Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) Membership Value and Fact Sheet

Who We Are

The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation. We are the largest global industry association, with more than 200 members worldwide, bringing together all the stakeholders in the online community in a confidential, open forum. We develop cooperative approaches for fighting online abuse.

Founded in 2004, M³AAWG is a technology-neutral, non-political working body. We systematically focus on operational issues of Internet abuse including technology, industry collaboration and public policy. Members include Internet service providers (ISPs), communications service providers, social networking companies, hosting and cloud services providers, major antivirus vendors and security vendors, email service providers, leading hardware and software vendors and major brands.

What We Do

We develop and publish best practices papers, position statements, training and educational videos, and other materials to help the online community fight abuse with a focus on operational practices. Our public policy advocacy (which is not lobbying) provides technical and operational guidance to governments and Internet and public policy agencies developing new Internet policies and legislation.

As an organization, we target abusive messaging, malware and other new forms of threats to end-users:

- **Messaging** – Addressing abuse on any messaging platform, from email to texting
- **Malware** – Spam and many other forms of abuse are only the symptoms of the real pathology, which are the bots, viruses and malicious code that surreptitiously infect users' systems
- **Mobile** – Protecting this ubiquitous platform as it comes under attack from malware and messaging abuse, including both text and voice services

How We Work

M³AAWG provides a trusted forum and a framework for open discussion on abuse issues among the professional online community in an atmosphere of confidentiality and cooperation. Following the Chatham House Rules: "What happens in M³AAWG stays in M³AAWG." Our work is driven by members who contribute ideas and content for best practices and other documents with input from a diverse community across industries, government, academia and civil society groups. We also seek feedback from relevant associations and experts within the online ecosystem.

Value for Our Members

The sharing within M³AAWG of the best approaches to fight abuse has proven very valuable to our members and is not available in any other forum. Members share information on deploying new technologies and operational-level evaluations of technical initiatives for stopping online threats. This often equates to free technical and operational consulting from peers, leading experts and our Senior Technical Advisors, and is a unique membership benefit.

Members participate in M³AAWG through relevant committees or interest groups with three main working committees: Collaboration, Technical and Public Policy. We have a Training Committee that programs training at each meeting, including online videos. M³AAWG members and the Board of Directors also collaborate frequently with other industry stakeholders including the Unsolicited Communications Enforcement Network (UCENet, formerly the London Action Plan or LAP) and numerous governmental regulatory agencies. Though M³AAWG does

not lobby on government or public policy matters, our Public Policy Committee does supply factual information to government organizations as they develop relevant policy or legislation.

Membership

M³AAWG membership includes more than 200 companies and organizations worldwide:

- Major ISPs, communications and social networking providers such as 1&1 Internet AG, AOL, AT&T, Bell Canada, CenturyLink, Comcast, Cox Communications, Facebook, Google, Internet Initiative Japan, LinkedIn, Microsoft, Orange, Rediff.com India, Sprint, Swisscom, TDC, Liberty Global, Verizon Wireless, and Yahoo
- Hosting and cloud service providers including Amazon Web Services, Endurance International Group, Gandi SAS, GoDaddy, OVH, Rackspace, Wix
- Major brands such as PayPal, JP Morgan Chase, Lloyds Bank, and significant volume email senders/ESPs
- Leading hardware and software vendors such as Apple, Cisco and Oracle plus major antivirus and security vendors
- Concerned government and industry entities and global anti-abuse organizations, such as Cable Television Laboratories, Inc.: CAUCE; eco-Association of German ISPs, Internet Society, NCTA, DNS-OARC, Spamhaus, Shadowserver, SURBL, i2Coalition, and LACNIC. M³AAWG also is an active member of UCENet.

A complete member listing is at www.m3aawg.org/about/roster/

Output

Among our recent best practices are:

- New M³AAWG and LAP Operation Safety-Net global best practices–Outlining online threats for government, business and industry with the proven recommendations to mitigate them
- Hosting and Cloud Service Provider Best Practices–Spamvertising, malware and other online threats could be significantly reduced by hosting companies that follow these hygiene and security processes.
- M³AAWG Mobile Messaging Best Practices for Service Providers–These industry best practices can help mitigate mobile messaging (i.e., SMS, MMS and RCS) abuse, including abuse with text messaging and connected services. The guidelines outlined here will help service providers and vendors sustain practical levels of trust and security across an open, globally interconnected messaging environment.

Among our publications:

- We have published more than 35 best practices and white papers, including the first to address how ISPs can work with consumers to detect and remove bots. This document became the basis for the IETF's RFC 6561. We also published the first senders best practices developed cooperatively with volume emailers and network operators.
- M³AAWG actively seeks to provide strategic technical guidance to protect end-users' online experience as governments and their agencies worldwide develop new cybersecurity policies and legislation.
- M³AAWG regularly submits comments on government and public policy proposals, including responses to ICANN and other Internet governing bodies, and to North American and European public policy agencies.
- All M³AAWG published documents can be access at www.m3aawg.org/for-the-industry.
- M³AAWG public policy comments are at www.m3aawg.org/activities/published-comments.

Meetings

M³AAWG holds meetings twice in North America and once in Europe each year. Attendees are veteran anti-abuse and security professionals actively engaged in the challenges of fighting spam, bots, malware and mobile abuse. Participation continues to grow and is generally over 300 attendees from 15 to 20 countries at each event. More than 500 industry representatives from 28 countries attended our 2017 San Francisco meeting.

These multi-track meetings held over four days feature presentations by academic researchers, public policy advisors, government representatives, industry experts, and innovative technology leaders with open discussion among industry peers. Upcoming meeting dates and locations are at www.m3aawg.org/upcoming-meetings.

More Information

See www.m3aawg.org for our published work, industry announcements and other details on our organization.
Questions? Please contact Jerry Upton, M³AAWG Executive Director, at jerry.upton@m3aawg.org.