M3AAWG publishes best practices, position statements, training/educational videos and other materials to help prevent online abuse.

The Messaging, Malware, and Mobile Anti-Abuse Working Group provides a collaborative global trusted forum that brings industry together to help fight and prevent internet online abuse.

As more advanced online abuse threats rapidly evolve, M3AAWG is proactively shifting its work to focus on 4 key areas, in addition to continuing to develop the organization, its partner ecosystem, while continuing to maintain a diverse and inclusive culture.

**Data and Identity Protection**
Protect online identity (ex. using multi-factor authentication), ensure data privacy and security through use of encryption/encrypted protocols, adopt Zero Trust principles by verifying explicitly, using least privilege and assuming breach.

**Communications**
Protect network, messaging, mobile, IoT communications/systems/devices from malware, spam, phishing, DDoS, DNS attacks.

**Supply Chain**
Understand downstream dependencies and risk, incorporate secure software development/testing practices, proactively monitor, detect and manage vulnerabilities.

**Readiness**
Shift to be proactive to identify emerging threats, focusing on prevention/mitigation/detection, deprecating older technologies.

Working with members, industry groups and global partners, M3AAWG will continue its efforts to help prevent online abuse, focusing on protecting communications, data privacy and security, and the supply chain.

www.M3AAWG.org