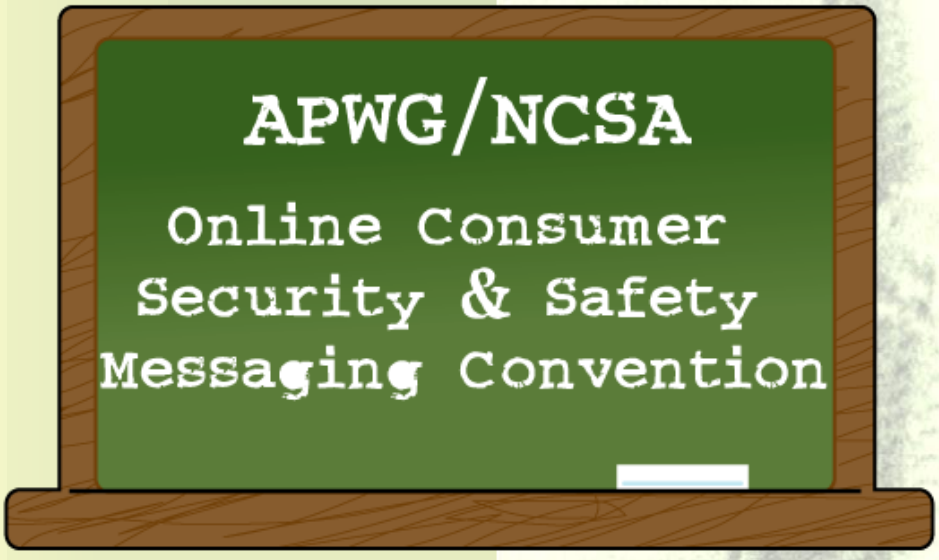
Optimizing Counter-eCrime Consumer Education Through Unified Online Safety Messaging

An APWG/NCSA Public Education Initiative Program Prospectus



STAYSAFEONLINE.org
National Cyber Security Alliance

APWG
Public Education Initiative

February 2010

Correspondent Authors and Convention Development Managers:
Peter Cassidy Cassidy, APWG, **pcassidy@antiphishing.org**
Michael Kaiser, NCSA, **michael@staysafeonline.org**
Aimee Larsen-Kirkpatrick, NCSA, **aimee@staysafeonline.org**

Disclaimer: The APWG, the NCSA and its cooperating investigators, researchers, and service providers have provided this prospectus as a public service, based upon aggregated professional experience and personal opinion. We offer no warranty as to the completeness, accuracy, or pertinence of these recommendations and program plans. Please see the APWG and NCSA websites — **http://www.apwg.org** - and **http://www.staysafeonline.org** — for more information. Institutional affiliations are provided for identification purposes and do not necessarily represent institutional endorsement of or responsibility for the opinions expressed herein.

Colophon: This program prospectus, published in February 5, 2010, is a revision to the initial edition, published in July 2009.

Convention Development Managers:
Peter Cassidy, APWG
Michael Kaiser, NCSA
Aimee Larsen-Kirkpatrick, NCSA

Research Contributors
Stephen W. Feingold, Kilpatrick Stockton LLP
Leigh Fulwood, Costco

Convention Introduction and Scope

There has been no dearth of educational campaigns to help consumers spot and avoid electronic fraud, with efforts mounted by such institutions as Citibank, Federal Trade Commission (FTC) and the National Cyber Security Alliance. All of these educational campaigns impart valuable, timely information to consumers to protect themselves from all forms of online fraud.

In the panoply of the messages delivered to consumers, however, there is inherent discord as the crush of advice and often highly technical instruction, from the consumer's point of view, meld into an incomprehensible, enervating haze of vague menace and half-remembered safety tips.

While there may never be a single facile convention like the PIN rule - 'no one needs to know your PIN, not even your bank' — it is clear that the counter-ecrime community needs to develop a strategy to consolidate its online security messaging for greater consonance and retention.

IT IS CLEAR THE COUNTER-ECRIME COMMUNITY NEEDS TO CONSOLIDATE ITS ONLINE SECURITY MESSAGING FOR GREATER RESONANCE AND RETENTION

The Anti-Phishing Working Group (APWG), the global pan-industrial counter-eCrime association, and National CyberSecurity Alliance (NCSA), the pre-eminent public-private partnership for cybersecurity awareness and education, have stepped forward to propose a pan-industrial **Online Consumer Security and Safety Messaging Convention** to craft and propagate essential online safety and security messages that can be used by a critical mass of consumer-based businesses – thus lending the unity and resonance in delivery of online safety messaging required for them to be retained and employed in a workday fashion by consumers.

This program prospectus discusses the work plan and the roles of participants in developing the Convention and helping to develop, manage and propagate its messages, the benefits of Convention participation, prerequisites for joining the Convention and intellectual property issues related to managing the Convention's messaging assets.

The APWG and NCSA invite retail-sector and consumer-facing companies to join this Convention, one they believe promises to deliver a messaging program that will resonate across retail sectors, media and international boundaries – providing online safety messaging as broad and as penetrating as the criminal enterprises that menace consumers worldwide.

Messaging Assets Focus and Convention Development Program

The sharable messaging assets envisioned for this Convention will provide an 'awareness' style messaging scheme, made up of text messaging and associated logography to be propagated through all media with minimally burdening licensing requirements for Convention members and other enterprises. The Convention's organizing objective will be to protect the largest consumer cohort possible at the lost possible cost.

During Convention meetings in Los Angeles at MySpace/Fox Interactive Media, in Washington, DC at the offices of Google and in Bellevue at Microsoft, representatives of the APWG, NCSA, their members and correspondents investigating Convention development discussed the shape and content of the messaging framework. It was agreed upon that the messaging assets developed by the Convention would operate at a high level in the style of an 'awareness' campaign, embodying these aspects in its communications content:

a. Personal Responsibility
b. Social Consequence
c. Relevant to contemporary threats
d. Actionable

Further, in terms of overall messaging assets development and usage, Convention members established three levels of Convention participation: the **organizing committee** which will actively manage messaging development and Convention governance vehicles with the APWG and NCSA and recruit other consumer-facing companies and government agencies to participate; **sponsors** who will provide financial assistance for development of the messaging assets; and **users/propagators** who will license [see p. 6] and deploy the messaging assets in their own consumer communication programs.

Messaging Assets: Work Development Plan

The Convention organizing committee is receiving and reviewing proposals from marketing and advertising firms to assist in the development of the public awareness message and/or messaging suite for online security and safety. The selected consulting company will be tasked with initial message composition as well as the testing of its efficacy with consumer audiences.

The development program's creative objective is to craft a high-level message that can be used independently - or as part of a framework for other actionable safety and security measures consumers can take in different areas of the Internet: ecommerce, social networking and banking, for example. The message should also have the potential to be used as the basis for a national Public Service Announcement campaign that the consulting group would potentially also help the Convention develop and execute.

The submission deadline is February 12, 2009 and the finalists will be selected to give in-person presentations at the Convention meeting in San Francisco on March 5, 2010 where the Organizing Committee and its correspondents will interrogate the responding companies' principals about their proposals. Incumbent upon the funding the development program, APWG and NCSA expects work to begin on the crafting of the messaging content in Q2, 2010.

The APWG/NCSA Convention management team will work in collaboration with the consulting messaging development firm and the Organizing Committee in a step-wise program of message content creation and message testing. The Convention development team will work through an online workgroup at the APWG members' website and a workgroup list - and through live conferencing at stand-alone working sessions as well as at APWG and NCSA conferences.

THE GREATEST CHALLENGE AT THIS STAGE IS IN FINDING THE MOST EFFICACIOUS LEVEL OF GUIDANCE, BETWEEN OVERARCHING PRINCIPALS AND TECHNICAL INSTRUCTIONS

The larger messaging development team will craft ideas for messaging content – the focus of the awareness concepts and guidance – as well as mechanisms for crafting the messaging assets and propagating the messaging assets through the networks of the Convention members and their public facing distribution channels (e.g. Websites; product boxes; ATM receipts; sales receipts; customer newsletters) and through broader channels such as radio, television, social media. The team clearly has its work cut out for it, logistically in managing all these viewpoints and members and creatively in crafting messaging assets that can protect the vast and variegated consumer landscape.

The largest challenge at this stage, however, is in finding the most effective level of guidance, waiting to be found somewhere between the extremes of overarching principals (e.g. *Be Alert!*) and direct technical instruction (e.g. *Right-click on the lock*

graphic in the browser's chrome . . .). The Convention's development managers, however, are confident that the development team's heterogeneous membership will deliver messaging assets that can be used for the very largest cohort of consumers – and maximally relevant to the customers of all participating members.

Messaging Assets Management, Licensing and Protection

The Convention organizing committee is organizing two legal instruments required for the long-term development and management of the Convention's messaging assets – and sculpting an intellectual property protection strategy to maximize messaging assets propagation while maintaining essential control of them.

The APWG and NCSA are establishing a new non-profit entity that would manage funding resources required to develop and maintain the messaging assets and to protect them from misuse and infringement. That new entity would be jointly owned and jointly operated by the APWG and NCSA.

Initially, this new organization will receive the sponsorship funding from Organizing Committee members and sponsors to fund the consulting group being engaged to develop and test the messaging assets. Later, it will use some blend of sponsorship and licensing fees to maintain and protect the messaging assets.

Secondly, the new organization will establish a formal licensing scheme for the users/propagators of the messaging assets that would maximize deployment of messaging assets while maintaining a level of control required to protect them should they be infringed upon or otherwise abused. The organizing committee also determined a tiered licensing scheme for commercial enterprises, government agencies and NGOs would allow the Convention to offer licenses geared for those sectors' specific needs.

Development of messaging assets management program would be incomplete, however, without a formal intellectual property protection strategy. The objective here is not to limit the use of the messaging assets, but rather to build a cooperative effort that allows for the broadest adoption of shared resources that each member can implement in a way that is most relevant to their network and customers - and still affords these assets protection from abuse. Ideally, the licensing structure would make it easy expand the network of users and recruit new members—corporate, government, and nonprofit—to the effort.

APWG, NCSA and one founding member of organizing committee are corresponding with an intellectual property management law firm that has given us some initial guidance as to possibilities in this regard. We discuss them here to open a dialogue on these issues and to give current correspondent companies and institutions considering joining the Convention a quick review of the choices at hand so they can determine which schemes would be most acceptable to their respective enterprises.

There are four generally accepted schemes that are available to the Convention for cooperatively securing a mark that is used to promote an association that supports a set of common principals, goals or practices:

1) A Certification Mark that denotes a level of performance, subject to an annual fee and a standardized audit
2) A Membership Mark that denotes membership in an organization and is used exclusively by its members
3) A Copyrighted Logo associated with a short phrase (which can't be copyrighted), available to anyone who agrees to abide by certain user criteria
4) A Service Mark, signifying a level of service supported by the company or institution or agency displaying it.

Each of these options comes with its own burdens and cost of policing to enforce ownership of intellectual property assets. Further, there are two other approaches for protecting the messaging assets, we've been advised, involving different levels of government participation.

The first is government adoption of a mark, effectively placing the burden of policing under the adoptive agency. The most well-known example of this scheme is the ubiquitous recycle symbol depicting a circle of green arrows, control of which was ceded to the Federal Trade Commission, we have been advised.

The second is special purpose legislation that would, by law, assign control of certain symbols to organizations that use them for their chartered missions. Well known examples are the Olympic five-ring symbol that is assigned to the United States Olympic Committee, the Red Cross' red cross and the 4H Club symbol.

The APWG/NCSA Convention management team presents these as potential models for consideration by companies joining in the program and in no way proffers any one of them as a preferred scheme. Convention members would confer

with corporate counsel and return their companies' preferences in development of intellectual property protection and licensing schemes.

Messaging Assets Deployment and Propagation Plan

The shape and scope of a media and distribution strategy will be largely dependent upon resources available to the Convention members. The APWG/NCSA Convention management team believes, however, that even a modest program of unified online safety messaging could engender substantial benefits without requiring new and heroic levels of investment for each Convention member.

EVEN A MODEST PROGRAM OF UNIFIED ONLINE SAFETY MESSAGING COULD ENGENDER SUBSTANTIAL BENEFITS WITHOUT REQUIRING NEW AND SUBSTANTIAL INVESTMENTS

Shareable, unified messaging assets could be instantiated on most any media, including existing instruments such as product boxes, software instructions, Web application instructions, e-commerce shopping receipts, banking and financial account statements, ATM receipts, instructional Web pages at social networking Web sites, Web sites, newsletters, essentially all manner of printed or digital materials already being produced by Convention members as well the traditional media channels of print, radio and television media.

The strength of this endeavor is the broad-reaching, consumer-facing networks the Convention members each have – and the strategy of leveraging a common message through them all simultaneously, helping consumers absorb and retain its protective content. Without large-scale investments, most members could adopt the messaging and disseminate it to their customers and the public using media mechanisms and distribution channels they already employ.

Development of the messaging assets, however, at some point in this process, most likely requires some investment by the Convention and its members. One area for consideration under discussion is how the Convention will share burdens of investment in developing and disseminating messaging assets equitably among Convention members.

UNIFIED MESSAGING ASSETS COULD BE INSTANTIATED ON MOST ANY MEDIA: PRODUCT BOXES, ATM STATEMENTS, PERSONAL CHECKS AND COMPANY WEB PAGES

If, for example, the Convention members desire to engage in a broad sweeping generalized campaign utilizing traditional media, other investments might also need to be made. These types of campaigns require substantial investment – whether through the Ad Council or other means. For example, a basic campaign with the Ad Council requires a three-year, three million dollar commitment, with an initial investment of $850,000 required for the first year.

In terms of distribution models, the Convention management team recognizes the contribution that large scale efforts can make to a program of safety education. However, the team also believes enough benefit can accrue from unified online safety messaging that even a relatively modest cross-industry program can yield powerful benefits over time.

The APWG/NCSA Convention management team is eager to develop the Convention to the largest possible extent, yet is prepared to work at any scale to realize real benefits today and build toward a larger deployment in the future. Inaction on our part only continues to deny the public benefits that industrially sponsored research and coordination of unified online safety and security messaging could deliver to the public.

Prerequisites, Privileges and Risks of Participation

The funding of the initial message development and testing phase will cost something within the low six-figure range. At this time, the Convention is requesting sponsoring companies contribute $5000 each toward the costs of retaining a PR or communications consultancy to manage and complete the work required.

The requirements for participation the Convention are still in development, although some obligation for institutions to commit at some level to use the messaging assets would be the minimum that the Convention's managers would expect of participants.

The Convention development team is asking all interested companies and institutions to ask their house counsel which messaging asset licensing and

management schemes [see p. 6] would allow them to participate in the program and use the messaging assets. Those responses will expose common barriers to participation that would have to be mounted by the development team and negotiated in the creation of the messaging assets and the licensing scheme adopted to manage them.

The benefits of participation in the Convention during its development phases are: influence in the shape and content of the final messaging assets; leadership in a national effort to engage the American public in cybersecurity awareness and education; and the civic recognition attendant development of the kind of public education program that was called for in President Obama's recent 60 Day Cyber Policy Review.

Risks at this stage are few but there is no guarantee that the final messaging assets that will be deployed will not directly or implicitly conflict with a Convention member's workaday operational policies, for example, inclusion of clickable links in emails from the company to the customers.

About the APWG

The APWG, a 501 c (6) association founded in 2003 as the Anti-Phishing Working Group, is an international industry, law enforcement, and government coalition focused on eliminating identity theft and fraud resulting from the growing problem of phishing, e-mail spoofing, and crimeware.

Membership, which exceeds 3,300 members, is open to qualified financial institutions, online retailers, Internet service providers (ISP), the law enforcement community, and researchers and solutions providers. More than 1,800 companies, law enforcement agencies, and government ministries worldwide are participating in the APWG.

APWG's websites (www.antiphishing.org and education.apwg.org) offers information to the public and to industry about phishing and e-mail fraud, including identification and promotion of pragmatic technical solutions that provide immediate protection. APWG directors and researchers have provided formal guidance and data to the OECD, European Commission, Council of Europe, United Nations Office of Drugs and Crime, US Congress, the Ministry of Economics, Trade and Industry in Japan and scores of government and justice ministries worldwide.

About the NCSA

NCSA's mission is to empower a digital citizenry that uses the Internet securely and safely, protecting themselves, the networks they use, and the cyber infrastructure.

NCSA, a 501 c (3) founded in 2001, is the pre-eminent public private partnership, working with the Department of Homeland Security (DHS), corporate sponsors(Symantec, CISCO, Microsoft, SAIC, EMC, McAfee, and Google), and nonprofit collaborators to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education.

Ultimately, NCSA measures its success to the degree by which cyber security has become second nature for all computer users. NCSA seeks to raise awareness of cyber security to the level of other cultural messaging that is universally good for citizens—healthy eating, exercise, and safe driving—by teaching skills and judgment to build a national understanding about appropriate online tools and behavior. NSCA's public facing presence is its website www.staysafeonline.org.