フィッシング対策協議会

月次報告書（２００５年８月分）

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

２００５年9月２０日

目次

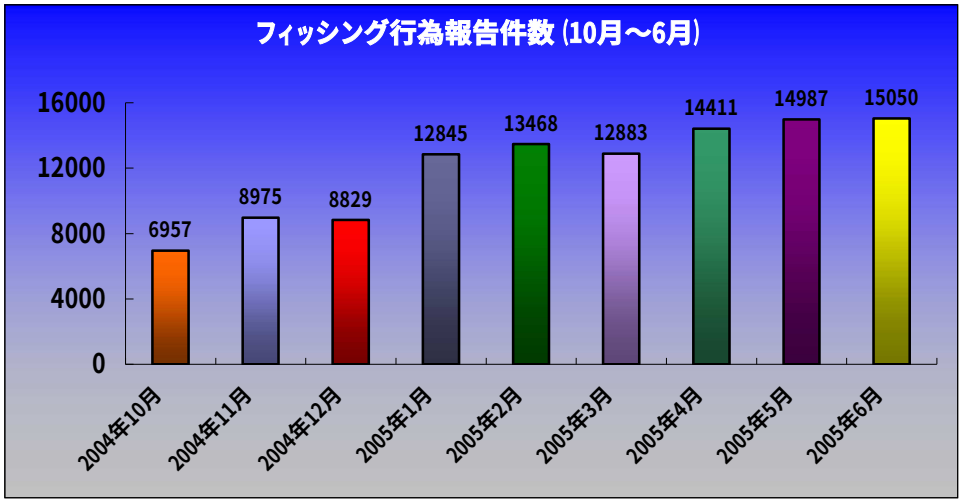
1. APWG Phishing Activity Trends Report 2005年 6月　日本語版

『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

・6 月期のフィッシングに関する報告件数	:	15,050
・6 月中にフィッシングによりハイジャックされた商標数	:	74
・6 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	:	5
・6 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	:	46%
・ＩＰアドレスのみでホストネームなし	:	41%
・ポート 80 を使用しないサイトの割合	:	8%
・サイトのオンライン上の平均残存期間	:	5.9 日間
・サイトの最長オンライン残存期間	:	30 日間



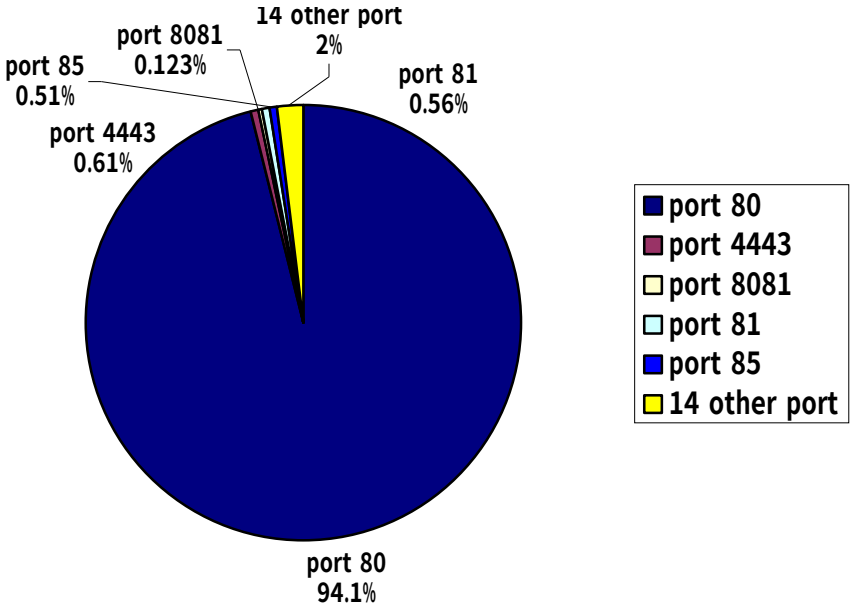
フィッシング行為報告件数（月単位／2004 年 10 月～2005 年 6 月）

『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

6 月期はフィッシング用ホスト・サイトにカズン（類似）ドメイン名を使用する傾向が続きました。その結果、代替ポートの使用は減少し、標準的なＨＴＴＰポート 80 の使用が報告を受けた全フィッシング・サイトの 94.1%に上りました。

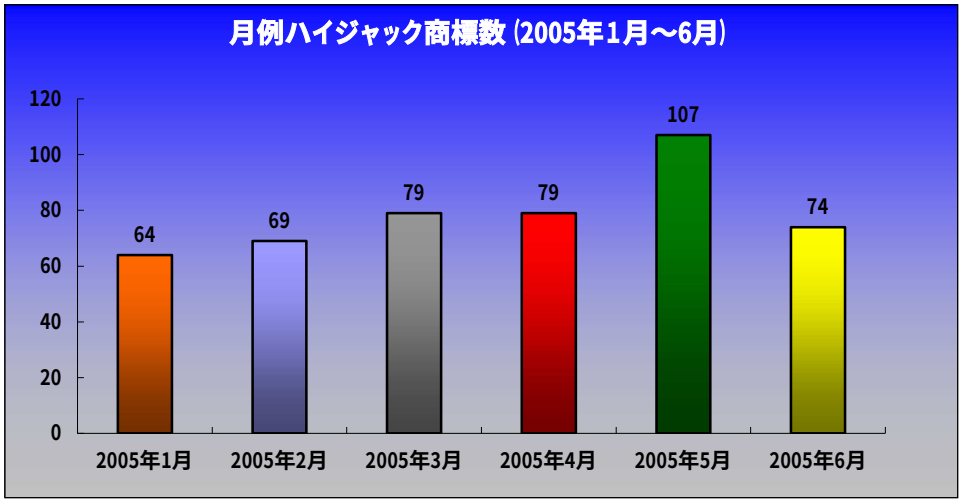


フィッシング・サイトとして最も使用された HTTP ポート

1.3. 【Brands and 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

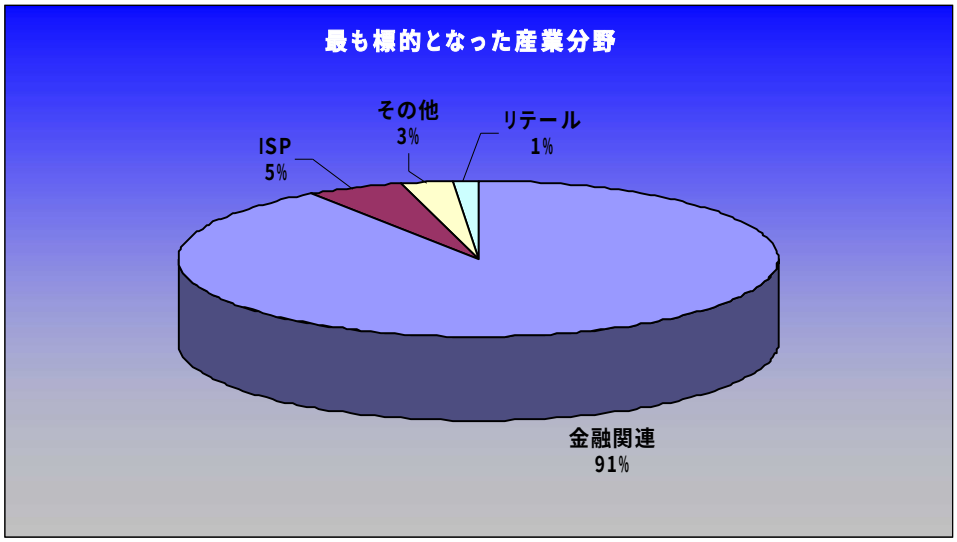
6 月期にフィッシング被害を被った商標の報告件数は 4 月期と比して減少し、それ以前の月例報告数とだいたい同数に留まりました。



ハイジャック商標数（2005 年 1 月～6 月）

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

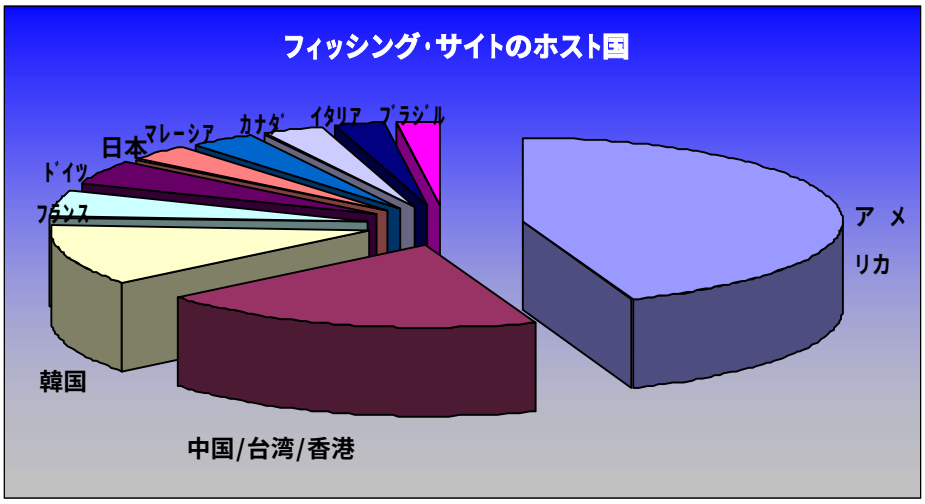
金融サービス分野が最もフィッシングの標的となった産業分野であり、全攻撃の 91%に上るまで増加しました。



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

6 月期 Websense Security Labs は、中国がホスト国であるフィッシング・サイト数の激減を確認しました。アメリカは全フィッシング・サイトの 35.5%のホストとなり依然として第一位に留まりました。トップ 10 のその他は、中国 11.2%、韓国 10.1%、フランス 5.6%、ドイツ 3.2%、カナダ 2.8%、日本 2.4%、イタリア 1.76%、ルーマニア 1.72%、オランダ 1.65%でした。



フィッシング・サイトのホスト国

攻撃方法最新事情

プロジェクト：クライムウェア

2004 年前期以来 APWG は犯罪者達が消費者の個人情報を盗み出すためにユーザーに疑いを抱かせないように攻撃を仕掛ける手法が世界規模で技術的な進歩を遂げていることを認めてきました。ソーシャル・エンジニアリングによる E メールのおびき寄せやウェブサイトの偽造が最も顕著なフィッシングのテクニックですが、それらに代わる方法として直接的な偽装を用いずに消費者のオンライン信用情報を取り込んだりアカウントのコントロールを奪うという手法が増加傾向にあります。（APWG が確認したところでは、ブラジルでの典型的なフィッシングの手法は実際のところソーシャル・エンジニアリングと技術的な偽装の併用です。キーロガー（入力操作監視誘導）を植え付けるために大衆を一般的な娯楽サイトに導くというような純粋にソーシャル・エンジニアリングの枠に納まる手法に比して明らかに効果があがるような手法を用いていることが警察により逮捕に至った過去数年のブラジルにおけるフィッシング犯についての報告などから確認できます。これにより一度に数十万、数百万件を超える被害が出ます。）

過去 18 ヵ月間にトロイの木馬系及びセッションのハイジャックを行う自動化されたシステムについての報告が世界各地でありますが、この３ヵ月はこの傾向が特に顕著になってきており、今後世界的規模で自動化されたフィッシング・システムによるフィッシング犯罪の体系が構築されていくであろうとの APWG の見解に沿ったものとなっています。

更に、PandaLabs はトロイの木馬タイプのフィッシング・システムの中でも従来のフィッシングと比して犯罪道具として最大の優位性を持つ「Trj/Bancos」の使用を検知しました。NL に何千もの商標保有者のドメインを含み、広範囲に及ぶ消費者信用情報の獲得のためのフィッシング技術の革新を示しています。この PandaLabs による発見は、一般的なキーロガーで発揮できる効力を総ての潜在的な信用情報ターゲットに対して実効させようとするフィッシング犯の衝動を示しています。

APWG の観測では、フィッシング犯達は今後技術面の改新によりソーシャル・エンジニアリングを補完し、またはそれに取って代わる、より自動化された攻撃システムを採用していくでしょう。このような傾向の研究報告を目的として APWG は「プロジェクト：クライムウェア」を立ち上げました。これは新たに出現した事例または今後出現しつつある事例を捉え記録する協同研究プログラムであり、APWG はこの研究成果及び可能であれば「クライムウェア」によってもたらされる脅威についての他の関連報告を月例報告に盛り込んでいきます。

ここで APWG が定義する「クライムウェア」とは、アドウェア、スパイウェアやマルウェアとは区別される技術上の分類であり、これはそのプログラムの設計上、金融（または企業）犯罪を活性化させるという唯一の目的のために開発されたものを指します。

「クライムウェア」分類詳細

「プロジェクト：クライムウェア」は、月例報告においてクライムウェアによる攻撃の区分体系を整理分類して報告します。

「フィッシング用トロイの木馬－キーロガー」

（定義）エンドユーザーの個人情報をこれらのユーザーの信用証明を奪う目的で収集することを意図して設計されたクライムウェアのコード。ほとんどの一般的なキーロガーとは異なり、フィッシングを目的としたキーロガーの場合、普通には金融機関、Ｅコマースやウェブをベースとしたメールサイトへのアクセスによる特定の情報獲得を目的とした特定の入力操作（そして特定の組織、最も重要なのは金融機関、オンライン小売業者、Ｅコマース商社）のみをモニターしようとする追跡モニター・コンポーネントを備える。

「フィッシング用トロイの木馬－リディレクター」

（定義）エンドユーザーをネットワーク上で本来意図されていない場所に誘い出すことを目的として設計されたクライムウェアのコードです。これにはホスト・ファイルや他のＤＮＳ特有の情報を改ざんするようなクライムウェア、詐欺サイトへ情報を誘導するようなブラウザー・ヘルパー、詐欺地点への誘導を行うネットワーク・レベルでのドライバーやフィルターのインストールを行うクライムウェアを含む。これらは全て個人のアイデンティティー情報の窃盗あるいはその他の信用証明の犯罪目的での獲得という、情報窃盗を意図してインストールされる。

「人為仲介フィッシング（ファーミング）」

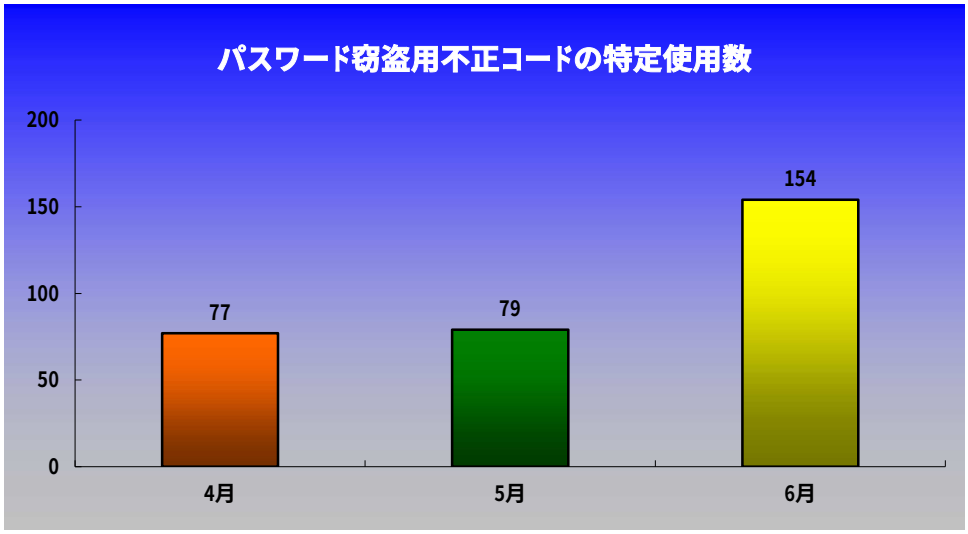
（定義）二者間のコミュニケーションにおける情報の流れを妨害することによりユーザーを詐欺地点に誘導しようとするもので、最も一般的な攻撃形態はＤＮＳキャッシュ汚染。

その他

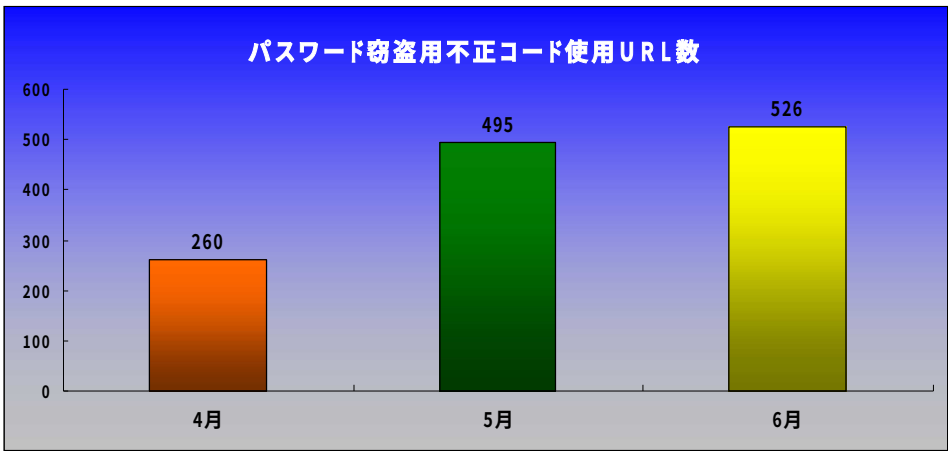
この欄は他の攻撃クラスに該当しない全ての攻撃形態について報告するものですが、新型の攻撃形態が頻繁に実行されるようになった場合は新項目を設定します。これに属する最近の事例には次のものがあります。

- タイポ攻撃： 人気のあるドメイン名の入力をミスタイプさせることによりクライムウェアに感染させる。
- サーチエンジン汚染： 単純にサーチエンジンを用いて検索を行うことにより個人のマシンにクライムウェアをダウンロードさせる詐欺用ウェブサイトに誘導する。

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)

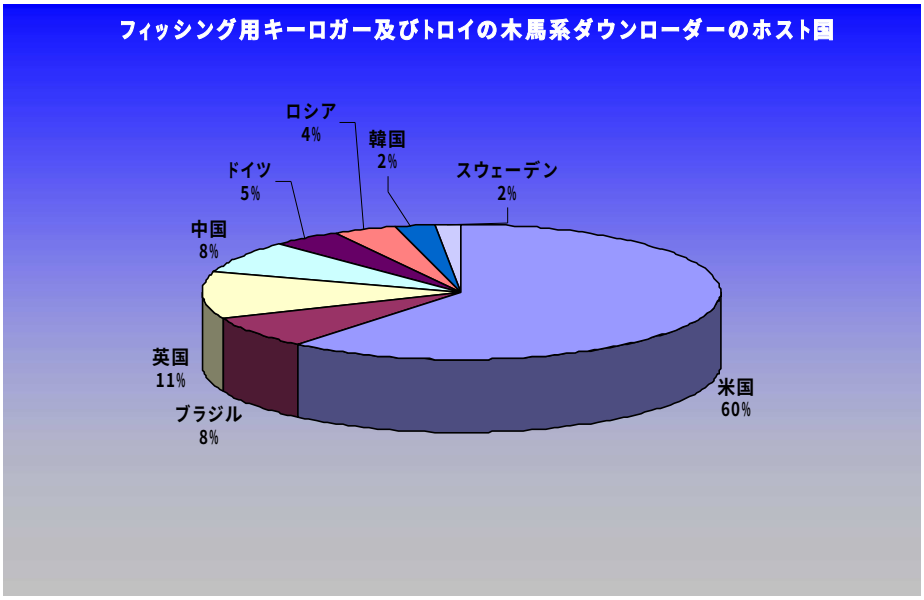


フィッシング用トロイの木馬とダウンローダーのホスト国 (IP アドレスによる)

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 6 月中に分類されたウェブサイトの内訳を示すものです。

興味深いのは、米国は依然として地理的所在地のトップで 55%以上を占めますが、ブラジルが第 3 位で 7 %近くに上ることです。現時点でブラジルは依然としてブラジルの金融機関をターゲットとしたポルトガル語で書かれた詐欺技術を用いたフィッシング用キーロガーの最も高い集積率を示しています。また、通常のフィッシング用ウェブサイトと異なり、一般的にコンプロマイズド（中間）マシンがホストとなるウェブサイトではありません。それらは自由にホスティングを実行する ISP やブログまたはパーソナル・ストレージがホストとなります。

その他の内訳は以下の様です。イギリス 10%、中国 7%、ドイツ 4.2%、ロシア 3.5%、韓国 2.2%、スウェーデン 1.5%でした。



メディアからのお問い合わせは、 Ronnie Manning, manning@websense.com または 858-320-9274 または、Peter Cassidy, APWG 事務局長　617-669-1123　までどうぞ。

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。