Phishing Activity Trends Report

Q1/2008

APWG

Committed to Wiping Out
Internet Scams and Fraud

January – March 2008

Phishing Report Scope

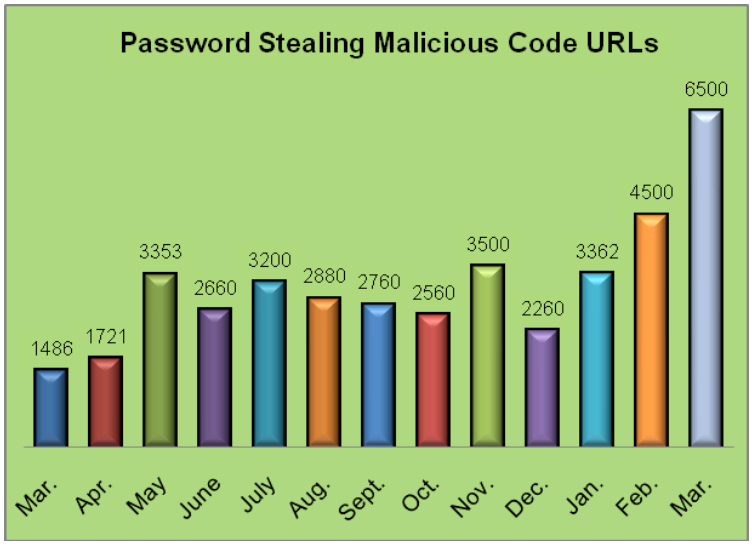
The quarterly *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, Global Research Partners, the organization's website at http://www.antiphishing.org and by email submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation and propagation of crimeware drawing from the research of our member companies. In the last half of this report you will find tabulations of crimeware statistics.

Phishing Defined

Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical-subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords - and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Crimeware-Spreading URLs Rise Swiftly in Q1, 2008 – Nearly Doubling Previous High



Numbers of crimeware-spreading URLs infecting PCs with password-stealing code rose 93 percent in Q1, 2008 to 6,500 sites, nearly double the previous high of November, 2007 - and an increase of 337 percent from the number detected end of Q1, 2007. Details on page 8.

Q1 2008 Phishing Activity Trends Summary

Numbers of unique phishing reports submitted to APWG declined by 12.5% by the end of the period, after a spike in February, attributable to IRS-related attacks

Unique phishing websites detected by APWG ended down by 12 percent from January, at 25,630 in March, spiking in February to 36,002, due to IRS-related attacks

The number of hijacked brands rose from 131 to 141 within the period, well within the average for the year

Financial Services was the most targeted sector during the quarter, running between 92 and 94 percent

While the United States remains the top country hosting phishing sites, China dropped to fifth at the end of the period

The number of unique Keyloggers and malicious code applications detected rose to a record 430 in the period

Methodology

APWG is continuing to refine and develop our tracking and reporting methodology. We have re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report emails as those in a given month with the same subject line in the email.

APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites.

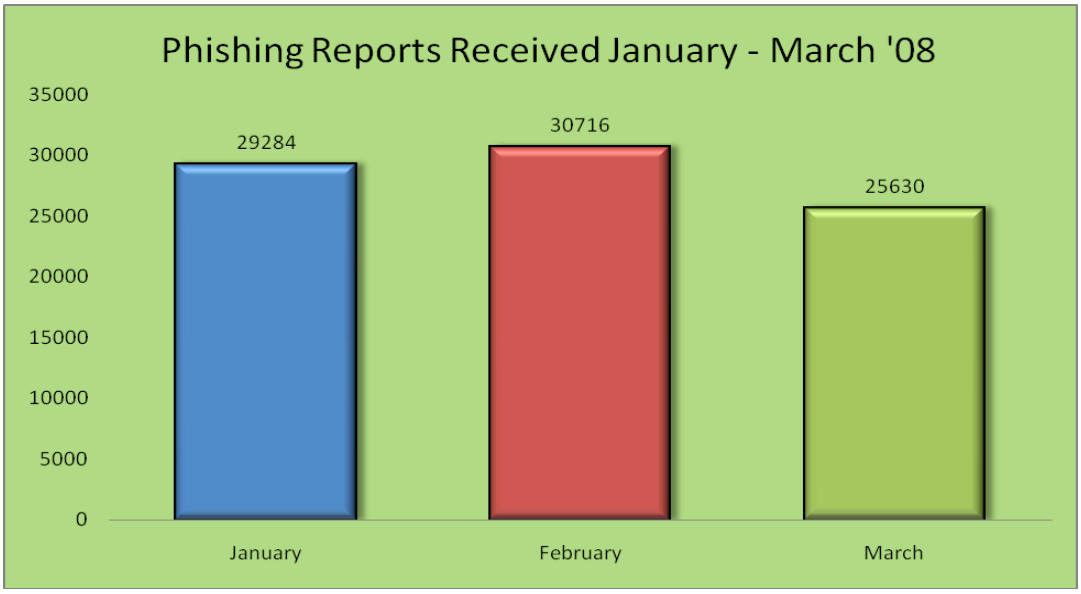
APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sites that are distributing crimeware (typically via browser drive-by exploits).

Statistical Highlights for Q1 2008

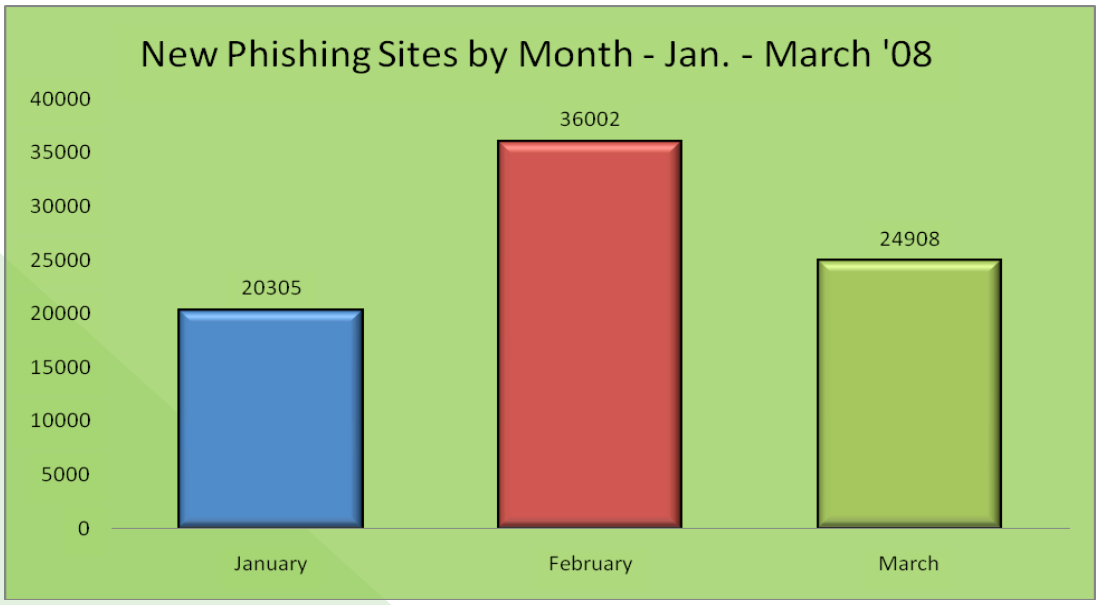
	January	February	March
Number of unique phishing reports received	29,284	30,716	25,630
Number of unique phishing sites received	20,305	36,002	24,908
Number of brands hijacked by phishing campaigns	131	139	141
Country hosting the most phishing websites	US	US	US
Contain some form of target name in URL	28.3%	23.2%	26.1%
No hostname; just IP address	5.5%	13.2%	4%
Percentage of sites not using port 80	.81%	.45%	.49%
Longest time online for website	31 days	29 days	31 days

Phishing Email Reports and Phishing Site Trends for Q1 2008

The number of unique phishing reports submitted to APWG in the first quarter of 2008 remained within a range of slightly over 5,000 unique reports. Over the quarter, reports received decreased by 12.5 percent ending at 25,630 in March, after a spike of attacks in February when the number rose to 30,716. The number at the close of the quarter is off from the high of September 2007 by 33 percent. This represents a count of unique phishing email reports received by the APWG from the general public, APWG members, and its research partners.



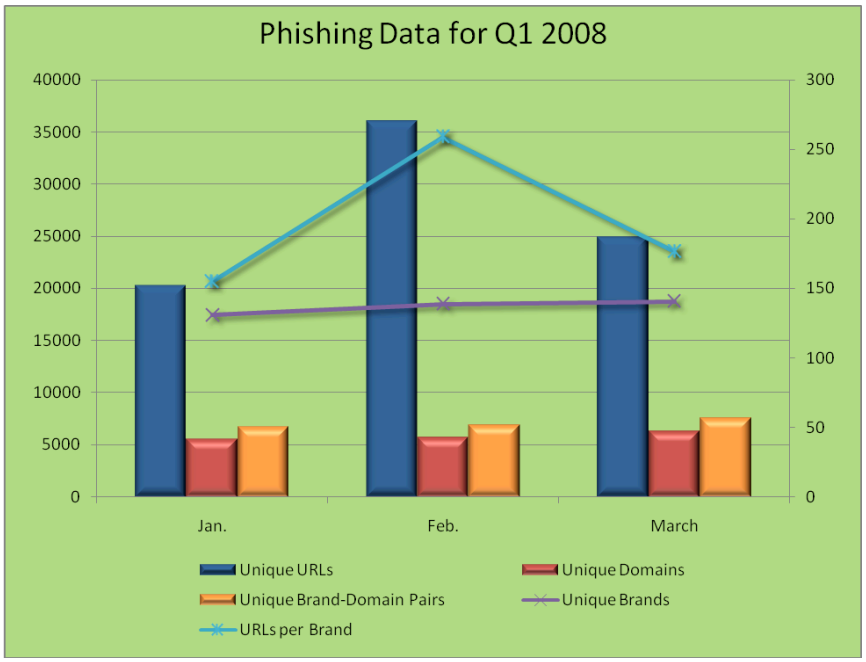
The number of unique phishing websites detected by APWG during the first quarter of 2008 saw a massive increase during the month of February, an increase of more than 77 percent from January 2008. However, a decrease of over 31 percent occurred during March, reflecting the cessation of seasonal IRS-related attacks.



Brand-Domain Pairs Measurement for Q1 2008

The following chart combines statistics based on brands phished, unique domains, unique domain/brand pairs, and unique URLs. Brand/domain pairs count the unique instances of a domain being used to target a specific brand. *Example*: if several URLs are targeting a brand – but are hosted on the same domain – this brand/domain pair would be counted as one instead of several.

Forensic utility: If the number of unique URLs is greater than the number of brand/domain pairs, it indicates many URLs are being hosted on the same domain to target the same brand. Knowing how many URLs occur with each domain indicates the approximate number of attacking domains a brand-holding victim needs to locate and neutralize. Since Phishing-prevention technologies (like browser and email blocking) require the full URL, it is useful to understand the general number of unique URLs that occur per domain.



Unique brand-domain pairs rose steadily throughout the sampling period from January through March, moving from 6,682 to 7,584.

John LaCour, CISSP, Director of AntiPhishing Solutions at MarkMonitor and APWG Phishing Activity Trends Report contributing analyst said, "Phishers seem inexhaustible."

"While the number of unique URLs declined by nearly a third due to lower rock phish activity, the actual number of attacks as measured by a combination of brand and phishing domain names increased 11%. This indicates that traditional phishing is as strong as ever and increasing," Mr. LaCour concluded.

	January	February	March
Unique URLs	20,305	36,002	24,908
Unique Domains	5,490	5,671	6,271
Unique Brand-Domain Pairs	6,682	6,861	7,584
Unique Brands	131	139	141
URLs Per Brand	155	259	177

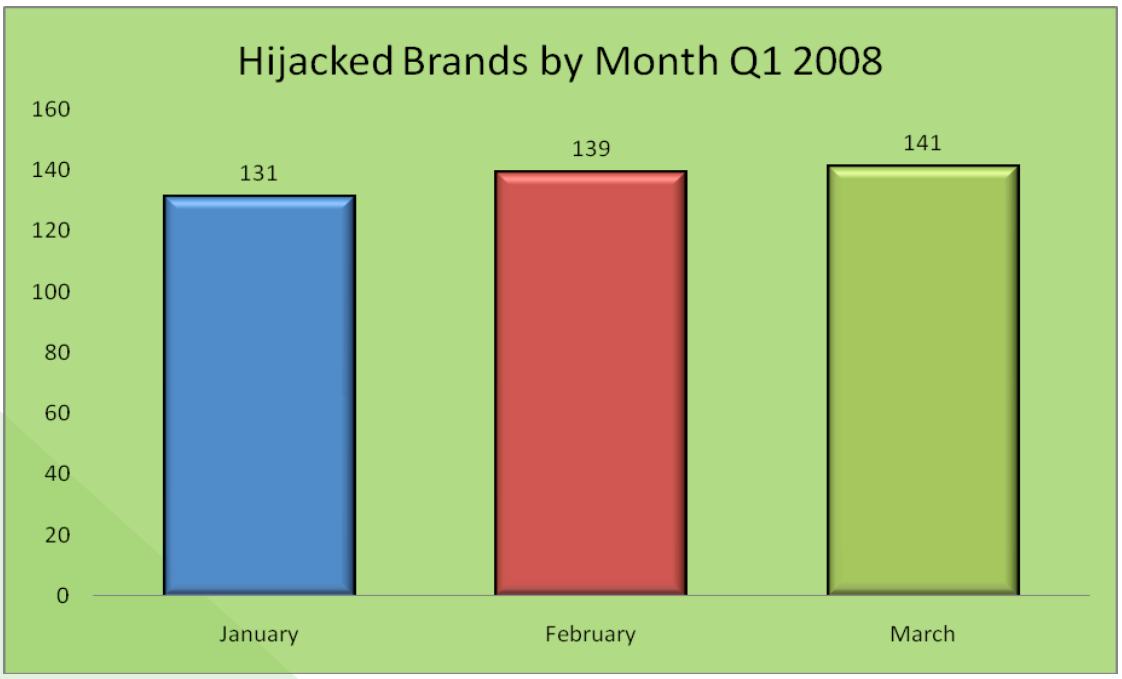
Most Used Ports Hosting Phishing Data Collection Servers in Q1 2008

The first quarter of 2008 saw a continuation of HTTP port 80 being the most popular port used of all phishing sites reported, a trend that has been consistent since APWG began tracking and reporting.

January		February		March	
Port 80	99.23%	Port 80	99.57%	Port 80	99.48%
Port 443	.28%	Port 82	.17%	Port 443	.20%
Port 84	.20%	Port 443	.12%	Port 81	.09%
Port 82	.17%	Port 8080	.07%	Port 82	.07%
Port 88	.04%	Port 4100	.04%	Port 84	.05
3 other	.08%	2 other	.03%	4 other	.11%

Brands & Legitimate Entities Hijacked By Email Phishing Attacks in Q1 2008

The first quarter of 2008 saw a rise of 7.6 percent from 131 to 141 in the number of hijacked brands victimized within the period. Consistently, brands remain in the 120-160 range, illustrating that attacks are directed at consistent types of targets. The end-of-quarter number is still 20 percent off the high of 178 in November, 2007.



Most Targeted Industry Sectors in Q1 2008

Financial Services continues to be the most targeted industry sector during the first quarter of 2008. This is consistent with results since the APWG began tracking targeted industry sectors. The uptick of Government as a target in March reflects a rise in IRS-related phishing attacks or similar scams – by phishing and other media – related to the IRS-administered 2008 Economic Stimulus Refund program.

	January	February	March
Financial Services	92.4%	94.2%	92.9%
Retail	1.5%	1.4%	1.4%
ISPs	3.8%	2.2%	1.4%
Government and Others	2.3%	2.2%	4.3%

Countries Hosting Phishing Sites in Q1 2008

Q1 2008 saw the continuation of the United States remaining the top country hosting phishing sites due to a large majority of attacks being targeted toward United States-based companies. Russia remained in the top four of all countries throughout the period. There was an interesting drop for China in the last month, when they only rendered 3% of top countries hosting websites.

January		February		March	
United States	37.28%	United States	27.11%	United States	38.23%
Russia	11.66%	China	19.25%	Russia	10.58%
China	10.30%	Canada	12.66%	France	6.38%
Germany	5.64%	Russia	10.22%	Germany	4.71%
Romania	5.09%	France	3.39%	United Kingdom	4.49%
Republic of Korea	3.76%	Germany	2.94%	China	3.07%
France	3.28%	Turkey	2.59%	Lebanon	2.48%
Canada	1.94%	Republic of Korea	2.23%	Canada	2.28%
United Kingdom	1.91%	Indonesia	2.08%	Italy	1.96%
Italy	1.59%	United Kingdom	2.04%	Republic of Korea	1.87%

Crimeware Taxonomy & Samples According to Classification

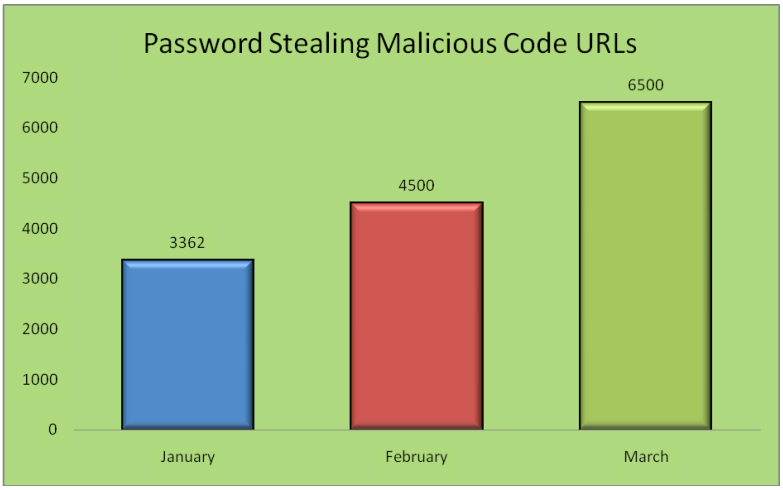
The APWG's Crimeware statistics categorizes crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

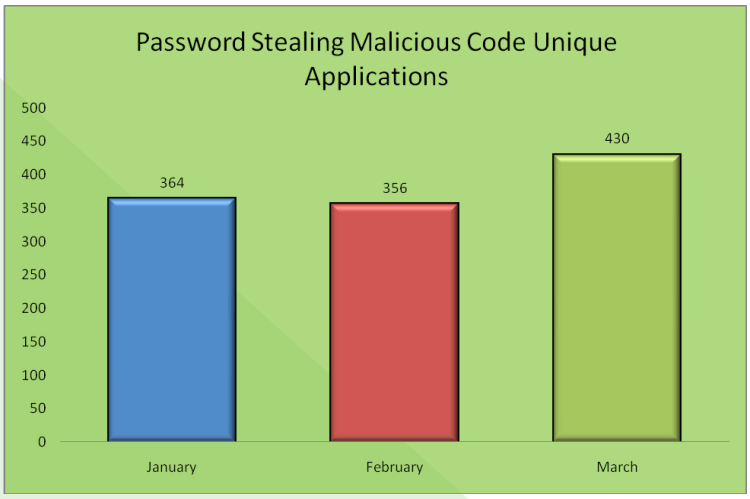
Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, most importantly financial institutions, online retailers, and e-commerce merchants) in order to target specific information. The most common types of information are: access to financial-based websites, ecommerce sites, and web-based mail sites.

Phishing-based Trojans – Keyloggers in Q1 2008

The number of Crimeware-spreading URLs detected rose from 3,362 in January to a record 6,500 in March. This rise represented an increase of nearly 86 percent from the previous record of 3,500 in November, 2007. The number of crimeware-spreading URLs reported at the end of this period was 337 percent higher than the same period in 2007.

Websense Chief Technology Officer and *APWG Phishing Activity Trends Report* contributing analyst Dan Hubbard said that this rise can be attributed to the increase in mass SQL injection attacks that have been on the rise this year.





The number of unique keyloggers and crimeware-oriented malicious applications detected during the period rose steadily, ending at 430, an all-time record some 18 percent greater than the number recorded in the previous record month of January, 2008, when 364 unique malicious applications were detected. Criminal hackers have apparently redoubled their efforts to develop new techniques and scripts to bypass security measures taken by consumers and enterprises.

Phishing-based Trojans – Redirectors

Definition: Crimeware code which is designed with the intent of redirecting end-users' network traffic to a location where it was not intended to go to. This includes crimeware that changes hosts files and other DNS-specific information, crimeware browser-helper objects that redirect users to fraudulent sites, and crimeware that may install a network level driver or filter to redirect users to fraudulent locations. All of these must be installed with the intention of compromising information which could lead to identify theft or other credentials being taken with criminal intent.

Along with phishing-based keyloggers, we are seeing high increases in traffic redirectors. In particular, the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with "good" answers for most domains; however, when they want to direct you to a fraudulent one, they simply modify their name server responses. This is particularly effective because the attackers can redirect any of the users requests at any time and the end-users have very little indication that this is happening as they could be typing in the address on their own and not following an email or Instant Messaging lure.

Phishing-based Trojans & Downloader's Hosting Countries (by IP address)

The chart below represents a breakdown of the websites which were classified during Q1 2008 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger.

January		February		March	
United States	43.39%	United States	38.55%	United States	46.21%
China	16.95%	China	11.59%	China	11.41%
France	6.89%	Republic of Korea	10.38%	Republic of Korea	7.38%
United Kingdom	5.92%	Russia	8.15%	Russia	7.25%
Republic of Korea	5.84%	Poland	7.77%	Poland	6.32%
Russia	4.46%	Romania	6.75%	Romania	4.90%
Spain	3.81%	India	5.77%	India	4.77%
Poland	3.41%	Germany	4.28%	Germany	4.42%
Romania	3.24%	France	3.49%	France	3.93%
Germany	3.16%	Argentina	3.26%	Argentina	3.42%

Phishing Report Contributors

MarkMonitor is the global leader in delivering comprehensive online corporate identity protection services, with a focus on making the Internet safe for online transactions.

PandaLabs is an international network of research and technical support centers devoted to protecting users against malware.

Websense Security Labs' mission is to discover, investigate, and report on advanced internet threats to protect employee computing environments.

The Phishing Attack Trends Report is published quarterly by the APWG, an industry and law enforcement association focused on eliminating the identity theft and fraud that result from the growing problem of phishing, crimeware, and email spoofing. For further information, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282. For media inquiries please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282 or Cas Purdy at 858.320.9493 or cpurdy@websense.com or Te Smith at 831.818.1267 or Te.Smith@markmonitor.com. APWG thanks its contributing members, above, for data and analyses in this report.

About the APWG

The APWG, founded as the Anti-Phishing Working Group in 2003, is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs and consequences, and to share information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement.

Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are more than 1,800 companies and government agencies participating in the APWG and more than 3,000 members. Note that because phishing attacks and email fraud are sensitive subjects for many organizations that do business online, the APWG has a policy of maintaining the confidentiality of member organizations.

The website of the APWG is http://www.antiphishing.org. It serves as a public and industry resource for information about the problem of phishing and email fraud, including identification and promotion of pragmatic technical solutions that can provide immediate protection and benefits against phishing attacks. The APWG, a 501c6 tax-exempted corporation, was founded by Tumbleweed Communications and a number of member banks, financial services institutions, and e-commerce providers. It held its first meeting in November 2003 in San Francisco and in June 2004 was incorporated as an independent corporation controlled by its steering committee, its board of directors, and its executives.