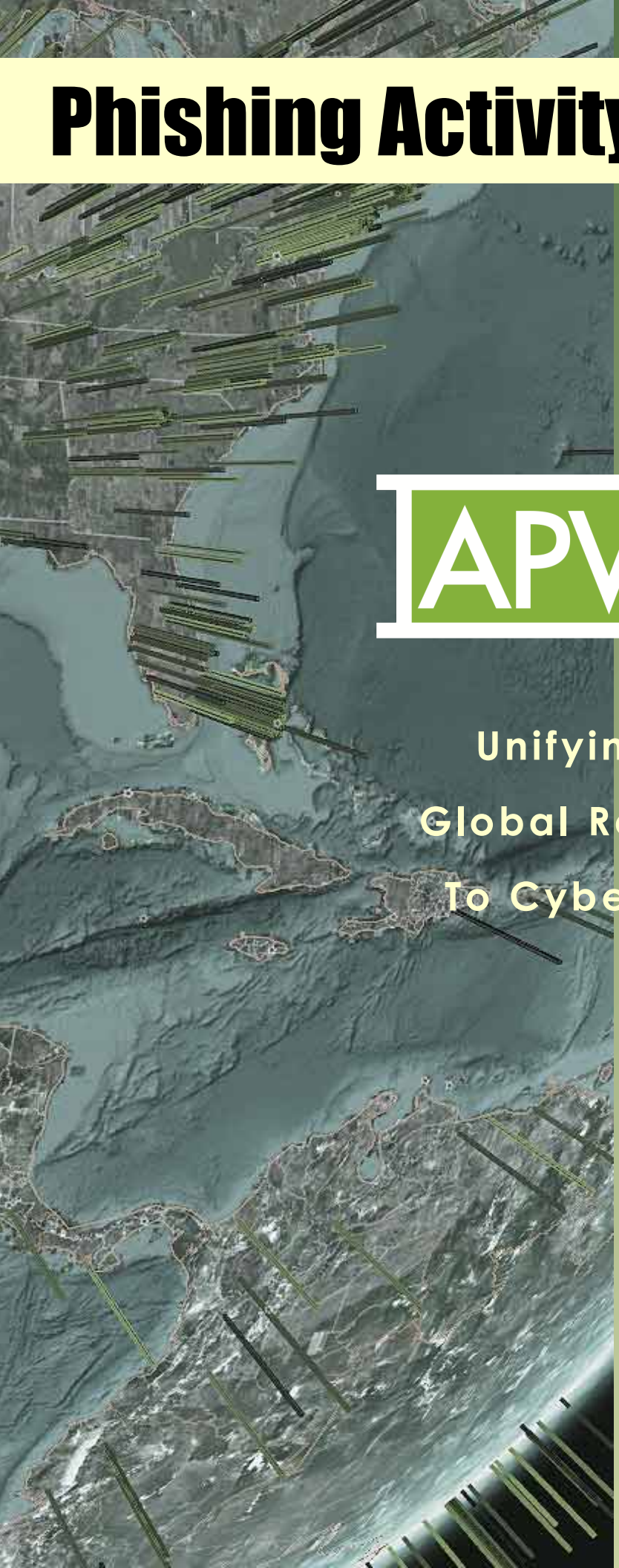
Phishing Activity Trends Report



2nd Quarter 2018

APWG

Unifying the
Global Response
To Cybercrime

Activity April – June 2018

Published October 18, 2018

Phishing Report Scope

The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of crimeware by drawing from the research of our member companies.

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, designed to lead consumers to counterfeit Web sites that 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 Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Phishing Maintains New High During the Second Quarter of 2018

Phishing attacks spiked in March and April 2018. The total number of phish detected in 2Q 2018 was down slightly from 1Q 2018, but remained far higher than in the same period in 2017. [p. 4]

2nd Quarter 2018 Phishing Activity Trends Summary

- There was an increase in phishing that targeted SAAS/webmail providers. Attacks against such providers constituted 21 percent of all phishing attacks. Payment processors continue to be the most-attacked industry sector. [p. 5]
- Brazilian cybercriminals took advantage of the FIFA World Cup to steal and re-sell televisions. [p. 8]
- Some 35 percent of phishing attacks were hosted on Web sites that had HTTPS and SSL certificates: New changes in Web browsers may tell us more about this phenomenon. [p.6]

Statistical Highlights for 2nd Quarter 2018

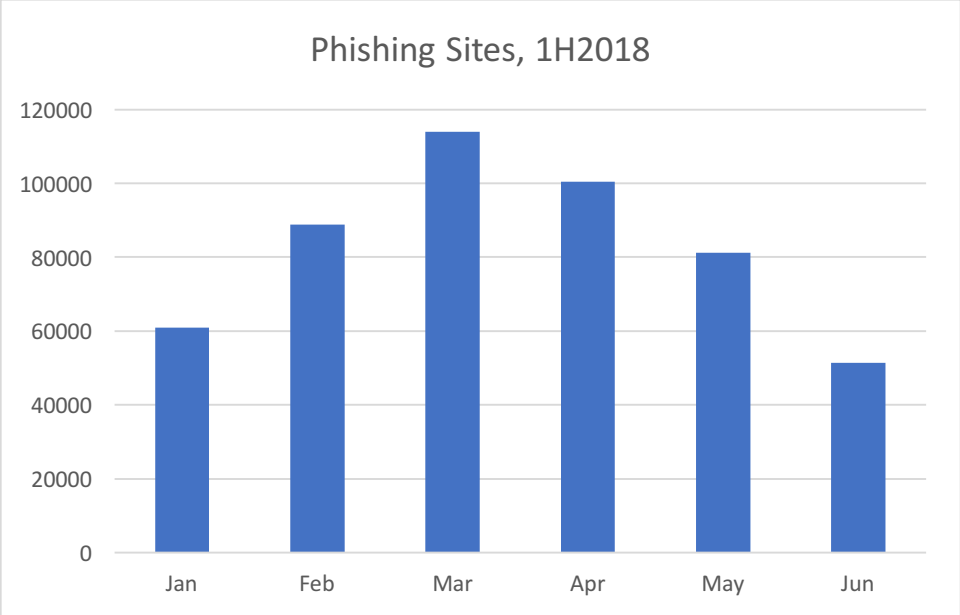
	April	May	June
Number of unique phishing Web sites detected	100,382	81,257	51,401
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	91,054	82,547	90,882
Number of brands targeted by phishing campaigns	274	285	227

The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG tracks and reports the number of unique phishing reports (email campaigns) it receives. An e-mail campaign is a unique e-mail 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 e-mails as those found in a given month that have the same subject line in the e-mail.

The APWG also tracks the number of unique phishing Web sites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLS, all leading to basically the same attack destination.) APWG's contributing members also track a variety of additional metrics and data sets in order to track the fast-paced nature of cybercrime.

Phishing Site and Phishing E-mail Trends – 2nd Quarter 2018

The total number of phish detected in 2Q 2018 was 233,040, compared to 263,538 in 1Q 2018. These totals exceed the 180,577 observed in 4Q 2017 and the 190,942 seen in 3Q 2017.

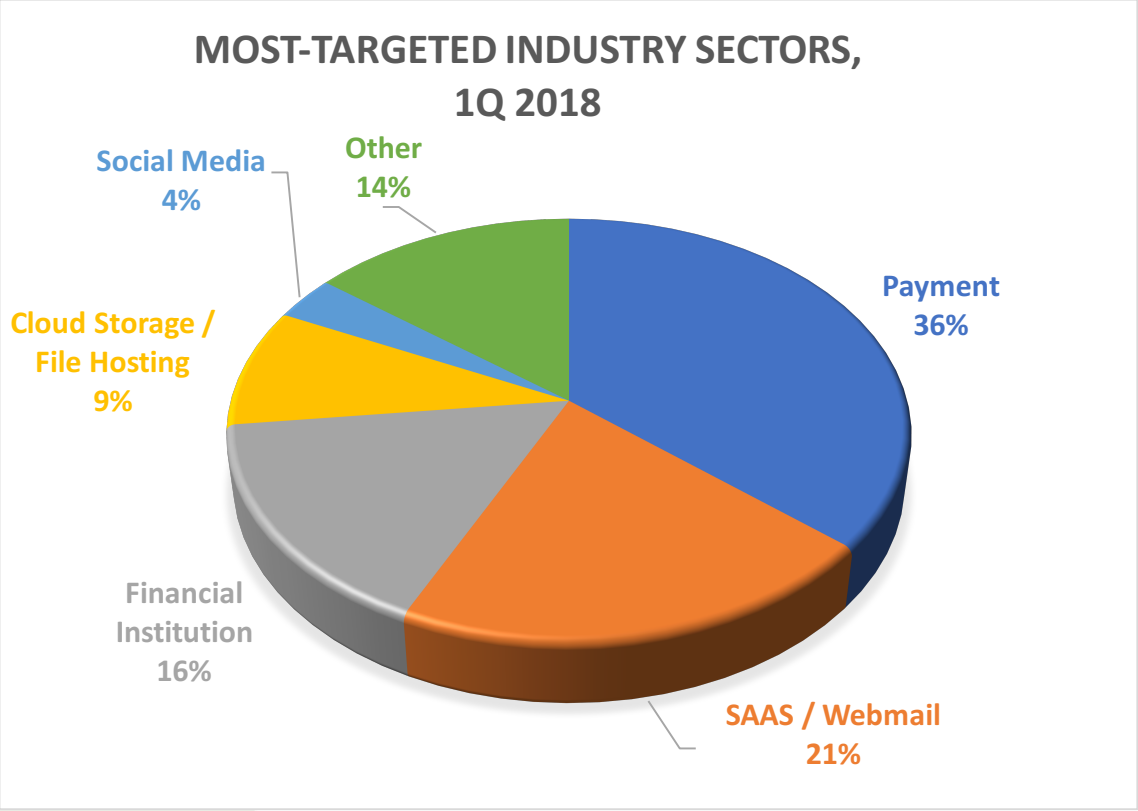


The number of unique phishing reports submitted to APWG during 2Q 2018 was 264,483, almost the same as the 262,704 seen in 1Q 2018.

"In the first quarter of 2018, we reported a huge increase in URL detections in relation to the use of one-time use URLs, inflating detection volumes," said Stefanie Ellis, AntiFraud Product Marketing Manager, MarkMonitor. "That trend has dropped significantly in the second quarter with URL detections nearly half in June from April's high of over 100,000 unique URLs. Unique domains, which is more indicative of actual shutdown volumes, have gradually declined January to June by 40 percent."

Most-Targeted Industry Sectors – 2nd Quarter 2018

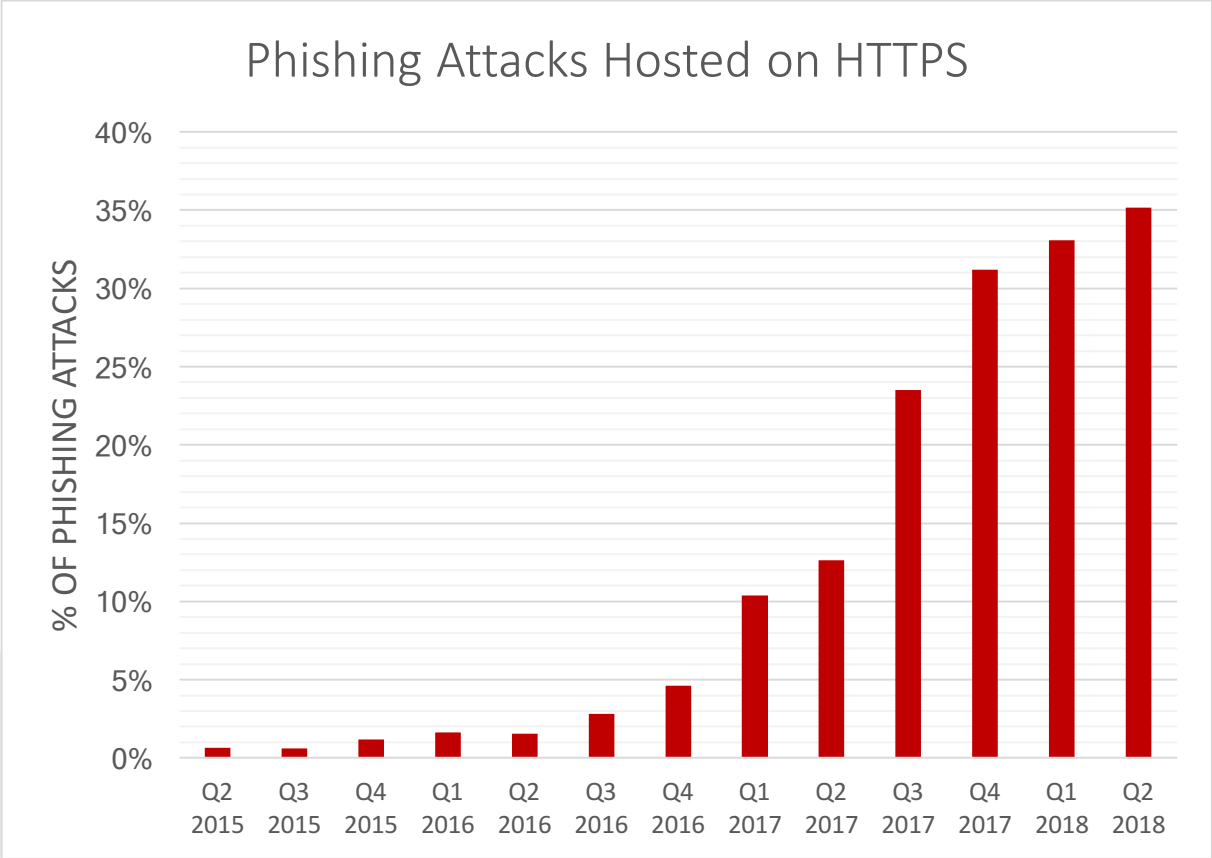
APWG member MarkMonitor saw an increase in phishing that targeted SAAS/webmail providers, jumping to 21 percent of all phishing attacks in 2Q 2018, up from 18.7 percent in 1Q 2018. Phishing that targeted cloud storage and file hosting sites dropped from 11.3 percent to 9 percent. Phishing against payment services and banks dropped slightly. Founding APWG member MarkMonitor is an online brand protection organization, securing intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.



How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking the numbers of phishing sites that are protected by the HTTPS encryption protocol. HTTPS is used to secure communications by encrypting the data exchanged between a person's browser and the web site he or she is visiting. HTTPS is especially important on sites that offer online sales or password-protected accounts. Studying HTTP on phishing sites provides insight into how phishers are fooling Internet users by turning an Internet security feature against them. PhishLabs provides managed security services that help organizations protect against phishing attacks targeting their employees and their customers.

At the end of 2016, less than five percent of phishing sites were found on HTTPS infrastructure. By the second quarter of 2018, however, 35 percent of phishing attacks were hosted on Web sites that had HTTPS and SSL certificates:



In July 2018, Google began labeling non-HTTPS websites as "Non-Secure" in the Chrome browser. "We expect that this use of negative indicators to denote websites that have not obtained legitimate SSL certificates will result in a sharp jump in the number of HTTPS websites, resulting in a likely surge of HTTPS phishing sites to be observed in the third quarter," said Crane Hassold, Director of Threat Intelligence at PhishLabs. "While phishing threat actors will continue to exploit vulnerabilities in legitimate HTTPS websites, they will likely also host more phishing

content on maliciously-registered domains and obtain easily- and freely-accessible SSL certificates so their phishing sites appear more legitimate and are free of negative browser indicators."

There are two primary reasons why phishing sites are protected with HTTPs:

> *1) More HTTPS Web sites = more HTTPS phishing sites.* As more Web sites obtain SSL certificates, the number of potential HTTPS Web sites available for compromise increases. According to Let's Encrypt, two-thirds of Web sites loaded by Firefox at the end of 2017 used HTTPS, compared to 45 percent at the end of 2016.
>
> *2) Phishers are taking advantage of unclear security messaging.* A significant number of HTTPS phish are hosted on domains that are registered by the phishers themselves.

Without an SSL certificate, the phishing page would still function as intended. But in these cases the phisher has obtained a valid SSL certificate. So why would a phisher take that extra step to create an HTTPS page when it is not actually needed? The answer is because phishers believe that the "HTTPS" designation makes a phishing site seem more legitimate to potential victims and, thus, more likely to lead to a successful outcome. And unfortunately, they're right.

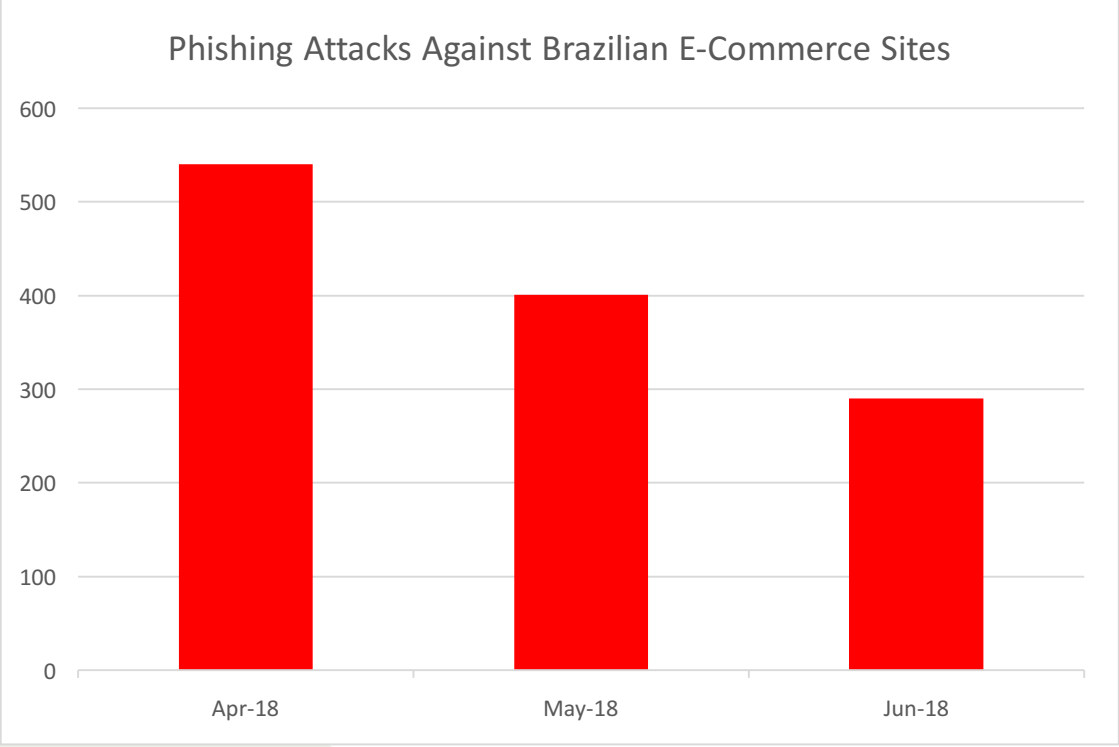
The general public's misunderstanding of the meaning of the HTTPS designation and the confusing labeling of HTTPS Web sites within browsers are the primary drivers of why they have quickly become a popular preference of phishers to host phishing sites.

Phishing and Identity Theft Techniques in Brazil

APWG member company Axur is located in Brazil and concentrates on protecting companies and their users in Brazil from Internet-based threats. Axur especially monitors attacks against banks, technology firms, airlines, and online marketplaces located in the country. Axur's data shows how criminals are perpetrating identity theft in South America's largest economy, and shows how these incidents are both a local and international problems.

Brazilian e-commerce websites are commonly used by criminals to purchase electronic products who use stolen credentials and credit cards, usually obtained through social engineering and phishing attacks. On the black market, the usernames and passwords of established e-commerce customers command a premium price, because thry are trusted more than the credentials of new users. There's even a whole market for login checkers that are sold on the Dark Web. Once the criminal possesses an account and a credit card, he then uses them to purchase products. The delivery address is usually that of a third party. When the product arrives it is used for personal use or resold by the criminal on consumer-to-consumer websites.

The Axur team observed that the number of phishing attacks against Brazilian e-commerce sites fell 53 percent from April to June. "We believe that this spike in April is a movement that has a direct connection to the FIFA World Cup event. In April, many criminals were doing phishing by offering TVs priced much lower than those offered in official stores," said Eduardo Schultze, CSIRT Coordinator at Axur.



APWG Phishing Activity Trends Report Contributors

Axur works to identify and fight the threats in the cyberspace that interfere with the interests of companies, governments, and individuals

iThreat provides risk data, intelligence tools, and analysis to help its clients protect their intellectual & Internet properties.

MarkMonitor, a global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PhishLabs provides 24/7 managed security services that help organizations protect against phishing attacks targeting their employees and customers.

RiskIQ is a digital threat management company enabling organizations to discover, understand and mitigate known, unknown, and malicious exposure across all digital channels

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail spoofing. Membership is open to qualified financial institutions, online retailers, ISPs, solutions providers, the law enforcement community, government agencies, multi-lateral treaty organizations, and NGOs. There are more than 2,000 enterprises worldwide participating in the APWG.

APWG maintains it public website, <http://www.antiphishing.org>; the website of the STOP. THINK. CONNECT. Messaging Convention <http://www.stopthinkconnect.org> and the APWG's research website <http://www.ecrimeresearch.org>. These are resources about the problem of phishing and Internet frauds– and resources for countering these threats. The APWG, a 501(c)6 tax-exempted corporation, had its first meeting in November 2003 in San Francisco and was incorporated in 2004 as an independent corporation controlled by its board of directors, its executives and its steering committee.

The *APWG Phishing Activity Trends Report* is published by the APWG. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver at +1.404.434.7282 or foy@apwg.org. For media inquiries related to the company-content of this report, please contact APWG Secretary General Peter Cassidy at +1.617.669.1123; Stefanie Ellis at Stefanie.ellis@markmonitor.com; Eduardo Schultze of Axur at +55 51 3012-2987, eduardo.schultze@axur.com; Stacy Shelley of PhishLabs,at 1.843.329.7824, stacy@phishlabs.com' Kari Walker of RiskIQ at +1.703.928.9996, Kari@KariWalkerPR.com, +1.703.928.9996. **Analysis and editing by Greg Aaron, iThreat Cyber Group.**