク－URLにユーザ名とパスワードが組み込まれている。これにより、リンクの実際の宛先を「覆い隠す」ことができる。たとえば、
http://security.commerceflow.com@phisher.com というURLは実際には http://phisher.com に結び付いている。
リダイレクトされるリンク－あるURLへの参照を別のURLへと変換する「リダイレクト」はWebプログラミングで使われることが多い。標的機関の不注意なプログラマーが任意の場所へのリダイレクトに使用できる「オープンなリダイレクト」をアクセス可能な状態にしたままにすると、フィッシャーによってフィッシング・サイトにリダイレクトする正規のようなURLの提供に使われる可能性がある。
偽装リンク－URLにはURLの意味を隠すエンコードされた文字が含まれることがある。これは、たとえば覆い隠されたリンクやリダイレクトされるリンクのターゲットを見えなくするためなど、他のタイプのリンクと組み合わせて使われることが多い。
プログラムによって見えなくされたリンク－スクリプトの実行が許可されている場合、ユーザがリンクの宛先を見るためにマウスをリンクにかざした際にJavascriptによってステータス・テキストを変更できる。
マップ・リンク－正規のようなURLを参照するHTML「イメージ・マップ」内にリンクを含めることができる。しかし、イメージ・マップ内をクリックした場合にブラウザーが誘導される実際の場所は、ユーザには表示されない。
同形異義語URL－リンクのURLにIDN（国際化ドメイン名）の同形異義語、すなわち通常の文字と同じに表示されるものの実際には異なる文字（キリル文字など、異なるアルファベットの文字が一般的）を使用できる。現在では、これは標準外の構成のブラウザーで問題となることがほとんどである。

電子メール・クライアントまたはブラウザーへの実装への対抗策の1つとして、ユーザに疑わしいものとして明確に示せる予測可能な方法で潜在的詐欺コンテンツをレンダリングすることが考えられる。たとえば、次のHTMLフラグメントとその典型的なレンダリングの例について考えてみる。

```
<CENTER><H1>Suspicious URLs</H1></center>
<P>To go to a surprising place via a cloaked URL, click on
<A HREF="http://security.commerceflow.com@phisher.com">this link.</A>
<P>To go to a surprising place via a cloaked URL with a password, click on
<A HREF="http://security.commerceflow.com:password@phisher.com">this
link.</A>
<P>To go to a surprising place via an open redirect, click on
<A HREF="http://redirect.legitimatesite.com?url=phisher.com">this link.</A>
<P>To go to a surprising place via misleading link, click on
<A HREF="http://phisher.com">http://security.commerceflow.com.</A>
```

詐欺リンクを含むHTMLコンテンツ

詐欺リンクを含むHTMLコンテンツのブラウザ表示

ユーザは、クリックする前にステータス・バーのURLを見ても、クリックするリンクの実際の宛先を理解できないことがある。リンクのぼかしが使われている場合、特にこれが当てはまる。とりわけステータス・バーのスプーフィングへの対抗策（たとえば、URLの重要な部分を必ず表示し、URLが表示される際にスクリプトでステータス・バーを変更できないようにする）と組み合わせた場合、電子メール・クライアントまたはブラウザーの拡張機能によって、混乱を招く可能性のあるURLの宛先をアイコンで示すことで、ユーザのためにこの状況を明確化できる。上記のページは次のようにより多くの情報を提供するようレンダリングすることもできる。

詐欺リンクを含むHTMLコンテンツのレンダリング、正規表示

ステップ2への対抗策：誘導の妨害
ユーザが、覆い隠されたリンク、ぼかされたリンク、マップされたリンク、または誤解を招くような名前のリンクなどの疑わしいリンクをクリックした際に、警告メッセージを示し、リンクのトラバースの潜在的な危険についてユーザに忠告することもできる。情報は率直に示すべきであるが、単純化する必要はない。ユーザが十分な情報に基づく決定を行えるよう、リバースDNSやWHOISルックアップなどのソースからのデータを有効に含める。

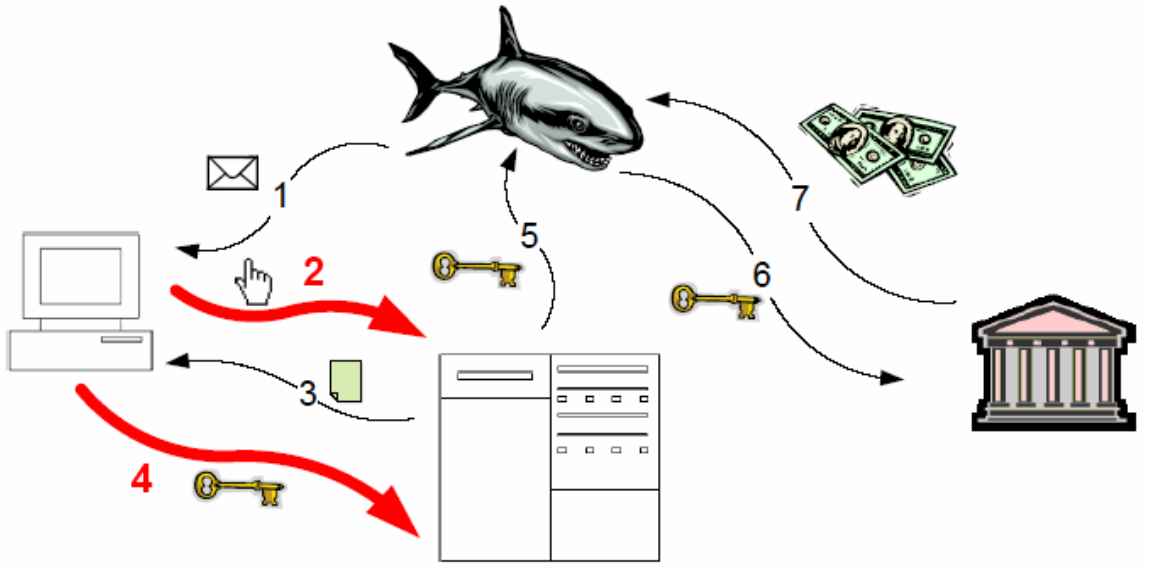
安全でないリンク・トラバーサルに関する警告メッセージ

情報を提供するような警告では、疑わしい性質の正規のリンクを許可する一方で、ユーザが適切な行動を決定するために必要な情報についてリスク評価を提供できるメリットがある。
調査によれば、このような情報は、ある動作を実現するためにユーザが実行すべき「重大な動作シーケンス」の一部になっていた方が、ユーザによってより確実に評価される。したがって、意図する選択肢をユーザがいくつかの選択肢から選択する必要のある対話の方が効果的である。

ステップ2への対抗策：一貫性のないDNS情報の検出
DNSベース・フィッシング攻撃は、ホストに誤ったDNS情報を提供できることに依存した攻撃である。このようなフィッシング攻撃は、ユーザが過去に関係を持っているサイトを訪問することが頼りのため、悪質な情報を検出できる可能性がある。過去のルックアップについて、DNSキャッシュとは別にレコードを保管できる。名前解決が別の結果をもたらした場合、信頼できるとされている外部ソースに正式な答えを求める。
また、数値IPアドレスを使用した攻撃（攻撃された自宅のマシン上のサーバのフィッシングにおいて一般的なシナリオ）において、対応するDNSルックアップが実行されていないIPアドレスへのアクセスを検出するにも効果

的な可能性がある。

ステップ2への対抗策：参照された画像の変更
フィッシャーは、標的企業によって制御されているサイト上の画像にアクセスし、正規の電子メールまたはWebサイトのルック&フィールをまねることがある。標的機関は、ある画像に対して届く要求の参照者フィールドを調べることでこの活動を検出できる。ひとたびフィッシング攻撃が始まれば、Webサーバはその画像の提供を拒否するか、またはフィッシング攻撃に関する情報提供のためのメッセージを表示した画像でその画像を置き換えることができる。
この対抗策は、電子メールから画像が参照されるようなステップ2に当てはまる。また、ステップ3で送信されたWebページが正規のサイトの画像を参照するステップ4にも当てはまる。自ら画像をホストしているフィッシャーには簡単に回避されるものの、今日まで多くの攻撃に有効となっている。



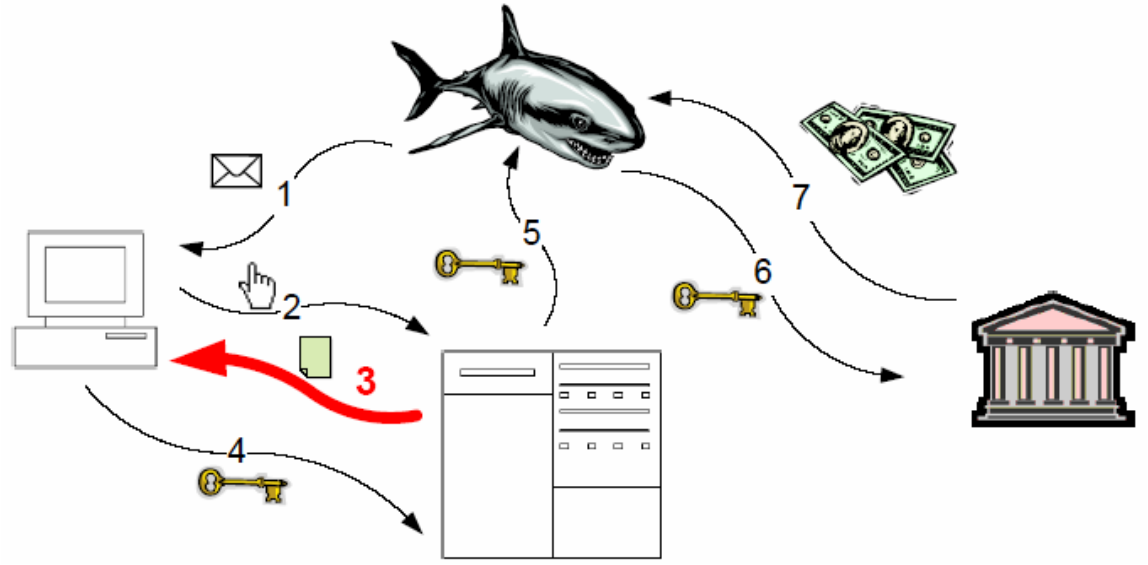
フィッシングにおける情報の流れ、ステップ2および4

ステップ2および4：誘導とデータ漏洩を防ぐ

フィッシングにおける情報の流れのステップ2は、ユーザをフィッシング攻撃に対して脆弱にするフィッシングサイトへのナビゲーションなどのユーザの行動である。ステップ4では、機密情報が漏洩する。

ステップ2および4への対抗策：アプリケーション間のデータ共有の増加
将来取り組みが進められる分野に、スパム・フィルタ、電子メール・クライアント、およびブラウザー間での情報共有の増加によるフィッシング対策がある。重要な情報はこれらのアプリケーションの境界で失われることが多い。スパム・フィルタがあるメッセージを不法扱いにしたとしても、拒否されるしきい値を下回っている限り、電子メール・クライアントでは信頼できる企業からの署名された電子メールと対等に扱われる。
メッセージの処理中に集められた情報もフィッシングの阻止に役立つ。電子メールが疑わしい場合、ユーザのホワイトリストの送信者またはBonded Sender Program（合法メール送信者の認定サービス）のメンバーからの認証されたメッセージとは別に扱うことができる。
疑わしいメッセージの視覚的な表示、スクリプトの不許可、リンクの真の名前の表示、フォームの不許可などが可能である。この対抗策は、フィッシングの情報の流れのステップ2に対応するものである。
同様に、ひとたびユーザが電子メール・メッセージ内のリンクをクリックすると、メッセージの信頼性に関する

情報が、トラバーサルを許可すべきかの判断に役立つ。リンクがトラバースされたら、信頼性が低めのメッセージで示されているリンクの機能（スクリプトの記述、フォームの送信、リンクの表示など）を制限し、フィッシングの情報の流れのステップ4の発生を防げる。
スパム・フィルタ、電子メール・クライアント、およびブラウザー間のインターフェイスは、信頼性に関する情報の送信を許可し、多くの新しいフィッシング対策法を可能にする。



フィッシングにおける情報の流れ、ステップ3

ステップ3：プロンプトの送信を防ぐ

フィッシングにおける情報の流れのステップ3は、不正な相手への機密情報の漏洩につながるユーザへのプロンプトである。ステップ3への対抗策ではこのプロンプトを攻撃し、プロンプトが届くのを防ぐか、または悪意のある相手に対し漏洩する情報が含まれるのを防ぐ。

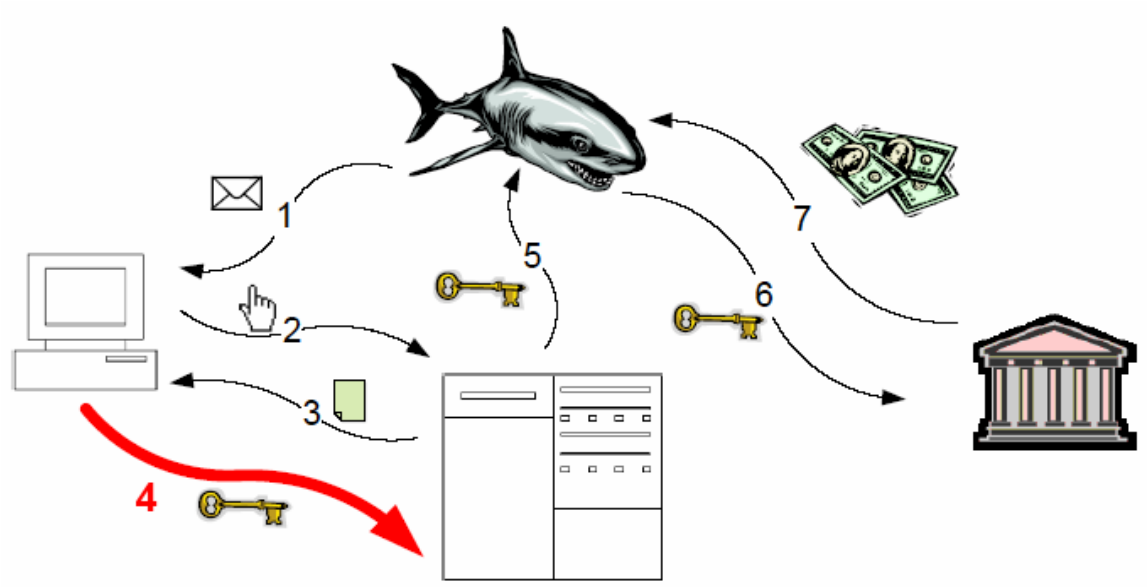
ステップ3への対抗策：クロスサイトスクリプティングの除去

クロスサイトスクリプティングは、2つある方法のいずれかによって行われるコンテンツインジェクション攻撃である。フィッシャーはフィッシングの流れのステップ1で、顧客によるレビュー、オークション、Webベース電子メール、または同様のコンテンツの一部として正規のサーバに保管することで、悪質なコンテンツを正規のWebページに注入できる。フィッシャーは、検索結果とともに表示されるスクリプトを検索クエリーに組み込むことで、ステップ1のユーザへの電子メールに含まれるURLに悪質なコードを含めることもできる。このようなURLに組み込まれたコンテンツは、ステップ2でユーザから正規のサーバに送られ、ステップ3で機密情報を求めるプロンプトの一部として戻される。
クロスサイトスクリプトは、ひとたび注入されると、ユーザがターゲットとした機関と通信していると信じるようホスト・サイトの要素を変更する。ユーザは実際にはフィッシャーに機密情報を提供することになる。
クロスサイトスクリプティングによってフィッシングの情報の流れのステップ3を妨害するには、画面に一度でも表示されたユーザ・データはフィルタにかけ、スクリプトをすべて除去する必要がある。悪意のある関係者は、Webベース電子メールのページの日付フィールドなど、予期せぬ場所にクロスサイトスクリプティング攻撃を組み込んできた。禁じられたスクリプト・要素を「締め出し」フィルタにかけて除去するのではなく、ユーザが提供したデータを「受け入れ」フィルタによって解析し、許可されたデータ・要素のみを受け入れるべきである。
クロスサイトスクリプトまたはその他のHTML要素はWebサイトの外観を損ねたり、変更したり、あるいは識別

情報の盗難とは関係のないその他の損害を招く可能性があるため、このようなフィルタリングは、さまざまな理由により適切なWebサイトの設計の一要素となっている。

ステップ3への対抗策：注入されたスクリプトの無効化
クロスサイトスクリプティングを導入する方法には多数のものがある。適切なフィルタを記述することは困難であり、コストも高く、エラーも発生しやすい。また、フィルタにかけられるべきコンテンツが不注意で見落とされることも多い。
ブラウザーの拡張により、将来クロスサイトスクリプティングに対する保護が提供される可能性がある。HTMLに含めることのできる<noscript>などの新しいタグが導入されれば、スクリプティングが一切行えない領域や、特定の機能が禁止された領域を定義できる。ブラウザーはこの動作を保証でき、十分なフィルタリングの採用は、検索結果またはオークションのリストなどのユーザが提供したテキストを適切な<noscript>および</noscript>タグで囲むだけというように簡単にできるようになる。
悪意のある関係者が有効な</noscript>タグを使用し、クロスサイトスクリプトを挿入することのないよう、<noscript>タグと</noscript>タグで一致する必要のある動的に生成されるランダム鍵を使用すべきである。このような鍵は、Webコンテンツのオーサリング・ツールによって自動的に生成できる。ユーザが提供したコンテンツはどの乱数が鍵に使われたか知るすべがないため、スクリプティングの特権を再度有効にするのに必要な情報を欠くことになる。たとえば次のようになる。

[サイトが提供したHTMLとスクリプト]
<noscript key=”432097u5iowhe”>
[スクリプト／機能が無効になっている、ユーザが提供したHTML]
</noscript key=”432097u5iowhe”>
[サイトが提供したHTMLとスクリプト]



フィッシングにおける情報の流れ、ステップ4

ステップ4：機密情報の送信を防ぐ

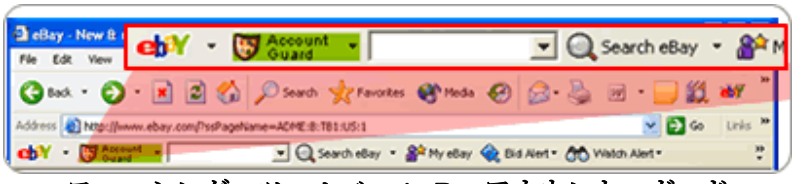
フィッシング攻撃を妨害できるもう1つの点は、ユーザがフィッシング情報の流れのステップ4で機密情報の送信

を試みるときである。詐欺フィッシングサイトが不正なものであることを対象となっている被害者に明らかにしたり、または情報の流れを妨害または変更し、機密情報をフィッシャーに利用できないようにしたり無駄なものにすることができれば、攻撃を阻止できる。
典型的な詐欺ベース・フィッシング攻撃では、フィッシャーはさまざまな技術を使用して、ユーザを正規のサイトにいると騙し続けようとする。これにも急速に変化する多数の技術が関与している。ブラウザーの場所についてユーザを騙す方法の1つに、詐欺リンクの使用がある。もう1つは、詐欺情報がURLバーに表示されるようにする方法である。たとえば、フィッシャーは、枠なしウィンドウ(borderless window)をポップアップさせてURLバーの実際のコンテンツを覆い隠し、ユーザがブラウザーのウィンドウを動かすと詐欺ウィンドウも動くようなJavascriptプログラムを作成した。これらのJavascriptプログラムは、ユーザが履歴ボックスをクリックすると、ウィンドウの履歴をまねる。
ブラウザーのロック・アイコンを見ることで、サイトへの接続が安全か（すなわちSSLを使用しているか）を判断することはできない。ロック・アイコンが信用できない理由はいくつかある。

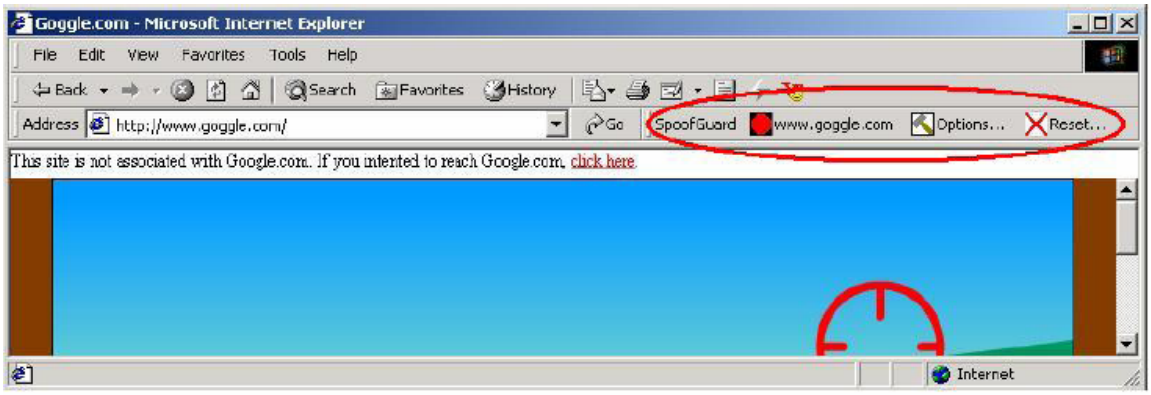
- ロック・アイコン単独では、サイトが証明書を持っているという意味しかなく、表示されている（詐欺）URLと証明書が一致することを確認するものではない。ユーザはロック・アイコンをクリックし、その意味を判断する必要があるが、これを行うユーザはわずかである。
- 特定の暗号化の設定により、自己署名証明書（有効な認証局によって発行されていない証明書）を使用してロック・アイコンを表示させることのできるブラウザーもある。
- URLバーの改竄に使われるのと同じ技術によって、ロック・アイコンをブラウザーの上に重ねることができる。この技法では、正当なものかを確認するためにユーザがロック・アイコンをクリックした際に、本物に見える証明書データを提示することもできる。

ブラウザー技術は絶えず更新され最近のフィッシング戦術に対応しているが、ブラウザーは、正規のWebサイトの設計者のニーズを満たすだけの十分な機能性と柔軟性を提供する必要のある、大規模で複雑なプログラムである。フィッシング技術に断片的に対応するだけで詐欺フィッシングの出現を完全に阻止できる可能性は非常に低い。

ステップ4への対抗策：フィッシング防止ツールバー
フィッシングサイトを特定し、ユーザに警告を試みるブラウザーのツールバーが提供されている。これらは研究プロジェクトと技術サプライヤーの双方から提供されている。フィッシング防止ツールバーは、既知のフィッシングサイトのデータベース、サイトのURLの分析、サイトの画像の分析、サイトのテキストの分析、フィッシングサイトを検出するためのさまざまなヒューリスティックなど、さまざまな技術によって安全でないサイトを見分ける。通常、サイトの安全性を示す信号機などによって視覚的に印を表示する。この場合、青は既知の良いサイト、黄色は知られていないサイト、赤は疑わしいサイトまたは既知の悪いサイトである。たとえば次のように表示される。



フィッシング・ツールバー：eBayアカウント・ガード
この例では、ユーザはeBayのサイトを表示しているため、インジケーターは青である。もう1つのツールバーの例では、ユーザは虚偽的な名前のサイトを訪問しており、危険を表示するとともに、ユーザが訪問していると信じている可能性が最も高いサイトへの容易な誘導を提供している。



フィッシング・ツールバー：スタンフォードのSpoofGuard

フィッシング防止ツールバーは、最新の技術を使用してなりすまされる可能性がある。画面上での場所の予約と組み合わせ、いかなるページまたはスクリプトによっても上書きされないようにすればこの危険性は回避できる。ユーザはさまざまなタイプのツールバーの表示に対し、異なる反応をすることが調査により明らかになっている。とりわけ、ある行動をとるべきか否かに関する具体的な案内を提供するツールバーは、サイトについて中立的またはプラスの情報のみを提供するツールバーに比べ、ユーザのトレーニング後には2倍以上の効果を実現することもある。しかし、最も効果的なツールバーでさえ、ユーザのトレーニングを行っていても、ユーザがフィッシングサイトを訪問した場合のフィッシングの成功率は依然として10%を超える。

フィッシング防止ツールバーによっては、ユーザが関係を持っているWebサイトに実際にアクセスした場合に、個人情報を使用して、ユーザが選択した名前または画像を表示するものもある。

アニメーション表示された境界線、ウィンドウの背景またはブラウザー・ウィンドウを囲む「クローム」のグラフィック・パターンなど、特殊なユーザ体験(experience)をブラウザー・ウィンドウごとに提供し、なりすましの防止を狙うブラウザー・プラグインもある。特殊なユーザ体験はクライアントでセッションごとに生成されるため、なりすましに対する耐性がある。このようなアプローチでは、異常なウィンドウの検出についてはユーザに依存しているため、スプーフされたウィンドウの検出の容易性と、美学的な容認可能性と押し付けがましさとのバランスが必要である。

フィッシング防止ツールバーの多くはサイトに関する情報の提供にとどまらず、フィッシングサイトと思われるサイトへのユーザの機密情報の入力の検出も試みる。ツールバーは機密情報のハッシュを保管し、発信される情報を監視して送信される機密情報を検出する。機密情報が検出されると、不正な場所に送られないよう情報の宛先が確認される。

発信データの監視には、克服すべき困難な障害がある。フィッシャーは発信情報を転送前に暗号化することがあるため、キー・ストロークは非常に低いレベルで傍受する必要がある（フィッシング・ツールバーによってはフォームの送信まで機密情報の検出を待つものもあるが、これは簡単な次善策に対して効果的でない）。同様に、Webページのスクリプトは文字がタイプされたそのままのデータを送信できる。さらに、キーロガーによる攻撃を防ぐためにアカウントとパスワード情報の順序を並べ替えてキー・ストロークを入力するユーザもおり、キーロガーの防御も無力になっている。フィッシング防止技術としての発信データの監視の長期的な実行可能性は不明だが、現時点ではほとんどのフィッシング攻撃には次善策が含まれていないため、効果的である。

ステップ4への対抗策：データ宛先のブラックリスト作成

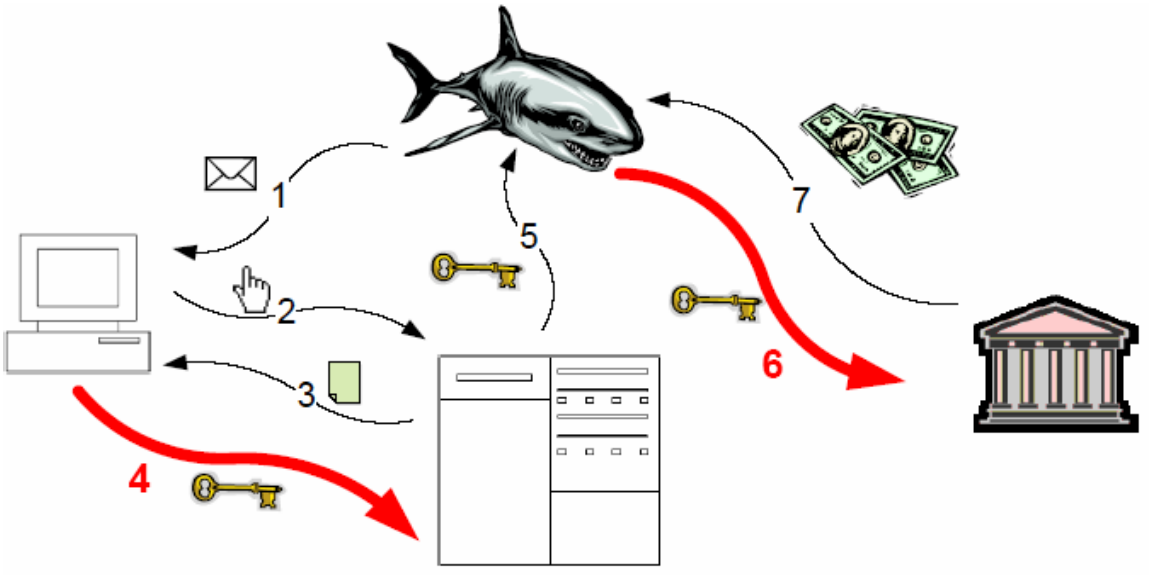
フィッシャーと関係があるとされている特定のIPアドレスへのデータ送信をブロックする案がいくつかある。これは、フィッシングの情報の流れのステップ4を妨害する試みである。

データ宛先のブラックリスト作成には主な課題が2つある。第一に、フィッシング攻撃は、ボットネットまたは同様の構成によって多くのサーバを使用して分散型で実行されることがますます多くなっている。すべてのフィッ

シング・サーバを探すのは難題である。それが可能だったとしても、ホスト名をIPアドレスに変換するのに使われるインターネットのドメイン・ネーム・システム（DNS）を使用し、情報を内密の通信チャネルを通じて送信できるため、情報の送信を持続的に防ぐことにはならない。この簡単な例としては、フィッシャーがphisher.comのDNSサーバを制御しており、「credit-card-info」を送信したい場合、「credit-card-info.phisher.com」でDNSルックアップを行う。DNSルックアップの結果は重要ではない。データはDNS要求自体によってすでに送信されたからである。DNSはインターネットの根本的な基礎であるため、不明なアドレスについてDNSルックアップをブロックすることは実行可能ではない。
すべてのフィッシング・ドメインのDNSルックアップを何とか防げたブラックリストでさえ、DNS経由での迂回に遭う可能性は残る。フィッシャーがDNSサーバを一切制御していない場合でも、罪のない第三者DNSサーバからのDNS応答の生存時間フィールドを使用してDNS経由で情報を送信できる。
実際には、内密の通信チャネルの閉鎖は難しい問題であり、決然たる対抗者に対しては有効でない可能性が高い。

ステップ4への対抗策：画面ベースのデータ入力
重要な情報については、代わりのデータ入力メカニズムを展開している企業もある。ユーザは情報をタイプする代わりに、画面で情報を選択することで入力する。これはフィッシングの情報の流れのステップ4のキーロギング・マルウェアを妨害する試みである。
フィッシャーは次善策を展開していないため、画面ベースのデータ入力は現時点では有効である。しかし、画面ベースのデータ入力がさらに広く展開されるようになれば、マルウェアが表示を妨害し、画面に表示されたデータとユーザのそれとの対話を評価し、それによって機密情報が漏洩することも考えられる。

ステップ4への対抗策：相互認証
パスワードなどの認証のための認証情報においては、多くの場合、認証情報は双方の関係者に知られる。それを送信する代わりに、相互認証プロトコルを使用すれば、両者が認証情報を持っていることを相互に証明し合うことができ、いずれの側も認証情報を送信する必要がなくなる。
このようなプロトコルは多数ある。これらはユーザが認証情報を持っていることをサイトに対し証明すると同時に、ユーザにはサイトが認証情報を持っていることを証明できる。フィッシングへの適用は、このようなプロトコルを確実に使用する必要がある場合に限られたものになっている。フィッシャーは、認証情報を求めるだけで、プロトコルは実行しない。したがって、このような認証情報をすべてWebサイトではなく特別なプログラムに入れておくか、または後に説明するような信頼できるパスによるメカニズムを使用するべきである。相互認証プロトコルが使われることをユーザに示すもう1つの方法は、コンテンツが相互認証に使われるすべてのウィンドウに特定の画像を表示するというものである。このような画像はクライアント側に保管され、容易に詐称されることのないよう外部の関係者には秘密にされる。
相互認証プロトコルのもう1つの潜在的問題は、双方の認証情報が一致しなければならない点である。ユーザのパスワードの保管は良い慣習ではない。ほとんどの場合、パスワードはソフトでハッシュされて保管される。解釈可能なパスワードを保管する必要を避けるために、パスワードの相互認証プロトコルを、フィッシングの情報の流れのステップ6で説明するパスワード・ハッシングと組み合わせることができる。



フィッシングにおける情報の流れ、ステップ4および6

ステップ4および6：データ入力を防ぎ、役に立たないものにする

フィッシング攻撃における情報の流れのステップ4では、データが漏洩し、ステップ6では漏洩した情報が金銭上の利益のために使われる。ステップ4と6を攻撃する対抗策は、情報が漏洩する可能性を低くし、漏洩した場合にフィッシャーが情報を使えないようにする。

ステップ4および6への対抗策：信頼できるパス

インターネットの信頼モデルの根本的な欠点は、入力したデータが最終的にどこに送られるかがユーザにとって明らかでない点である。なりすまし不可能な信頼できるパスでは、重要な情報が正規の受信者にのみ届くことが保証される。信頼できるパスは、詐欺ベース・フィッシングとDNSベース・フィッシングに対する保護を提供する。オペレーティング・システムに実装されれば、アプリケーション・レベルのマルウェア攻撃からの保護も可能である。

信頼できるパスは、画面内の予約したエリアまたは傍受不可能な入力のいずれかのメカニズムを使用し、ログイン情報のために使われてきた。後者の例としては、Windows NTファミリーのオペレーティング・システムを使用したコンピュータへのログインにおけるCTRL-ALT-DELの使用がある。これは、C2認定のための米国コンピュータ・セキュリティ・センターの要件の一環として実装された。

従来型の信頼できるパスのメカニズムは、ユーザとオペレーティング・システムの間にローカル・マシン上で信頼できるチャネルを確立できる。有効なフィッシング対策のためには、悪質なサーバやプロキシーが存在する中、ユーザとリモート・コンピュータの間の信頼できないインターネット上に信頼できるパスを確立する必要がある。オペレーティング・システムは、次の2つの別々のタイプの引数によって呼び出される信頼できるパスのシステム・サービスを提供することで、センシティブな情報の入力を保護できる。

- 要求者のID、表示するロゴ、および公開鍵を含む認証局によって暗号署名された証明書
- 要求されているデータの仕様

この最も簡単な実装方法は、現在のWebページの受信に使われたアクティブなSSL接続に使われているサーバの証明書を使用し、データ入力に信頼できるパスを使用すべきだと指示するタグをHTMLフォームに含めることである。HTMLフォームは、ブラウザーからの信頼できるパスのサービスへの呼び出しにおいて、要求されたデータの仕様として使用できる。

オペレーティング・システムが信頼できるパスによる差し迫ったデータ入力について知らされると、ユーザは「セキュア・アテンション・シーケンス」として知られる傍受不可能なキー・シーケンスの入力を求められる。WindowsではCTRL-ALT-DELはセキュア・アテンション・シーケンスとなっている。これを使用するか、またはより使いやすい実装として、キーボードの特別なキーを信頼できるパスによるデータ入力専用にしておくこともできる。

信頼できるパス：要求の通知

ユーザがセキュア・アテンション・シーケンスを入力すると、オペレーティング・システムは信頼できるパスによるデータ入力が要求されたと判断して標準入力画面を表示し、データ要求者のIDとロゴを証明書から表示し、指定された入力フィールドを表示する。

信頼できるパス：入力画面

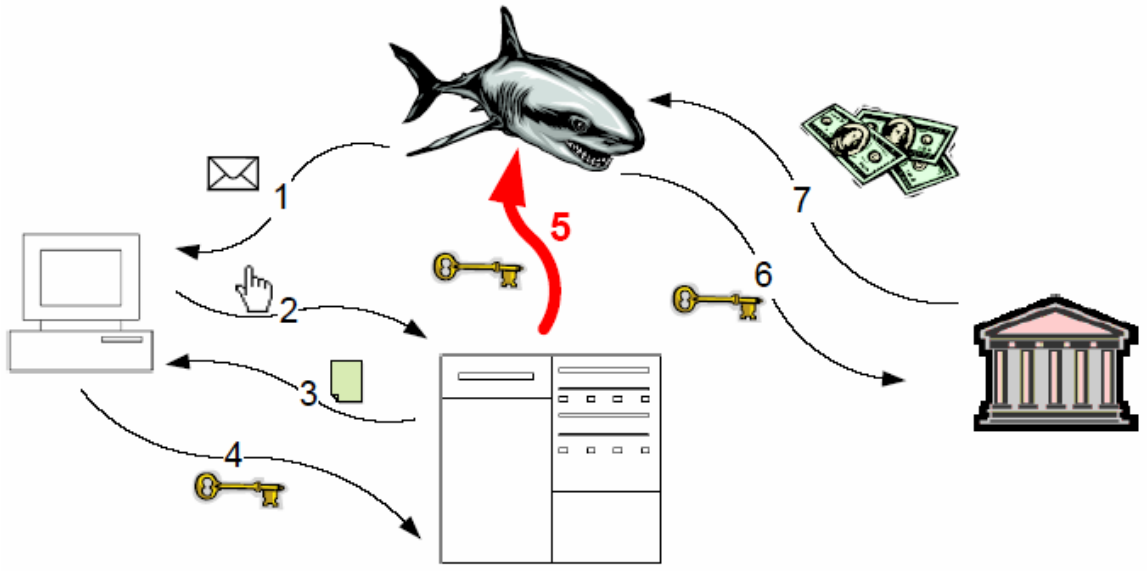
セキュア・アテンション・シーケンスを受け取るのはオペレーティング・システムのみのため、オペレーティング・システムは確実に主導権を持つことができる。信頼できるパスによるデータ入力画面は、制御された環境にあるオペレーティング・システムによって直接表示される。このモードでは、表示を変更したり、キー・ストロークを傍受できるユーザ・プロセスはない。オペレーティング・システムによるこのレベルの制御により、管理レベルでのセキュリティ攻撃がない限り、フィッシャーによる改竄は不可能になる。フィールドが入力されると、データは証明書の公開鍵を使用してオペレーティング・システムによって暗号化されるため、対応する秘密鍵を所有する認定されたデータ受信者のみがデータを読めるようになる。暗号化されたデータは、要求したアプリケーションに提供される。

この特定の信頼できるパスのメカニズムでは、証明書を付与する前に認証局が申請者のIDとロゴを検証する必要がある。信頼できるパスの証明書は、少数の管理された権限者によって発行され、これらの権限者はIDの明確な証明を求め、不正なロゴが使われることのないよう徹底する。信頼できるパスのための信頼できる認証局になるための要件は、少なくともSSL証明書のルート認証局と同程度、おそらくはそれ以上に厳しくする必要がある。または、信頼できるパスにおいて、SSLよりも高いセキュリティのレベルの証明書を求めることもできる。

ロック・アイコンなどの勧告表示要素の確認を求める忠告とは異なり、信頼できるパスを通じてデータ入力画面にたどりつくことは、ユーザのサイトとの積極的な対話の一部である。信頼できるパスのメカニズムを必ず使用して機密情報（パスワード、クレジット・カード番号、ソーシャル・セキュリティ・ナンバーなど）を入力することにユーザが慣れると、信頼できるパスを使用しない機密情報の要求は直ちに危険信号となる。これは、信頼できないサイトへのデータ送信、または機密情報の入力を知らせる検出システムによって増補できる。

信頼できるパスは、フィッシャーがセンシティブな情報を解釈するために、その実際のIDを使用して要求するか、または信頼できるパスのメカニズムを使用せずに要求しなければならなくなるという点から、ステップ4への対抗策になる。ユーザは、信頼できるパスを使用してセンシティブな情報を入力することに慣れている場合、それを提供しない可能性が高い。信頼できるパスはステップ6への対抗策でもある。フィッシャーは証明書を盗み、盗ん

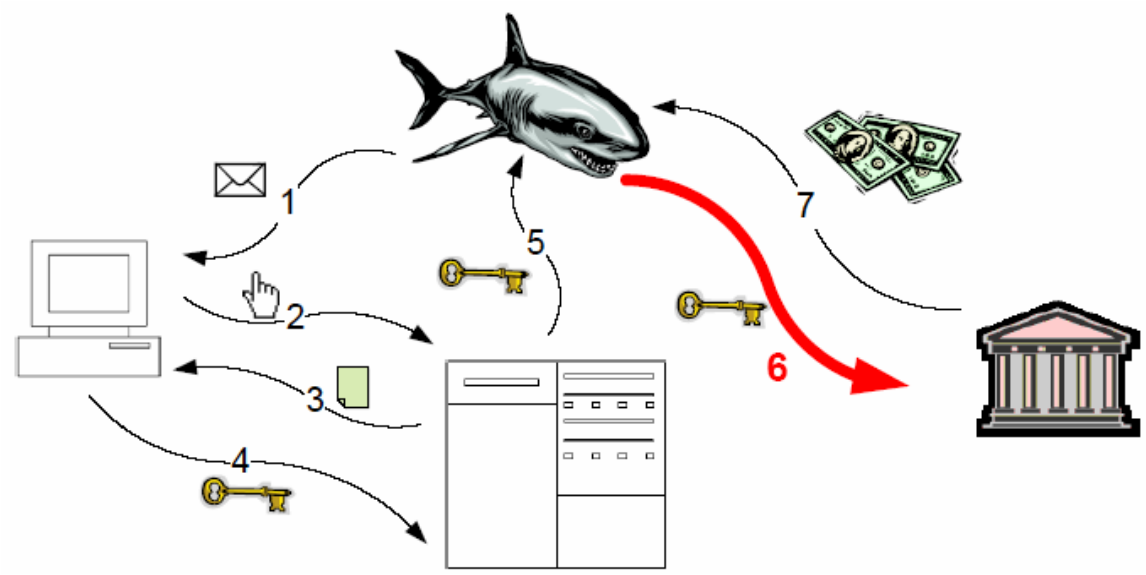
だ証明書を使用してデータを要求できる。しかし、センシティブなデータを複合するために必要な秘密鍵は正規の証明書の所有者のみが持っているため、フィッシャーはデータを解釈できない。
信頼できるパスはアプリケーション・レベルでも実装できる。スタンフォード大学のPwdHashプログラムにおける、パスワード入力のためのセキュア・アテンション・シーケンスとしての「@@」の使用は、アプリケーション・レベルでの信頼できるパスの実装である。ブラウザーに実装された信頼できるパスは、詐欺ベース・フィッシング攻撃とDNSベース・フィッシング攻撃に対する保護を提供できる可能性がある。ユーザ特権マルウェアに対する保護のためには、オペレーティング・システム・レベルでの実装が必要である。



フィッシングにおける情報の流れ、ステップ5

ステップ5：漏洩した認証情報の送信を追跡する

フィッシングにおける情報の流れのステップ5では、漏洩した認証情報がフィッシャーによってフィッシング・サーバまたはその他の収集者から取得される。Web上のトロイの木馬、キーロガー、またはローカル・セッション・ハイジャッキングなどのローカルに実行された攻撃の場合、漏洩した認証情報が取得されるフィッシング「サーバ」は、顧客のコンピュータの場合もある。
フィッシャーは、足跡を覆い、漏洩した情報の最終的な宛先を隠すために、入念な情報の流れを組み立てることがある。これらの情報の流れは、攻撃された「ゾンビ」マシン、インスタント・メッセージ、チャット・チャネル、匿名ピア・ツー・ピア・データ転送メカニズムなど、複数のメディアをまたぐこともある。学術論文では、Usenetへの投稿など公開された通信に情報を挿入できる公開鍵ステガノグラフィーなどの、最終的な証明書の利用者の検出を困難にする技法も提案されている。
一般的に、内密の通信チャネルを防ぐことは非常に難しく、現段階での対抗策は、フィッシャーへのデータの返信に先立ったフィッシング・サーバの撤去や、犯罪者を起訴するための情報の流れの追跡などを中心としたものである。



フィッシングにおける情報の流れ、ステップ6

ステップ6：漏洩情報の使用を妨げる

フィッシング対策としてのもう1つの技術ベースのアプローチは、漏洩情報の価値を下げることである。これは、フィッシングにおける情報の流れのステップ6において、フィッシャーが漏洩情報を不法収益に換えることを妨げるものである。以下の対抗策は、フィッシングの情報の流れのステップ6を攻撃する。

ステップ6への対抗策：従来型の二要素認証

データ漏洩の影響を軽減する最も一般的なアプローチは、*二要素認証*として知られているものである。これは、取引の実行を許可するために、以下の3つの基準のうちの2つの証明を必要とすることを意味する。

- 自分自身（指紋、網膜のスキャンなど網膜のスキャンなど）
- 持っているもの（スマートカード、ドングルなど）
- 知っていること（アカウント名、パスワードなど）

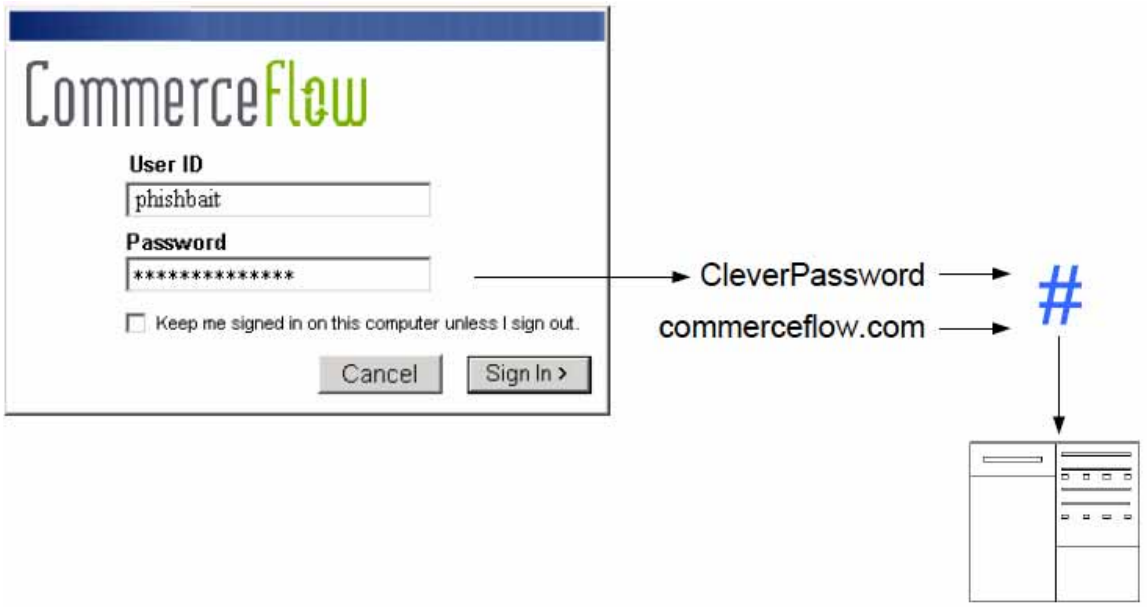
今日のフィッシング攻撃は、ユーザが*知っていること*を漏洩する場合が多い。このような情報はフィッシング攻撃によって容易に漏洩されるため、フィッシングの情報の流れのステップ6は、パスワード・タイプの証明書に加え、ユーザが*持っているもの*またはユーザ*自身*の何かを必要とすることで妨害できる。認証の追加要素は、一般的に「二要素認証」と呼ばれる。二要素認証は、アカウントにアクセスするため、または取引を実行するためのいずれかの目的で求めることができる。二要素認証はあらゆる取引に必要な場合もあれば、下記の*取引の確認*で説明するように、不正取引の可能性が高いと考えられるものにのみ必要なこともある。
米国で最も広く展開されている二要素認証デバイスは、ワンタイム・パスコード（OTP）デバイスである。このようなデバイスでは、定期的な間隔、または使われるたびのいずれかで変わるコードが表示される。ユーザがデバイスを持っていることを示すために、ユーザは、最新のパスコードの入力を求められる。このパスコードは、使われているシーケンスと最新の値を把握しているサーバによって検証される。
OTPは理解しやすく、盗まれた証明書を後で販売するための二次市場を大いに排除できる。しかし、OTPは、OTPが依然として有効な間に経済的損害が生じるようなフィッシング攻撃に対し脆弱である。OTPがフィッシングの情報の流れのステップ4でフィッシャーに渡されたときから、ステップ6で認証情報が使われるまでの間の時間が短い場合（中間者攻撃やセッション・ハイジャッキング攻撃などではこのような状況が考えられる）、フィッシャ

ーはステップ6でOTPを使用できる。
その他の形式の二要素認証には、このような攻撃に対する耐性がある。スマートカードやUSBドングルは、暗号処理を内部で実行し、盗聴者が解釈できないような手法で、認可された相手と直接認証を行うことができる。適切に実装されたバイオメトリック認証システムでは、中間者が最終的なサーバからのチャレンジに対するレスポンスを再利用できないような形で通信チャネルと結び付けられた、チャレンジ・レスポンス・プロトコルを使用する。

ステップ6への対抗策：コンピュータ・ベースの二要素認証
別のハードウェアによる二要素認証デバイスは、効果的な対抗策になる。しかし、購入、展開、サポートが高価であり、一部のもの（スマートカードなど）ではインフラストラクチャーへの恐ろしいほどの投資が必要である。さらに、不便さゆえに、顧客はハードウェアによる二要素認証デバイスの使用に抵抗を示してきた。従来型の二要素認証は、商業銀行のアカウントのような価値の高いターゲットに適しているが、今のところ米国では典型的な消費者アプリケーションにおいては広く展開されていない。
これよりコストが低い二要素認証のアプローチとして、顧客のコンピュータを*持っているもの*の認証要素として使用する方法がある。これは、顧客は自宅または職場の少数のコンピュータのいずれかからオンライン・バンキングを実行することが多いという観察に基づいている。コンピュータ・ベースの二要素認証ではこれらの認可されたコンピュータを顧客のアカウントに登録し、それらの存在を二要素認証に使用する。
これは有効なアプローチであり、ハードウェア・ベースの二要素認証と比べた場合、コストと使いやすさの面でメリットが大きい。しかし、セキュリティ上の考慮事項がいくつかある。まず、認証情報を受け取る際にDNSベース攻撃を避けるために、マシンのID情報は中間者攻撃を受けにくい方法で送信する必要がある。たとえば、ID情報の受信者を認証する特別なソフトウェア・プログラムの使用、またはSSLによって自らの認証を行ったリモート・サイトにのみ送られる安全なcookieの使用などである。
第2に、コンピュータ・ベースの認証は最終的にはローカルで実行されるセッション・ハイジャッキング攻撃またはユーザのコンピュータを使用して取引が行われるその他の攻撃を受けやすい可能性がある。ある意味、悪質なソフトウェアがひとたび顧客のコンピュータで実行されると、そのコンピュータはもはや顧客のものではなくなり、フィッシャーが所有し、認証に使えるものになる。
コンピュータ・ベースの二要素認証の主なセキュリティの問題として、新規のコンピュータの認可、または既存のコンピュータの再認可がある。ユーザは時には外部からのコンピュータまたは新たに取得したコンピュータを使用したり、認可情報が取り除かれた場合にはコンピュータを再認可する必要がある。コンピュータの認可は、ユーザにいくつかの質問に答えてもらったり、2次パスワードを提供してもらうことで行われる場合もある。この情報はフィッシングされる可能性があり、2つ目の*知っていること*要素として、コンピュータ・ベースの認証を1因子認証へと縮小する。
真の2つ目の認証要素であるためには、コンピュータ・ベースの認証は*持っているもの*を使用して新しいコンピュータを認可する必要がある。たとえば、ユーザが新しいコンピュータの認証を要求した場合、ワンタイム・パスコードがユーザの携帯電話に送信される。ユーザはこの情報を特別なプログラムにタイプし、それは適切な宛先に送られる。この場合、ユーザがパスコードを決してWebページには入力しない点が重要である。フィッシングサイトがパスコードを取得し、フィッシング・マシンの認可に使用する可能性があるためである。コンピュータの認可のための*持っているもの*もう1つの形態に、電子メール内のクリック可能な認可リンクがある。このリンクは、リンクをクリックするために使われたIPアドレスにあるコンピュータを認可する。

ステップ6への対抗策：パスワード・ハッシング
パスワードのフィッシングは、フィッシング・サーバに送られたパスワードが、正規のサイトでも有用なものでない限り無駄である。フィッシャーが有用なパスワードを集めるのを防ぐ方法の1つとして、ユーザ・パスワードを使われる場所に依存させてエンコードし、エンコードされたパスワードのみをWebサイトに送信する方法がある。これにより、ユーザは複数のサイトについて同じパスワードをタイプでき、各サイト（フィッシングサイト

も含む）は、個別にエンコードされたバージョンのパスワードを受け取る。このアイデアを実装したものを、パスワード・ハッシングと呼ぶ。パスワード・ハッシングでは、パスワード情報は送信前に送られる先のドメイン・ネームとともにハッシュされるため、実際に送信されたパスワードは、パスワード・データを受信したドメインでのみ使える。パスワード・ハッシングは、最終的には、パスワード・フィールドで自動的に実行される組み込みメカニズムとしてブラウザーで提供できる。オフライン・辞書攻撃を防ぐために、パスワード・ハッシングを使用するサイトは適切なパスワード要件も施行すべきである。パスワード・ハッシングでは、詐欺ベース・フィッシング攻撃で漏洩したパスワード・データが正規のサイトで再利用できないことから、フィッシングの情報の流れのステップ6への対抗策になる。



パスワード・ハッシング

フィッシングに対するセキュリティに加え、パスワード・ハッシングは、サイトからの大規模なパスワード・データの盗難によるフィッシング以外の形態での識別情報の盗難に対する適切な保護も提供する。サイトが平文でのパスワード・データの保管を行わないことと、パスワードが別のサイトでは再利用できないことの両方を保証する。ユーザは複数のサイトで同じパスワードを使用することが多く、あるサイトで盗まれたユーザ名とパスワードが別のサイトで再利用される可能性がある。パスワードが辞書攻撃において想像されにくいものである限り、パスワード・ハッシングは盗まれた認証情報のそのようなサイト間での再利用を防げる。相互認証プロトコルと組み合わせることで、パスワード・ハッシングは、相互認証パスワードを平文で保管する必要性を除去することもできる。

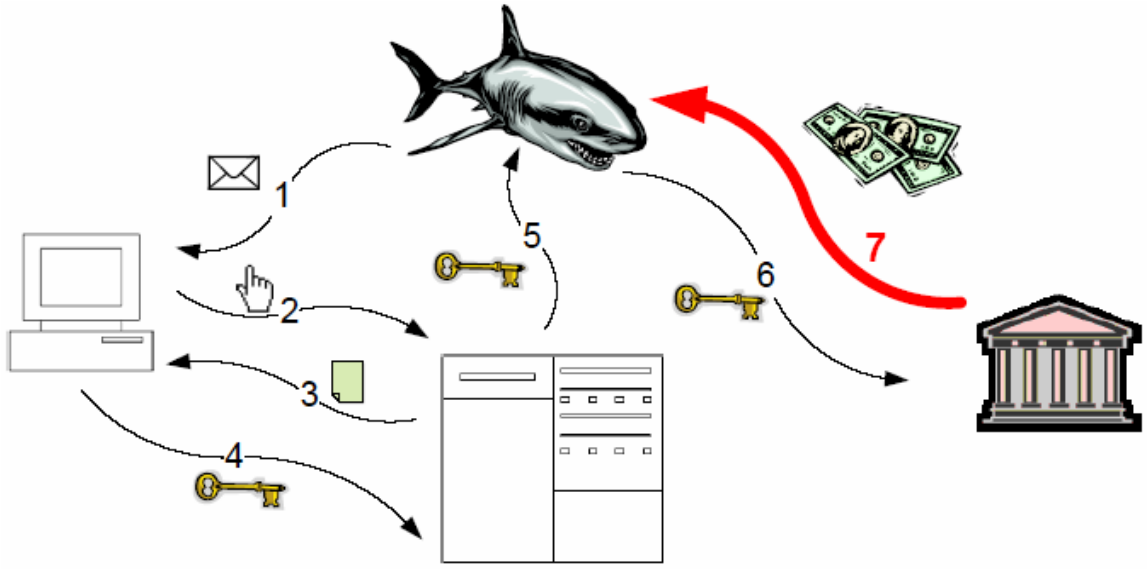
フィッシャーは、パスワードを求めた後にパスワード・ハッシングを行うことはないため、パスワード・ハッシングは単独では詐欺フィッシング攻撃への保護を提供するものではない。したがって、パスワード・ハッシングを施行するために、パスワード入力を他のデータ入力と異なるものにする方法が必要である。前述の信頼できるパスがこの目的に適している。スタンフォード大学のPwdHashプログラムでは「@@」をセキュア・アテンション・シーケンスとして使用し、入力フィールドでパスワード・ハッシングが使われていることを確認する。このセキュア・アテンション・シーケンスはブラウザー・プラグインによって傍受され、プラグインはフォーカスがフィールドから離れるかまたはフォームが送信されるまでパスワード・データをスクリプトから隠す。この時点で、パスワードのハッシュされたバージョンが置き換えられる。

ステップ6への対抗策：取引の確認

フィッシングのリスクを軽減するアプローチの1つに、不正な可能性のあるオンライン取引への集中がある。これは銀行が実社会で実施しているリスク管理対策と似ている。クレジット・カードの取引はすべて評価され、疑わしい取引は顧客に確認が行われる。
オンライン取引の分析は、ユーザのIPアドレス、ユーザのマシン上でのcookieなどの認証情報の存在、取引の量、仕向先の銀行口座、仕向先の銀行口座の特徴、取引パターンの口座間分析など、さまざまな測定基準を使用して実施できる。このような分析は、銀行のオンライン・システムに統合されたソフトウェア、またはWebトラフィックを監視する「アプライアンス」で実施できる。疑わしいとして取引にフラグが立てられると、取引別の認証が顧客に求められる。
批判的に見ると、このような認証はフィッシングされるおそれのあるような「what you know(知っていること)」という質問の形で行うべきではない。強固な形の取引の認証では、電話などの信頼できるデバイスを2つ目の要素として使用する。顧客のものとして知られている番号に電話がかけられたり、SMSメッセージが顧客の携帯電話に送られると、顧客は取引を音声または返信メッセージによって確認できる。確認情報には取引自体の詳細を含めることが重要である。さもなければ、フィッシャーがセッション・ハイジャッキング攻撃を行い、ユーザが確認する取引を変更できてしまうからである。バイオメトリック・デバイスが、信頼できる状態で取引の詳細を表示できる場合、バイオメトリックスも認証に使用できる。
一部の調査によれば、顧客は確認を求められることを予想している場合、詳細をチェックすることなく取引を確認することがある。したがって、このような確認は非常にまれにするか、または確認する取引をユーザが自発的に選択することを求めるユーザ・インターフェイスを使用すべきである。
取引の分析と確認は、適切に実施されれば、管理者特権マルウェアなどのあらゆるタイプのフィッシング詐欺だけでなく、フィッシング以外によるその他の形態の識別情報の盗難におけるステップ6の効果的な軽減になる。100%の保護を提供するものではないが、オンライン取引による損害を大幅に削減できる。銀行はこのメリットを、展開コストと予想されるユーザ経験の混乱と比べて評価すべきである。

ステップ6への対抗策：ポリシー・ベース・データ
ステップ6へのもう1つの対抗策は、データを、どのようにまたは誰が使えるかを決定するポリシーと密接に組み合わせることで、第三者が使えないようにすることである。これはフィッシング攻撃のステップ6への対抗策にとどまらず、ハッキングまたはインサイダー攻撃によるデータ盗難など、フィッシング以外による識別情報の盗難にも適用できる。
この技法は、データを受信し保管するサイトが、データの最終的な利用者ではないような状況に適している。たとえば、電子商取引のサイトやISPでは、ユーザが買い物の支払いまたは繰り返し発生する請求書への支払いに便利に使えるよう、クレジット・カード番号を記録しておく必要がある。しかし、クレジット・カード取引は電子商取引会社またはISPによって行われているわけではない。実際には、支払処理会社が請求に責任を持つ。
サイトではクレジット・カード情報と、そのサイトのみが請求を行えることを定めたポリシーを組み合わせることができる。この組み合わさった情報は、クレジット・カード情報を保管する前に、支払処理会社が所有する公開鍵を使用して暗号化される。この情報は、支払処理会社のみが所有する秘密鍵なしでは復号できない。したがって、データは盗まれても盗難者にとっては役に立たない。社内でデータを保管している人が通常、復号鍵を利用でき、そのような人がわいろを受け取ったり、その他の方法で復号データが漏洩し得るような従来型の暗号化データベース方式とは異なる。
取引の実行時には、暗号化されたクレジット・カード情報が取引の詳細とともに送信される。支払処理会社はこの束を復号し、ポリシーをチェックする。取引がポリシーの下で認可されていない場合、たとえばポリシーではCommerceFlowのみがカードに請求できるとされているのに対し、PhishingEnterprisesが請求をしようとしている場合などは、請求は拒否される。
フィッシングのための対抗策とするためには、これを前述の信頼できるパスのメカニズムと組み合わせることもできる。ポリシーは、フォームに組み込み、指定した入力フィールドと組み合わせ、ID情報を画面上に表示できる指定された鍵で暗号化できる。フィッシャーが何とかサイトの主なデータにアクセスできたり、その他の方法

で情報を漏洩できたとしても、ポリシー・ベースの認証情報は依然としてフィッシャーにとって役に立たない。



フィッシングにおける情報の流れ、ステップ7

ステップ7：金銭上の利益を妨げる

フィッシングにおける情報の流れのステップ7では、ステップ6で漏洩した認証情報を使用して経済的利益が実現する。
金融機関は、フィッシング攻撃に使われている口座を検出するために、特定のタイプの送金に遅れを設けてきた。保留期間中に不正な受取口座が特定されれば、送金は無効にされ、経済的損失が防げる。
ステップ7は捜査当局もかなり関心を持っているステップである。フィッシャーは、盗まれた認証情報の使用による金銭の流れを追跡することで捕らえられることが多い。
フィッシャーは、複数の層によって金銭をフィルタにかけ、匿名の換金手段を使用することが多いものの、最終的にはフィッシャーが金銭を受け取るため、このような流れは追跡できることが多い。

技術以外のベスト・プラクティス

本報告書は、主としてフィッシング防止技術を取り上げたものである。とはいえ、フィッシングの標的になり得るすべての関係者が知っておくべき慣習がいくつかある。

- 自社のブランドに似た最も騙されやすいドメイン・ネームで利用可能なものを登録する。これは最も安価な保険である。
- ドメイン・ネームを商標登録し、一見同じようなドメイン・ネームを登録した関係者に対する償還請求に備える。
- 最近のドメイン登録を監視し、自社のドメイン・ネームと一見同じようなものを登録した関係者に対し、行動を起こす。
- DNSレコードの電子メール認証情報を公開し、顧客とのすべての通信に認証電子メールを使用する。代理でメールを送信してくれる関係者についても適用すべきである。
- 顧客宛のすべての発信メールにデジタル署名をすることを検討する。メール・サーバで実行できない場合は、電子メール・ゲートウェイで行うこともできる。

- 電子メールの慣習に関し、個人情報を決して尋ねない、またはクリック可能なリンクを決して電子メールで提供しないなど、明確なポリシーを確立する。ポリシーは、組織内のすべての利害関係者にとって受け入れられるものにする。自社に代わって電子メールを送信するすべての第三者にポリシーを徹底する。ポリシーを顧客に定期的に伝え、可能であればすべての電子メール通信、印刷物による発表などのその他のメディアでも伝える。
- 顧客への電子メールには必ず個人情報を含める。個人情報とともに、毎回そうすることが自社のポリシーだという教育的な記述を添える。
- その電子メールが本当に自社からのものかを確認するために顧客が電子メールを送れる、spoof@yourcompany.comというような電子メール・アドレスを提供する。フィッシング・メッセージの報告方法に関する明快な指示をWebサイトや自社からの通信に掲載する。
- 顧客との対話に、異常な名前や予期せぬ名前のWebサイトを使用しない。
- 自社のWebサイトがSSLを使用しており、すべての証明書が最新のものであることを確認する。
- 自社サイト上の開かれたURLリダイレクトをすべて取り除く。
- クロスサイトスクリプティングとSQLインジェクションにおいては、受け入れフィルタを使用し、ユーザが提供したデータがすべて厳重にフィルタにかけられるようにする。
- 識別情報の盗難による損失に責任を持ち、フィッシングによる損失から注意が逸れるような他の潜在的損失（不適切な貸出決定など）には責任を持たない上級職を組織内に設ける。
- フィッシング攻撃への対応に責任を持つ部門間タスク・フォースを設立する。参加する人員は上級社員で、迅速な意思決定と実行を行う権限を持つ。責任と手順を明確に描く。「防災訓練」を行い、役割が理解され、伝達が速やかであることを確認する。
- フィッシング攻撃が発生した際に送信する顧客への通信を事前に準備し、攻撃が始まったときに送信が遅れるのを防ぐ。
- 電子メールのバウンス・メッセージ、顧客からの問い合わせの件数、口座の異常な動き、疑わしい画像の使用、フィッシング・グループに関するディスカッションなど、フィッシング攻撃の兆しを監視する。
- フィッシング攻撃が発生したら署名ベースでのチェックを使用する電子メールのフィルタリング会社に直ちに通知し、フィッシング電子メールの例を提供する。これらの会社では、意図する受信者への多くの電子メールをブロックするルールを展開できる可能性がある。
- フィッシング攻撃が確認されたら捜査当局に直ちに知らせる（付録B参照）。
- フィッシング攻撃が確認されたら、Webサイトに警告を掲示し、電子メールで顧客に攻撃について知らせることを検討する。
- フィッシング・サーバを追跡し、できる限り早くシャットダウンする。この作業を支援できるサービス・プロバイダーもある。
- 大規模なフィッシング攻撃が確認されたら、顧客サービスのスタッフを増やす。
- フィッシャーを後で起訴できるよう、フィッシング攻撃の証拠を保存する。
- 第三者には、前述の慣習に反して代わりに行動をとれるような権限は与えない。

結論

フィッシングを完全に阻止できるような単一の技術はない。しかし、適切な組織と慣習、最新の技術の正しい適用、セキュリティ技術の改善などの組み合わせにより、フィッシングの普及とそれによる損失は劇的に軽減される可能性がある。特に重要なのは次のような点である。

- 価値の高いターゲットはベスト・プラクティスに従い、それらの継続的な発展について確認し続ける。
- フィッシング攻撃は、顧客の報告、バウンスの監視、画像の使用の監視、ハニーポット、管理者による行動への警告、およびその他の技法の組み合わせによって迅速に検出できる。

- Sender-IDや暗号署名などの電子メール認証技術は、幅広く展開されれば、フィッシング電子メールがユーザに届くのを防げる可能性がある。
- 画像(imagery)の分析は、フィッシング電子メールの特定について将来研究が期待される分野である。
- 暗号化されたパッチは、マルウェアの作成者にセキュリティの脆弱性を知られるのを防ぎ、脅威への迅速な対応を自動化できる。
- 個人情報はすべての電子メール通信に含めるべきである。ユーザがカスタマイズされたテキストおよび／または画像を入力または選択できるシステムは特に有望である。
- 潜在的詐欺コンテンツの表示や、安全でない可能性のあるリンクを選択した際の警告などのブラウザーのセキュリティのアップグレードは、フィッシング攻撃の有効性を大いに削減できる。
- 不正なDNS情報の検出は、有望な検討分野である。
- フィッシング攻撃に関与するコンポーネント（スパム・フィルタ、電子メール・クライアント、およびブラウザー）間での情報共有は、フィッシング・メッセージおよびフィッシングサイトの特定を改善し、疑わしいコンテンツとの危険な行動を制限できる。
- コンテンツインジェクション攻撃は拡大中の問題である。ユーザのコンテンツはすべて受け入れフィルタを使用してフィルタにかけるべきである。ブラウザーのセキュリティ強化により、クロスサイトスクリプティング攻撃が発生する可能性を小さくできる。
- フィッシング防止ツールバーは、フィッシングサイトの特定と、フィッシングサイトと思われるサイトが検出された際にセキュリティを強化するための有望なツールである。
- パスワード・ハッシングなどによるドメインごとの証明書の変更は、識別情報の盗難に対する強力な対抗策であり、信頼できるパスと組み合わせれば非常に効果的なフィッシング防止策になる。
- データの安全な入力と送信のためのOSレベルでの信頼できるパスは、不正な相手への機密データの漏洩を劇的に削減できる可能性がある。
- ハードウェア・ベースの二要素認証は、フィッシングに対して極めて有効だが、一部のアプローチは短期間でのフィッシング攻撃に遭いやすいため、価値の高いターゲットでの少数のユーザが関与する状況で推奨される。
- コンピュータ・ベースの二要素認証は、適切なセキュリティ面での特徴と低い展開コストを提供するが、特定のタイプのマルウェア攻撃を受けやすい。新しいコンピュータをどのように認可するかが、セキュリティ設計における重要な検討事項になる。
- アウト・オブ・バンドの通信チャネル経由での取引の確認は、マルウェアへの耐性のある強力な技法である。
- 可能な限り、データはフィッシャーによる使用を防ぐポリシー・ステートメントと組み合わせ、下流のデータ利用者の公開鍵で暗号化するべきである。これにより、漏洩データの不正使用が防げる。
- 捜査当局が役立てられるようなログを保管し、損失を定量化できるようにしていれば、捜査当局の対応をより効果的なものにできる。