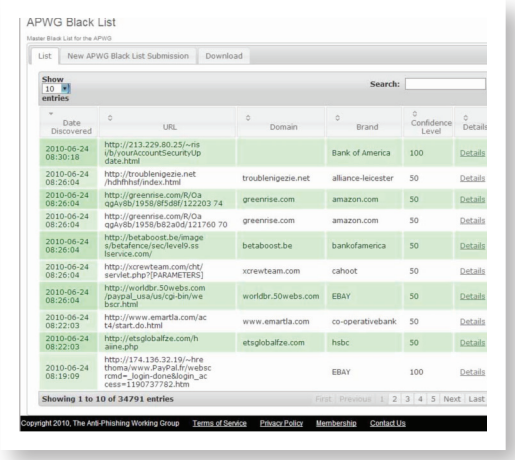
Institutional Profile: The APWG is the global coalition whose mission and charter is to unify the global response to cybercrime across industry, government, law enforcement and international diplomatic sectors. With more than 2000 member institutions worldwide, APWG works to resolve common challenges to the responder, technology and security communities which step up to fight cybercrime every day.

APWG delivers the data, reporting tools and standards these communities need to engage cybercrime programmatically and, with its conferences, the network extensions so vital to their enterprises. APWG is routinely tapped to advise technical governance organizations, hemispheric trade associations and global treaty organizations. The institution's peer reviewed research conferences advance the state of the art of cybercrime research. APWG's public education and awareness programs provide the most potent behavior-modifying system possible, raising awareness while instructing at-risk users.

2003 — Cybercrime Threat Necessitates Crime Event Data Exchange



The URL Block List (UBL), the initial keystone of APWG's cybercrime machine-event data mobilization program, has been in operation in 2003 after financial services and technology firms urged APWG to establish a clearinghouse for phishing attack data. UBL, housed on the APWG eCrime Exchange (eCX), collects and shares phishing data to alert businesses and consumers and help protect them from the latest cybercrime attacks. Updated in real-time with an archive of five years of phishing data, APWG's UBL informs the security routines of brand holders, browser and toolbar developers, AV vendors, cybercrime responders and researchers worldwide to alert businesses and consumers and help protect them from the latest attacks.

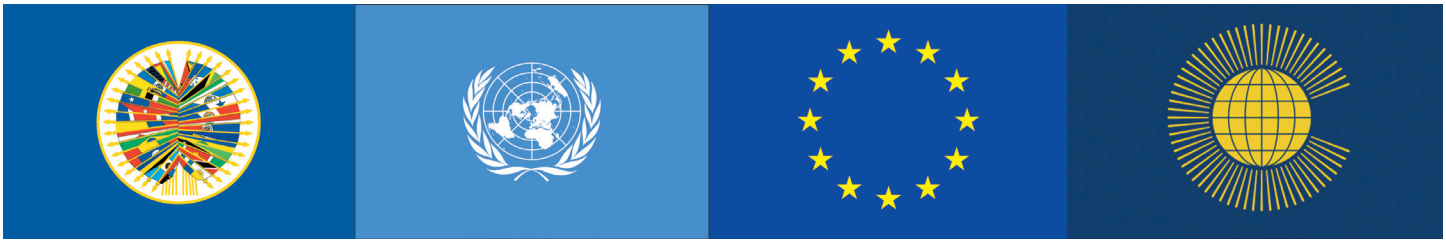
The data streams that APWG archives through its clearinghouses, and receives from contributors are also used in its statistical and technical analyses, such as its quarterly trends report on phishing, its industrial advisories and research reports on such vital topics as the mobile financial crimes threatscape, computer device clean-up schemes, counter-cybercrime best practices for Registrars, domain name abuse and web-server clean-up after recovery. APWG's objective remains to mobilize cybercrime event data though data resources such as the UBL and utilities such as the malicious domain name process and the botnet node notification program. All are tools that help professionals respond to cybercime more programmatically and, someday, automatically. Early on it became clear to the APWG that cybercrime data mobilization would require concerted activity in development of standards and in the engagement of industrial and public policy — essential diplomatic dimensions it attends to with the same dedication as it lends to its cybercrime event data logistics.

APWG has erected a global, cross-sector enterprise against cybercrime of the sort not seen since the Hansa cities of northern Europe took on maritime piracy in the Baltic Sea in the 13th century

2005 — Data Mobilization Leads APWG to Technical Diplomacy

APWG's managers, research fellows and members of the APWG Internet Policy Committee are expert witnesses, advisors and collaborators to industrial governance organizations such as ICANN and the ITU, as well as to governments and treaty organizations that include most every nation on earth as signatories or observers. APWG lends operational insight to the United Nations Office on Drugs and Crime, the G8 (High Tech Crime Sub-Group), the Council of Europe (Convention on Cybercrime), the European Commission, Organization for Security and Co-operation in Europe (OSCE) and the Organization of American States (Inter-American Committee against Terrorism) with which APWG has a memorandum of understanding to co-promote the STOP. THINK. CONNECT.™ cybersecurity awareness campaign.

APWG actively contributes to global standards organizations and has successfully composed and promoted standards (e.g. IETF 5901) and conventions for cybercrime data reporting, and launched a standards-based Bot Infection reporting platform called the Bot-Infected Systems Alerting and Notification System (BISANS). APWG has been instrumental in technical diplomacy within multi-lateral treaty organizations advocating the freeing of cybercrime machine-event data from restrictive laws and regulations, for example consultating with the Council of Europe's Cybercrime Convention T-CY committee in 2013 on data exchange policy.



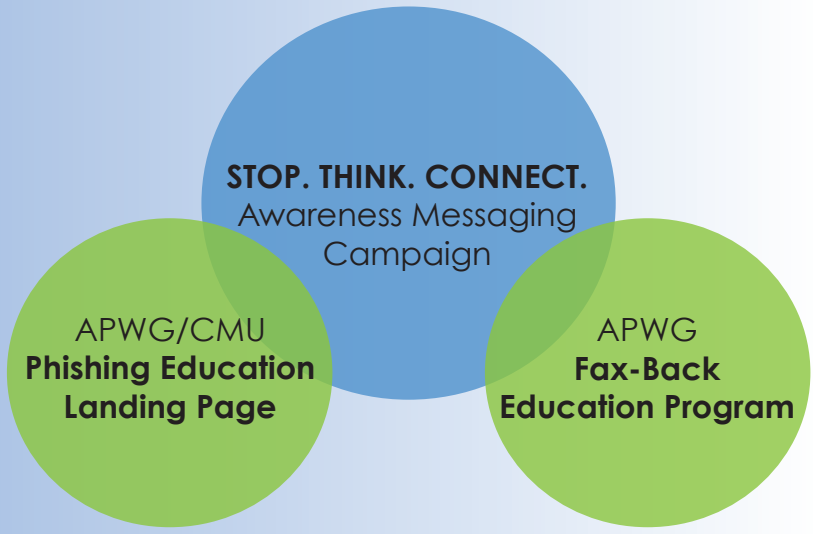
2006 — New Counter-Cybercrime Industry Calls for New Science

The APWG Symposium on Electronic Crime Research (APWG eCrime), established in 2006 convenes the global community of cybercrime researchers with this annual peer-reviewed conference. APWG eCrime's proceedings are dedicated exclusively to cybercrime studies and are published by the IEEE, one of the world's oldest and largest engineering associations. Projects conceived at APWG conferences such as APWG eCrime and subsequent discussions are instrumental in ongoing development of important and permanent cybercrime resources and institutions to which APWG members have exclusive and/or priority access. Among the precipitates of APWG eCrime research has been a number of keystone papers in the nascent discipline of cybercrime research, a field this conference and other APWG programs is helping to achieve its own disciplinary stature.

APWG eCrime
Symposium on Electronic Crime Research

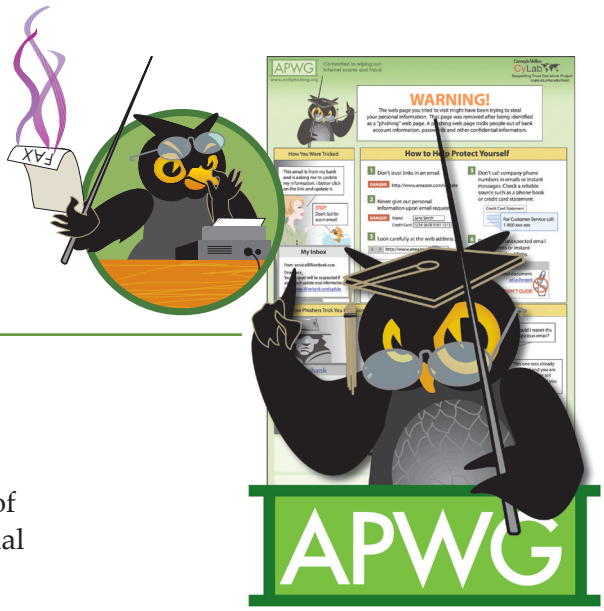
2009 — Learning When Education Can Have Operational Impact

The first resources to have appeared from the APWG's academic research appeared relatively early on and inspired an abiding commitment by the APWG to apply its insights in data logistics to the task of public education. APWG's Phishing Education Landing Page and Fax Back Phishing Education Programs, in part inspired by research papers accepted by the APWG eCrime conference, alerts and advises the most at-risk consumers who've been ensnared in a phishing lure and instructs them on how they can help themselves avoid being similarly victimized again in the future.



Real-time interventions for at-risk users who click on phishing links and answer fax-based frauds, combined with the ubiquitous messaging of the global **STOP. THINK. CONNECT.** campaign effect the most potent and effective behavior-modifying scheme possible — reinforcing best practices broadly while individually instructing the most at-risk users to adopt better online habits

A comprehensive counter-cybercrime strategy needs to include a broad awareness campaign to remind the general public of their role in securing their devices, their data and their transactions. APWG's STOP. THINK. CONNECT.™ campaign, developed with NCSA in 2009, represents a unified global safety and public-awareness program already adopted in the United States, Canada, Panama, Paraguay, Japan and Uruguay - with more nations in the process of adoption. The objective: global deployment.



In its scope, APWG's Public Education Initiative's program is designed to provide both direct intervention of the at-risk user at the same time – while broadly educating the general public of best computing hygiene practices, effecting many of the essential elements of a public-health agency model of intervention.

2014+ — Toward a Response to Cybercrime without Frontiers

All of APWG's research efforts, technical diplomacy and educational efforts are directed toward crafting common data logistics, mutual data exchange paradigms and standards essential to establishing a global response infrastructure on the order of weather reporting systems, global communicable disease reporting and mitigation programs and maritime piracy reporting systems — all cooperative schemes that promote the public safety against a number of persistent, predictable threats. By making cybercrime more transparent and predictable, with education designed to enable safer and more secure online behavior, APWG works to provide resources to manage and finally marginalize cybercrime threats worldwide. Establishment of APWG.EU in 2013 and its continued promotion of the STOP. THINK. CONNECT.™ campaign worldwide is evidence of APWG's commitment, today and in years to come, to a global cybercrime response without frontiers.

The APWG's own development in every dimension describes the awakening of a global culture of shared innovation and mutual assistance against the cybercrime onslaught