フィッシング詐欺の脅威

Sophos White Paper
August 2005

このホワイトペーパーは、フィッシング詐欺と呼ばれるオンライン不正行為について、昨今の急激な増加の状況と脅威について説明します。フィッシング詐欺の手口を紹介し、フィッシング詐欺から企業のコンピュータ環境を保護する方法について解説します。

フィッシング詐欺とは

フィッシング詐欺とは、近年急激に増加しているオンライン詐欺行為のことをいいます。電子メールを使って偽の Web サイトにユーザーを誘導し、オンラインで個人情報を盗むなどの行為を行います。『フィッシング (phishing)』は魚釣り (fishing) に由来したハッカー用語で、偽の電子メールと Web サイトを使って『餌』とみなされる犠牲者を釣り上げるところからきています。まず金融機関などの実在の有名企業が発信者であるかのように見せかけた電子メールがユーザーに送信されます。メールの内容は決まっていませんが、多くの場合、受信者がリンク先にアクセスすると個人情報を入力するフォームが表示される形態をとります。ここで表示されるフォームはフィッシングの発信元であるフィッシャーが作成した偽ページですが本物そっくりに作られているため、簡単に見破ることはできません。

フィッシング詐欺で送信される電子メールのほとんどは無視されますが、フィッシャーは少数の被害者から大きな利益をあげています。

フィッシャーは、送りつけた電子メールのほとんどが無視されてしまうことを前提として「数打てば当たる」方式で大量の電子メールを発信します。実際、数パーセント程度の犠牲者をみつけることができさえすれば、フィッシングサイトを立ち上げているほんの短期間に大きな利益をあげられます(フィッシングサイトはほんの 2〜3 週間しか存在しません)。Web サイトの立ち上げと大量の電子メール発信にさほどの費用がかからないことを考えても、少数の被害者から大きな成果を得ていることがわかります。フィッシング詐欺対策の業界団体である Anti-Phishing Working Group (APWG) によると、フィッシャーは 5% 以内の成功率で十分な利益を得られるといいます。

世界に拡がる被害

ひとたび個人情報を獲得すると、フィッシャーはそれを好きなように活用します。通常は盗まれた個人情報に直接関連している銀行口座などを解約すればそれ以上の被害を防ぐことができますが、それだけにとどまらず、窃盗された個人情報で新たに口座を作成されてしまったり、他のネットワークに侵入する際に利用されてしまうなど、被害が拡大することもあります。

フィッシング詐欺は世界各地で詐欺行為が行われるため、国によっては海外送金が簡単にはできないことがありますが、そのような場合でも、フィッシャーが海外送金の資格を持つ人を『運び屋』として利用することがあります。ソフォスの調査によると、ビジネスチャンスを餌にフィッシャーにだまされ、送金に荷担してしまった人々の例が実際に報告されています。[1]

ビジネスの脅威となるフィッシング詐欺

フィッシング詐欺は今日のビジネス環境で多様化･複雑化し、多発しているセキュリティ脅威のひとつです。スパム送信者の手法は洗練を重ねています。スパムはマルウェア(悪意のあるソフトウェア) と結びつき、オンライン不正行為や窃盗のツール、または悪質なプログラムの拡散に使用されています。

フィッシング詐欺は電子メールを使ったネットワーク脅威のひとつです。

実際に、フィッシャーがマルウェアを活用した例も数多く存在します。ソフォスの調査によると、ブラジルではコンピュータ上にトロイの木馬をインストールさせた疑いで 53 名が逮捕された例が報告されています。このトロイの木馬はバックグラウンドで動作してユーザーのオンライン アクセスをモニタリングし、特定のオンライン バンキング サイトにアクセスすると、ユーザーの詳細なログインデータをフィッ

この文書は、2005 年 5 月にソフォスから発行された『Phishing and the threat to corporate networks』を翻訳し、編集したものです。

シャーに密かに送信するというものでした。[2] これはフィッシングサイトを使用しないフィッシング詐欺の例で、最初にスパムを使ったマルウェアのインストールに成功した時点で、詐欺が成立してしまっています。

その他にもフィッシング詐欺の手口はたくさん存在します。やはりブラジルで発覚した例では、ユーザーがインターネット ブラウザのアドレス バーにオンライン バンクの正しい URL を入力しても、自動的にフィッシャーのフィッシングサイトに接続させてしまうトロイの木馬が使用されていました。[3]

つまりフィッシング詐欺はネットワーク環境での深刻なセキュリティ脅威になり得ると同時に、今後も次々に新手の複雑な手口が発生していくと考えられています。スパム、マルウェア、その他あらゆるコンピュータ犯罪と同様、フィッシング詐欺もビジネスに対する大きな脅威となっています。

フィッシング詐欺は通常一般消費者をターゲットに行われますが、専門の IT 部門を持たない中小企業にとっても大きなリスクとなっています。大企業がスパムの被害者となるケースはあまり見られませんが、すべての企業内のコンピュータ環境と従業員は、このような不正行為から保護されなければなりません。

そのためには、企業のゲートウェイをフィッシング攻撃その他の電子メール ベースのセキュリティ脅威から保護する統合的で堅牢なソリューションの導入が絶対に必要です。

急増するフィッシング被害

フィッシング詐欺の発生数は劇的に増加しています。APWG によると、フィッシング被害の報告数は 2003 年 11 月から 2004 年 5 月までの半年間に 40 倍にもふくれあがったといいます。また、Gartner の 2004 年 5 月のレポートでは、過去 1 年間に少なくとも 180 万人の一般消費者がフィッシング詐欺の被害にあったと報告されています。[4] IDC は 2004 年 10 月のレポートで、アジア太平洋地域で最も増加率の高い非暴力犯罪のひとつにフィッシング詐欺を挙げています。[5]

フィッシング脅威への対策

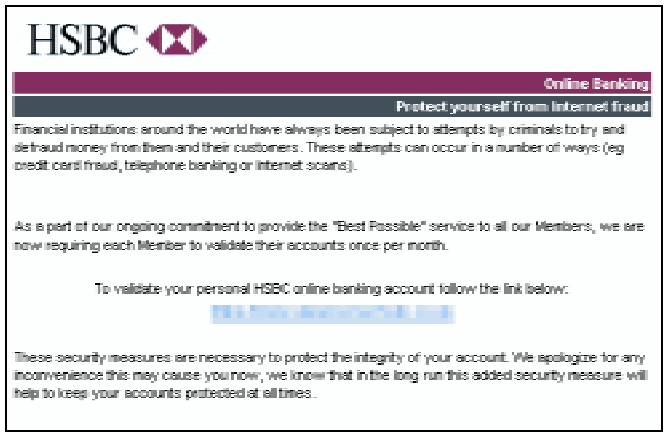
企業の IT 環境や個人の PC をフィッシング攻撃から防御する方法はいくつか考えられます。重要なオンライン アカウントの扱いには特に慎重さが必要です。

機密情報を要求する電子メールには回答しない。

銀行をはじめとする信頼できる企業が、ユーザーに電子メールでパスワードや個人情報を問い合わせることは絶対にありません。たとえ電子メールの内容が理にかなっていると思われる場合でも、決してそのまま返信せず、電話で問い合わせるか、企業の正当な Web サイトにアクセスして内容をよく確認しなくてはなりません。たとえ過去に受け取ったことがあるものと同じように見えるファイルでも、添付ファイルを開いたり Web からファイルをダウンロードする際には十分な注意が必要です。

> ***懸賞当選、あるいはユーザーの ID が不正使用されているとの警告メールを送りつけるなど、フィッシャーは手の込んだ方法でユーザーをつりあげます。***

ユーザーを騙すためにあらゆるテクニックが駆使されています。たとえば添付ファイルやダウンロードドキュメントには、当該企業が通常使用しているロゴ、フォント、レイアウトなどが使われていて、慎重なユーザーでも簡単には真偽を判別することができません。実際に、20万人に電子メールを送付してテストを行ったところ、フィッシング メッセージと正当なメールを見分けることができたユーザーは 10% に満たなかったという結果がでています。6


HSBC

Online Banking

Protect yourself from Internet fraud

Financial institutions around the world have always been subject to attempts by criminals to try and defraud money from them and their customers. These attempts can occur in a number of ways (eg credit card fraud, telephone banking or Internet scams).

As a part of our ongoing commitment to provide the "Best Possible" service to all our Members, we are now requiring each Member to validate their accounts once per month.

To validate your personal HSBC online banking account follow the link below:

These security measures are necessary to protect the integrity of your account. We apologize for any inconvenience this may cause you now, we know that in the long run this added security measure will help to keep your accounts protected at all times.

図 1 HSBC の顧客に送付されたフィッシング メールの一部

銀行やオンラインショッピング等の Web サイトにアクセスする際は電子メールに記載されているリンクから直接アクセスせず、アドレス バーに正確な URL を入力する。

企業が情報発信している顧客向けの電子メールには、ニュース記事や製品カタログ ページなどのリンクが添付されています。気をつけなければいけないのは、フィッシャーは必ず個人情報を要求するという点です。銀行やオンライン サービス プロバイダからの電子メールに疑わしい点がある場合には、決してリンクをそのままクリックせず、ブラウザのアドレス バーに URL を正確に入力してください。フィッシング詐欺では、クリック操作でフィッシャーのサイトに誘導するよう、さま

ざまなトリックが用いられているからです。

最も単純なフィッシング詐欺の例では正当なアドレスに似た URL が使用されます (ハイフンやドットを加えたり、ドメイン名を変えしたりします)。その他、本物のサイトそっくりに構成されたフィッシングサイトが表示されることもあります。一般的な HTML コードで簡単にリンク先を隠せるため、HTML 形式の電子メールを使えば非常に簡単にフィッシングサイトに誘導できます。

テキスト形式の電子メールでは URL の最初の部分だけをブラウザのアドレス バーに表示するように調整することができます。たとえば本物の企業のアドレスで始まる無意味な文字の羅列をつづけ、末尾にフィッシングサイトへのリンクをつけて誘導する手口があります。

上記の手口に対してはすでに 2004 年 2 月にマイクロソフトから重大なアップデートが提供されていますが、パッチが適用されていない環境には脆弱性が残っています。また、Mozilla ブラウザでも、パッチが適用されていない場合にはフィッシングサイトにアクセスした際にアドレス バーに本物の URL が表示されてしまう脆弱性があります。[7] フィッシング詐欺の被害を防ぐためには常にアップデートを適用しなければなりませんが、それでもフィッシャーに攻撃の余地が残されていないと言い切ることはできません。

アクセス中の Web サイトのセキュリティ レベルと正当性を検証する。

銀行口座情報その他の機密情報をインターネットで送信してしまう前に、目視で確認できることがいくつかあります。たとえば、アクセスしているページに、機密情報を送信するにふさわしい暗号機能が採用されているかどうかは以下で確認できます。

- アドレス バーに表示されている Web アドレスを確認する。SSL 認証されているセキュアなページであれば、ヘッダに “https://” と記載されています (通常は “http://”)
- ブラウザのステイタス バーを確認する。アイコンにカーソルをあわせると暗号化のレベルに応じたビット数が表示されます。

しかし、これらはあくまでもデータ転送の暗号ステイタスを示すもので、Web サイトが偽でないことを示すものではありません。フィッシング サイトが本物のセキュアなサーバーとまったく同じように設定されている可能性もあります。

その他の手段として、アドレス バーに表示されている URL と実際にアクセスしている Web サイトの URL が一致するかをプロパティで確認することもできます。Microsoft Internet Explorer の場合、Web サイト上でマウスを右クリックして「プロパティ」を選択するとポップアップ ウィンドウに実際のアドレスが表示され、アドレス バーに表示されている URL と比較できます。両方が完全に一致するかどうかを確認することで、フィッシング詐欺でよく使われるアドレス詐称のトリックを防ぐことができます。このトリックは、ブラウザで本物の正当な Web サイトを表示しつつ、ポップアップ ウィンドウでフィッシャーのサイトを表示し、ユーザーの個人情報を入力させる手口です。ここでデータを入力するとポップアップ ウィンドウだけがクローズするので、ユーザーはデータを盗まれたことにまったく気づきません。

アカウントを定期的にチェックする。

定期的にオンライン アカウントにログインして表示される内容を確認してください。少しでも怪しいトランザクションを発見した場合は、すみやかに取引先の企業に確認してください。

アクセスしている Web サイトのセキュリティ レベルを判断する方法はいくつかあります。

電子メールと機密情報を慎重に扱う。

銀行や企業の Web サイトにはセキュリティに関するページが設けられており、安全な処理を行うための情報や機密情報の扱いに関するガイドラインなどが記載されています。

PIN やパスワードを他人に教えたり書き留めたり、複数のオンライン アカウントに同一のパスワードを使ったりすることは避けてください。また、スパム メッセージへの返信も厳禁です。返信することで、そのアドレスが実際に使用されていることがわかってしまうからです。電子メールは常識的な範囲で使用してください。あやしい話やうますぎる話は危険です。

疑わしきはすべて報告する。

疑わしい電子メールを受信した場合には必ず送信元と思われる企業に確認してください。不正行為の報告をうけるための専用の電子メールアドレスを準備している企業もあります。世界的に、オンライン犯罪に対する法律も整備も進んでおり、英国、ブラジルなどの国々ではすでにフィッシング詐欺への法律が制定されています。オーストラリアでは、数百万ドルを窃盗した電子メール犯罪者に対して懲役 5 年が宣告されました。[8]

常にコンピュータのセキュリティを確保

フィッシング攻撃にしばしば使われるトロイの木馬は、コンピュータやネットワークへの攻撃の門戸を開ける役割を務めます。これを防ぐためにはパーソナル ファイアウォールのインストールも有効です。また、OS を常にアップデートして最新のセキュリティパッチを適用することも、既知のフィッシング詐欺の手口には有効です。前述のトロイの木馬や URL 詐称などにはすでにアップデートが提供されています。しかし、ファイアウォールやパッチ適用ではユーザー自身が騙されてフィッシングサイトに個人情報を入力してしまうことまでは防御できませんし、セキュリティ対策の裏を書いて続々と現れる新手のフィッシング攻撃に対しても無力です。

その他の有効な対策として、認証技術があります。例として SPF (Sender Policy Framework) があげられます。SPF 機関はあらかじめ許可され登録された電子メール送信者リストを保持します。電子メールが受信されると送信元が検証され、『認証済』のリストにない場合は、詐称メールとして受信が拒否されます。現時点では、 SPF などの送信者認証は最新の技術で、フィッシャーは『未認証』のサーバーからしか電子メールを発信できないため、フィッシング詐欺の防御には効果的です。認証による防御の問題点は、送信者のアドレスが詐称されていないことや、送信元のドメインがスパム送信者に使用されていない信頼できるドメインであることを受信者が検証しなければならない点です。

急速に拡大するフィッシング詐欺をはじめとする多様なセキュリティ攻撃から企業を保護するためには、24 時間対応のグローバルなウイルス/スパム対策のセキュリティ ソリューションの採用が必須です。統合的なセキュリティ ゲートウェイ ソリューションの導入は、セキュリティ脅威から企業のビジネスを保護する最も効率的な方法です。

Sophos PureMessage は、各種アワードを受賞しているウイルス対策ソリューションです。ウイルス、スパム、フィッシング攻撃に使われるトロイの木馬などから電子メール ゲートウェイを保護します。企業のセキュリティ ポリシーを遵守して、マルウェアの攻撃から企業を守り、生産性を向上させます。簡単な使いやすい管理ツール、24 時間テクニカル サポートが全ライセンスに含まれます。世界中のソフォスのウイルスラボが常時、新種ウイルス脅威に迅速に対応してアップデートを提供して企業をセキュリティ脅威から保護します。PureMessage の詳細につきましては、ソフォスのサイト (www.sophos.co.jp) をご参照ください。

参考

1. www.sophos.com/spaminfo/articles/phishrecruit.html ["Phishers recruit UK computer users into stealing money, 'Don't be a mule' says Sophos," 2004 年 11 月 3 日].
2. www.sophos.com/virusinfo/articles/brazilarrest.html ["53 arrests as Brazil cracks down on phishing Trojan authors, Sophos comments on online bank fraud," 2004 年 10 月 21 日].
3. msnbc.msn.com/id/6416723 ["A new, more sneaky phishing attack". By Bob Sullivan, 2004 年 11 月 5 日].
4. "increased Phishing and Online Attacks Cause Dip in Counsumer Confidence" By Avivah Litan, Gartner, 2002 年 6 月 22 日].
5. www.idc.com/getdoc.jsp?containerId=AP223108L ["Security Threats in Asia/Pacific (Excluding Japan) 2004 年"].
6. www.informationweek.com/showArticle.jhtml?articleID=48800408 [Deceptive E-Mail Could Cost Consumers $500 Million, Study Finds". By Thomas Claburn, 2004 年 9 月 30 日].
7. www.millersmiles.co.uk/identitytheft/phishing.html ["Spoof Email Phishing Scams and Fake Web Pages or Sites". By Mat Bright, 2004 年 2 月 23 日].
8. www.sophos.com/spaminfo/articles/marinellis.html ["Email scammer who stole over £2 million sent to jail, Sophos reports," 2004 年 11 月 8 日].

その他

APWG (Anti-Phishing Working Group) は、増大するフィッシング詐欺の被害に対応してフィッシャーの特定とフィッシング詐欺の撲滅にフォーカスした業界団体です。詳細については APWG のホームページをご参照ください。(www.antiphishing.org)

ソフォス株式会社
〒231-0062　神奈川県横浜市中区桜木町1-1-8 日石横浜ビル15F
Tel. 045-227-1800　　E-mail. sales@sophos.co.jp