# Engaging the FTC on Web Host Security Tips for Small Businesses

INTERNET INFRASTRUCTURE COALITION

*i2Coalition.com*

*718 7th Street NW*
*2nd Floor*
*Washington DC 20001*

*membership@i2coalition.com*

*(202) 524-3183*

M3AAWG
MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

*m3aawg.org*

*781 Beach Street,*
*Suite 302*
*San Francisco, California 94109*

The Federal Trade Commission recently issued a statement "**Hiring a web host? FTC has security tips for small businesses**" from information gathered in a series of Small Business Security Roundtables last summer. We are very pleased to see the FTC take an active interest in these important issues. Just in the past year, the FTC's Office of Technology Research and Investigation (OTech) also looked at **11 web hosts that market their services to small businesses** and issued "**Do Web Hosts Protect Their Small Business Customers with Secure Hosting and Anti-Phishing Technologies?**," which addressed whether the hosting companies offer SSL/TLS technologies that help secure communications between a website and its visitors and whether the companies supported email authentication technologies.

The FTC report details whether the web hosts they analyzed actually integrate SSL/TLS into the setup of small business clients' websites and if the hosting companies supported email authentication technologies such as Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM). The SSL/TLS integration had favorable results but email authentication technologies did not. The recommendations generated from these reports were provided as important considerations for small business owners interested in hiring a web hosting company and to operators of web hosting review sites.

All of the noted technologies are widely-implemented security standards that can help protect both business customers and the overall internet from attacks and fraud. For example, in an attempt to secure and authenticate emails, the U.S. Department of Homeland Security (DHS) issued **Binding Operational Directive 18-01** this past October requiring all federal agencies to use the email authentication technologies SPF, DKIM and DMARC (Domain-based Message Authentication, Reporting and Conformance) and the SSL/TLS technologies in STARTTLS, which encrypts email in transit.

We wish to address the FTC recommendations for hosting providers with the following guidance:

> Web hosting companies should continue to help small businesses implement SSL/TLS. Given the significant security benefits, hosts should also consider including this and email authentication protective technologies by default. Web hosting companies that cater to small businesses can play a big role in increasing the use of SPF, DKIM and DMARC by automatically configuring those technologies for their clients. These technologies are free and the implementation cost for web hosts is small. And what web hosting company would not want to truthfully tout the benefits of its built-in security features?

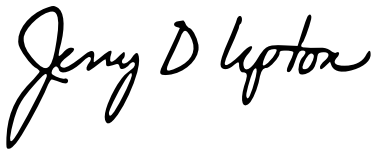
We applaud the FTC's recommendations and wish to build on them by drawing attention to an even more detailed blueprint for this kind of positive action that exists for the industry in a document produced by our organizations. The document is i2Coalition/M³AAWG **Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers**, issued in March 2015 and subject to

periodic review and updating by the Messaging, Mobile and Malware Anti-Abuse Working Group (M³AAWG).

Our organizations believe that all the advocacy we can encourage around SSL/TLS and SPF, DKIM and DMARC adoption is worthwhile. We also believe that industry is most effective when it produces best common practices together, which is what groups like i2Coalition, M³AAWG and other internet groups comprised of industry experts are doing. As we continue working to address these issues, we hope to directly engage the FTC to reinforce the ongoing work already being done on these important issues. As the FTC continues conversations on these important matters, we hope to be included in these discussions. As we continue our efforts, we look forward to working with the FTC as well.

Sincerely,

Christian Dawson, Executive Director
Internet Infrastructure Coalition
718 7th Street, 2nd Floor
Washington DC 20001



Jerry Upton, Executive Director
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109

INTERNET INFRASTRUCTURE COALITION

*i2Coalition.com*

*718 7th Street NW*
*2nd Floor*
*Washington DC 20001*

*membership@i2coalition.com*

*(202) 524-3183*

M³AAWG
MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

*m3aawg.org*

*781 Beach Street,*
*Suite 302*
*San Francisco, California 94109*

INTERNET INFRASTRUCTURE COALITION

## About The i2Coalition

The Internet Infrastructure Coalition (i2Coalition) ensures that those who build the infrastructure of the Internet have a voice in global public policy. Founded in 2012 by a diverse group of Internet infrastructure companies, the i2Coalition is now the leading voice for web hosting companies, data centers, registrars and registries, cloud infrastructure providers, managed services providers and related tech. The continued growth of the Internet's infrastructure is essential to the global economy, and i2Coalition fulfills a vital role of protecting innovation in the Internet's infrastructure, worldwide.

M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

## About the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is where the industry comes together to work against bots, malware, spam, viruses, denial-of-service attacks and other online exploitation. M³AAWG (**www.m3aawg.org**) members represent more than one billion mailboxes from some of the largest network operators worldwide. It leverages the depth and experience of its global membership to tackle abuse on existing networks and new emerging services through technology, collaboration and public policy. It also works to educate global policy makers on the technical and operational issues related to online abuse and messaging. Headquartered in San Francisco, Calif., M³AAWG is driven by market needs and supported by major network operators and messaging providers.