

Why Your Browser Matters

Promoting Teachable Moments Implementation Guide



Developing and advocating best practices and public policies which mitigate emerging privacy, identity and security threats to online services, government agencies, organizations and consumers, thereby enhancing online trust and confidence.

Updated October 11, 2011

INTRODUCTION

The goal of this program is to reach consumers, home-based businesses and small businesses, promoting the importance of using up-to-date browsers. With the assistance of OTA members and supporters, the emphasis is on reaching leading ecommerce, social networking, and banking sites where consumers share personal data or conduct online transactions. This program relies on the concept of teachable moments: providing contextual recommendations to consumers based on their online activities, applications and services used while visiting a known and trusted website.

This effort to drive browser updates is not new. In 2009, visitors to YouTube who were using an older browser were encouraged to update.¹ Most recently in June 2011, Google announced it was phasing out support for Firefox 3.5, Internet Explorer 7, Safari 3 and their predecessors in Google Apps in favor of browsers that handle HTML5.² The OTA *Why Your Browser Matters* initiative leverages these efforts and lessons learned from driving hundreds of thousands of consumers to update their browser.

The recommendations in this document reflect the general consensus of OTA members and the OTA browser upgrade working group, which includes representatives of the browser community, technology providers, and consumer facing web sites. It is important to acknowledge that there are tradeoffs in providing consumer recommendations including clicking on links to download software.

The working group identified several top issues in developing these recommendations: 1) the risk of the initiative being exploited by cybercriminals, 2) ensuring the instructions are intuitive and easy to understand by non-technical users and 3) ensuring the recommendations are universal and apply to the broadest set of operating systems and browser scenarios. In an ideal world, every computer would be set to seamlessly automatically update and upgrade applications. Unfortunately this is not possible due to a broad range of technical limitations with legacy operating systems, privacy and regulatory issues, and compatibility issues.

This initiative understands the complexities of website management and the user experience. It is anticipated that many websites may take several months to implement their version of this initiative and others will need to wait until after the fourth quarter holiday period before making site changes. To support these efforts, OTA will continue to update materials and highlight early adopters who have demonstrated leadership and commitment to online security and privacy.

This effort reflects broad industry and business support as well as input from industry and business leaders. An updated list of supporters may be found at <https://otalliance.org/browser/supporters.html>.

¹ <http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=175292>

² <http://www.eweek.com/c/a/Messaging-and-Collaboration/Google-Apps-Phases-Out-Older-IE-Firefox-Safari-Versions-412196/>

EXECUTIVE SUMMARY

Today over 40% of users are using non-current or legacy browsers, many of which are no longer supported by their vendor. Older and un-patched browsers have known vulnerabilities which cybercriminals continue to attempt to exploit. Unfortunately the majority of consumers do not understand that the use of non-current browsers risks jeopardizing their personal data, their computers and their identity.³ The use of a non-current browser also prevents users from realizing the feature-rich browsing experience offered by a growing number of sites.

Fortunately in the past year, every major browser has made one or more updates, greatly expanding their security and privacy feature set. These new versions are faster, more secure and offer more privacy enhancing features than ever before. Best of all, consumers can update their browser with minimal effort and at no-cost, easily obtaining peace of mind in minutes.

Upgrading to an up-to-date browser is important for two reasons:

1. Old browsers are vulnerable to attacks because they typically do not include the latest security and privacy fixes and features. Browser vulnerabilities can lead to identity theft, installation of malicious software, or worse. An up-to-date browser helps guard against security threats like phishing, malware, and malicious downloads. In addition with the support of privacy enhancements, users have added capabilities to protect their privacy including the ability to opt-out of tracking by third parties.
2. Web standards have evolved. Many of the latest features on websites and web applications work only with the newest web browsers. Up-to-date browsers have improvements that let users run web pages and applications quickly, along with support for current technologies and standards such as Extended Validation SSL Certificates, always on SSL, HTML5, CSS3, and accelerated JavaScript. Users of old browsers are unable to realize the enhancements of faster performance, streaming, video and graphics.

This initiative focuses on the consumers, home offices and small businesses that have not yet updated their web browser. It is important to note just using a current browser is not a “silver bullet”. Users need to keep their operating system and applications up to date, use current anti-virus software, and practice safe computing.

While this initiative is primarily aimed at consumers, home office, and small business users, business users need to review their IT policies and impact on proprietary and line of business applications for compatibility. In addition, existing plug-ins may not be compatible with browser upgrades. It is important to note, such plug-ins may inherently have security vulnerabilities and should be tested and continues business use validated.

³ See Appendix A. Data as reported by comScore for users of Windows based PC and devices, analyzed by OTA as of August 31, 2011.

IMPACT TO WEB SITES & BUSINESSES

Consumers are not the only ones impacted by the use of outdated browsers. Businesses bear significant costs associated with supporting older browsers. These include both direct operational costs associated with supporting legacy browsers and the direct costs resulting from fraud, account takeovers, password provisioning, and management. Recommending that site visitors upgrade their browser will:

- Help protect users from online threats and instill trust and confidence in your site
- Reduce support for legacy browsers including development resources and testing
- Allow websites to focus on the latest technologies & site innovation
- Reduce dependency on plug-ins and extensions
- Reduce risk of your customer's data and log on credentials being compromised
- Reduce account takeovers and resulting site fraud

Site Considerations

Asking a customer to upgrade their browser is generally no different than asking a customer to install or update a browser add-on like Adobe Acrobat, Adobe Flash, Oracle's Java, etc. Major sites make such recommendations thousands of times each day with little or no issues. The site detects their customer's versions, compares the results to a minimal version level (e.g., "Flash 10.x or greater is needed for this site"), communicates with their customer that an update is needed, and then directs their customer to the appropriate third-party site.

Prior to implementation of this initiative it is highly recommended that sites analyze their customer profiles by browser version and operating system. Websites may find that their customer base is more up-to-date than the general Internet population. Preliminary research from OTA member companies suggests that in some cases only 20% of their customers have out-of-date browsers. This research suggests that highly engaged customers are more likely than not to be early adopters and have already updated their browsers.

It is important to note some legacy operating systems such as Windows XP (which includes Internet Explorer 6, released in 2001) or older Mac OS versions are not fully supported by all current browsers. Sites may choose not to message some customers with very old browsers or old operating systems due to potential compatibility and support issues. Given the potentially low percentage of older browsers or operating systems that do not have an update path, websites should understand that the majority of their customers may not be affected by the Why Your Browser Matters initiative and never see the update message.

Sites also need to consider the point of interaction with the user. For some sites, it is optimal to interact with consumers on the home page while other sites may choose to limit interaction to the "sign on/authentication" pages of their sites. Other alternatives include interacting after customers have visited the website more than "x" times or have viewed more than "y" pages on the site.

Sites need to consider user experience and potential customer "friction" and "frustrations" leading to possible site abandonment. To address repeated messages, a site may choose to set

a cookie on the customer's browser so the site does not repeatedly provide an update message to the consumer.

Each site will need to think about its customers, their navigation and their user experience to find the optimal path. Sites may consider alternative forms of messaging based on their site architecture including the use of pop ups or pop under messages. In addition, creative alternatives might be deployed including sending out-of-band email messages or greeting card reminders to encourage the customer to update after the website session is completed. Another possibility is to provide a "teachable notice" after a purchase is made, focusing on the order confirmation page or order confirmation email ("Thanks for the order. We noticed that you are using an older browser. We suggest you update to a newer browser." Etc.)

Operational considerations:

- Impact to online flow and user experience
- Risk to site or cart abandonment
- Pervasiveness or frequency of notice
- Value of threat mitigation
- Ease of cybercriminals to mimic site and notices

Messaging considerations:

- Tone and personality - Messaging should be concise, easy-to-understand and appropriate for the target audience. Informative and actionable, yet not alarmist. Consider a "layered message", providing customers the option for more information.
- Focus on no more than three main points - Performance, privacy, and security. Websites should create a list of basic answers for their customer service personnel (i.e., Why is our site participating in this program? Why did you get a message to update? Is it safe to update?) Convey that you care about your customer's security, privacy and browsing experience.
- Frequency - Do not overwhelm consumers with repeated messages to avoid burnout, which could result in the consumers ignoring the upgrade your browser messages.
- Languages - Consider multi-lingual or localized messaging or offering alternative messages.

TECHNICAL CONSIDERATIONS & REQUIREMENTS

OTA acknowledges that organizations need to review and consider the impact to the user experience on their site. In the following scenarios, it is important to recognize that a subset of customers may be presented with messages and teachable moments. Sites may wish to consider a tiered or phased implementation, first focusing on the oldest browsers and adding others over time.

The following is an outline of two customer messaging concepts:

1. Based on defined rules (see appendix) applied after validating the browser user string (OS and browser version), messages to consumers with older browsers will be dynamically created.
2. Customers will be directed to a page explaining why they should update (Figure 2).
3. As an alternative, a site may choose to serve an in-page banner presented within the DOM (Figures 3 & 4). In this scenario the banner could link to a “teachable moments landing page” (Figure 2) or provide a link to directly update to a newer version of their browser. A working mockup of such a notice may be found at <https://otalliance.org/browser/landing.html>.

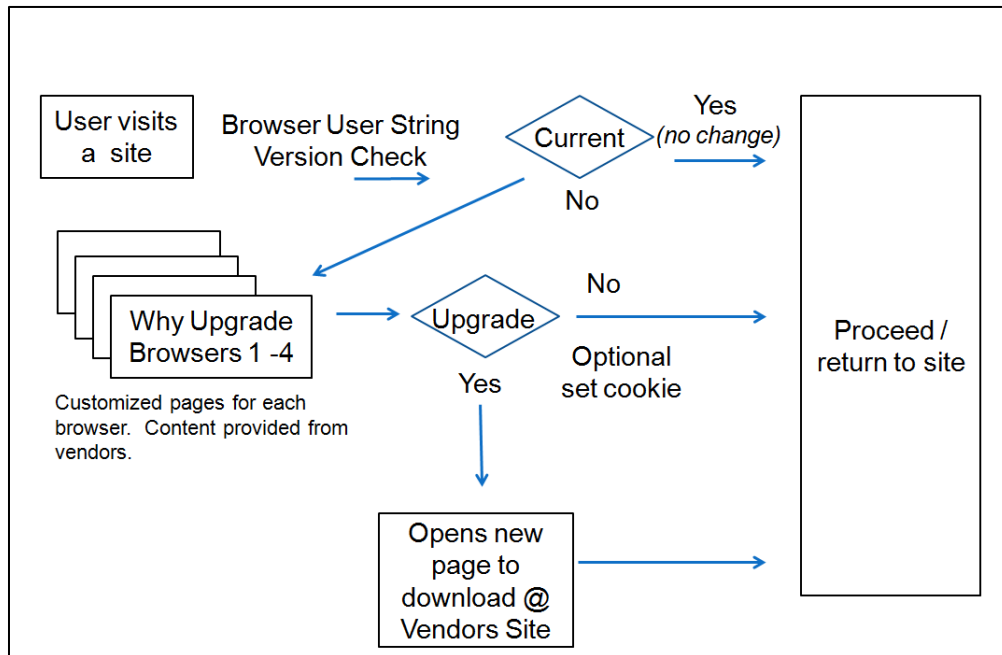


Figure 1 – Option 1 – Redirect session to Why Your Browser Matters landing page

OTA
Online Trust Alliance

Join OTA
Contact us
About Us
Privacy Policy

Resources • Initiatives • Events • News Room • Members • Member Login

Why Your Browser Matters

As part of our efforts to provide site visitors the best on line experience, we have noticed you are using an older version of <browser name>. Your browser is the first line of defense and we recommended you **upgrade your browser today at no-cost**.

The modern browser is faster, more featureful, more secure and offers privacy enhancing features than ever. Continued use of outdated browsers needlessly expose users, their identity and data to malicious attacks and prevent users from realizing a feature-rich browsing experience offered by a growing number of sites. [More Information >](#)

[Yes I want to Upgrade - Take Me to the Download Site](#)

[No Thanks. I prefer to upgrade later](#)

Note – If you use an older operating system, you may not be able to install the latest browser version and take full advantage of the latest security, privacy and performance features. In addition, certain legacy business applications may not be supported by newer browsers. Business users should check with their system administrators before installing.

Information is provided for information purposes only. <Company xyz> does not endorse any of the the above produces. Users should check compatibility before installing.

©2011. All rights reserved. Online Trust Alliance (OTA)

Figure 2 - Teachable moments landing page

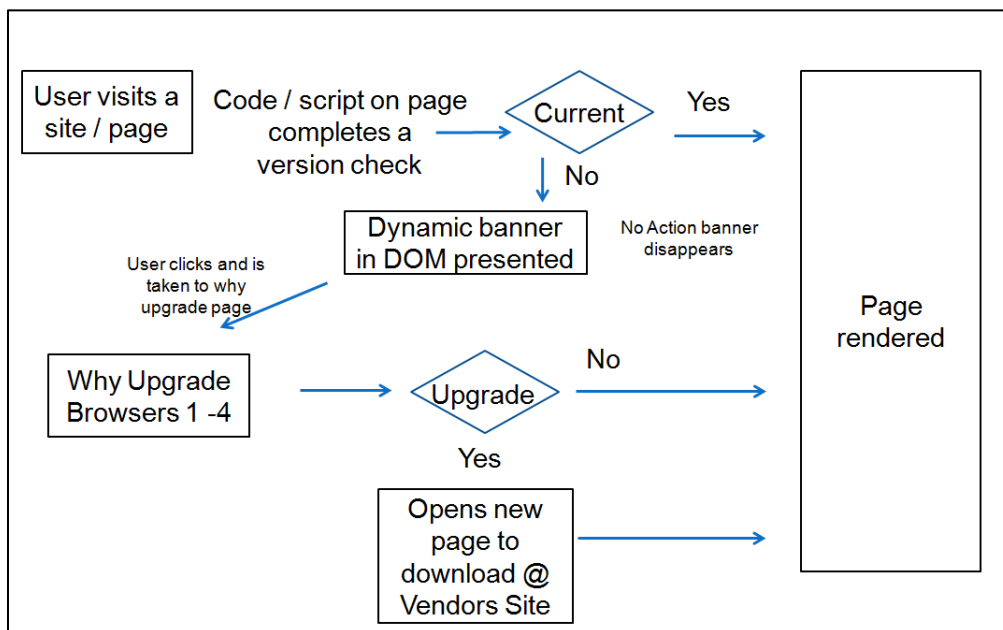


Figure 3 – Option 2 – Use of in page notice (see Figure 4)

The OTA recognizes that there are many combinations of browsers, browser versions, operating systems, service packs, mobile versus PC browser, connection speeds, etc. These combinations may cause “corner cases” which can have unknown results. Websites may choose to eliminate particular operating systems, browser versions, etc. because of low customer penetration, technical concerns, etc.

CUSTOMER MESSAGING - CONCEPTS

The following are samples of webpage banners for consideration. Sites may wish to customize their messaging based on their customer profiles. Additional versions are posted at <https://otalliance.org/browser/gallery.html>.

The “Learn More” URL (which links to a page posted on the site for more information) could be changed to “Update Now” as shown in Figure 5, linking directly to the browser update page specific for the customer’s browser; for example, a customer using Firefox is linked to the appropriate Firefox/Mozilla update page or an Internet Explorer customer gets linked to the Microsoft update page. See <https://otalliance.org/browser/updatelinks.html> for major browsers’ update links. Figure 6 as implemented at PrivacyChoice.org directly links to the respective update page. The Update Now approach has the benefit of not requiring the site to host any pages, but fails to control the messaging to the customer, relying on the respective browser vendor to provide the compelling update information.

Note depending on the browser detected, an alternative user notice is recommended such as “Show me how to upgrade” or for Firefox users “Check for Updates” selecting option in the “About Firefox” menu.



Figure 4 – In page warning (concept)



Figure 5 - In Page Warning - Upgrade Now



Figure 6 - Sample Notice (PrivacyChoice.org)

WHY CONSUMERS SHOULD CARE – CONCEPT COPY

The following is a summary of key points and conceptual messaging copy that websites may adopt. As every site has its unique personality and tone, websites may adapt and use copy as they deem appropriate. Key points:

- Current browsers include significant innovations in security, privacy and performance.
- An up-to-date browser is the first line of defense against a variety of cybersecurity issues.
- Upgrading is simple, fast and at no cost (using broadband connectivity).
- Benefits include enhanced security and increased protection of personal data from phishing and deceptive websites, malicious downloads and socially engineered exploits.
- Enhanced control on consumers' privacy, online browsing activities and the use of consumer data by third parties.
- Increased website functionality and performance including captivating graphics & animation.

The following are two examples of message copy that sites may wish to use. In both cases the copy is recommended to be dynamic based on customer's browser and links to that browser's update page. While each website may have their own perspectives on what browser is best from a security and privacy perspective, the OTA recommends that the website should not attempt to persuade a customer to directly switch browser brands. Suggesting that the browser be changed can lead to customer confusion and added support requirements. Efforts must be non-competitive and vendor neutral.

Short Landing page copy (draft only):

As part of our efforts to provide our site visitors the best online experience, we notice you are using an older version of <browser name>. The current version is faster, more secure and offers more privacy-enhancing features.

Continued use of your outdated browser exposes you, your identity and your data to malicious attacks. An updated browser will allow you to realize the feature-rich browsing experience offered by most websites.

Best of all, you can easily update your browser—and your security—at no cost in just a few minutes.

[Yes, I want to Update - Take Me to the Download Site](#)

Expanded landing page copy, (layered notice):

As part of our efforts to provide our site visitors the best online experience, we notice you are using an older version of <browser name>. The current version is faster, more secure and offers more privacy-enhancing features.

Continued use of your outdated browser exposes you, your identity and your data to malicious attacks. An updated browser will allow you to realize the feature-rich browsing experience offered by most websites.

Best of all, you can easily update your browser—and your security—at no cost in just a few minutes.

Upgrading to an up-to-date browser is important for several reasons:

- Old browsers are vulnerable to attacks because they typically aren't updated with the latest security/privacy fixes and new features. Browser vulnerabilities can lead to identity theft and installation of malicious software.
- An up-to-date browser helps guard against security threats like phishing, malware and malicious downloads and offers added privacy protection of your data and online activities.
- Web sites evolve quickly. Many of the latest features on today's websites and web applications won't work with out-of-date browsers.
- Up-to-date browsers have the speed improvements that let you run web pages and applications quickly, along with support for modern web technologies such as streaming, internet phone, video and graphics.

Of course, using an updated browser alone is not a “silver bullet”. You still need to keep your operating system and other applications up to-date, use current anti-virus software and practice safe computing.

[Yes, I want to Update - Take Me to the Download Site](#)

Other Safe Browsing Resources (available at <https://otalliance.org/browser/resources.html>)

OTA IMPLEMENTATION RESOURCES

Sample code <https://otalliance.org/browser/code.html>

Image Gallery <https://otalliance.org/browser/gallery.html>

Update Links <https://otalliance.org/browser/updatelinks.html>

Frequently Asked Questions <https://otalliance.org/browser/FAQ.html>

Legal – Recommending customers to update to a leading browser is not unlike asking customers to install a browser add-on or suggesting customers to download new versions of Adobe Flash, Adobe Acrobat, Java, etc. Such disclaimers should state the information is being provided for information purposes only and sites are neutral, not endorsing any browser over another. Sites should consider adding a note mentioning that while it is uncommon, certain customized business or enterprise applications and browser plug-ins may not work with updated browsers. Business users should check with the IT department before upgrading.

THIRD-PARTY IMPLEMENTATION RESOURCES

Migrating from IE 6 - Enterprise Application Compatibility with IE 9
<http://technet.microsoft.com/en-us/magazine/hh360991.aspx>

Running IE 6 Applications in IE 9 - Run IE6 Line-of-Business Applications in IE8 or IE9 with UniBrowser <http://www.browsium.com/>

BrowserHawk <http://browserhawk.com/> (detects customer's browser details including version, service pack, OS version, connection speed, etc.)

RELATED RESOURCES

Sites may consider providing added resources on a “more information” page. *Note this is not recommended on the default landing page. A/B testing has shown pages with added links, adversely impact click through to the upgrade link.*

[U.S Department of Homeland Security](http://www.dhs.gov/files/cybersecurity.shtm) <http://www.dhs.gov/files/cybersecurity.shtm>

[U.S Federal Trade Commission – OnGuardOnline.gov](http://www.onguardonline.gov)

[Stop. Think. Connect. - Campaign](http://www.dhs.gov/files/events/stop-think-connect.shtm) <http://www.dhs.gov/files/events/stop-think-connect.shtm>

Your Browser Matters <http://www.yourbrowsermatters.org/> (Microsoft)

What Browser <http://www.whatbrowser.org> (Google)

20 Things I Learned On the Web <http://www.20thingsilearned.com/en-US/home> (Google)

APPENDIX A – ADOPTION DATA

Understanding browser market share, version terminology and operating system compatibility is critical to a site's implementation of the Why Your Browser Matters initiative. The browser community utilizes varied nomenclatures for version numbering, including a lack of a consistent approach to what constitutes an update (typically fixes and security patches) versus upgrades including new features and functionality. Addressing this issue OTA has defined "Current" to include the current version offered by the browser vendor from their download site and the prior version, provided that version is supported with automatic security updates from the vendor.⁴

For example, for Internet Explorer, (IE), "Current" includes both IE 8 and IE 9. Conversely "Legacy" includes prior versions which may or may not be supported. While IE 7 is still supported by Microsoft, it is classified as a legacy browser since it is more than two versions old. The decision to not include such earlier versions is that they lack several security and privacy enhancements as well as lack of support web standards found in current browsers.

It is important to note browser share for a specific web site may be significantly different than what is reported. Actual percentage of users of out-of-date browsers could be closer to 20% or 25% based, which would reduce the number of users who would receive a notice or page redirect. This underscores the importance of sites to analyze their user data.

World Wide			
	All	Current	Legacy
Chrome	27.7%	25.5%	2.1%
Firefox	16.5%	10.2%	6.3%
IE	55.0%	22.6%	32.4%
Safari	0.9%	0.9%	0.0%
Total	100.0%	59.1%	40.9%

Figure 7 – World-wide Browser Market Share

US & Canada			
	All	Current	Legacy
Chrome	20.4%	19.8%	0.5%
Firefox	14.3%	9.2%	5.1%
IE	64.2%	33.1%	31.1%
Safari	1.1%	1.1%	0.0%
Total	100.0%	63.2%	36.8%

Figure 8 - North American Browser Market Share

⁴ Source: comScore, month ending September 31, 2011 for users of Windows based PCs and devices. <http://www.comscore.com>. For updated data visit <https://otalliance.org/browser/data.html>.

APPENDIX B - FUNCTIONAL RULES AND NOTICE LOGIC

The following is a rough draft of sample rules to create. Sites need to address the corner cases of users of legacy operating systems and browsers, as these versions may inhibit upgrading – or the process might create support and technical issues. Based on this and other dynamics including the low traffic of customers, certain customer groups may be ignored or updated to a less than current version (but more secure than their current browser).

1. If OS = XP & browser = IE, version < 8, update to IE 8
2. If OS = Vista or Windows 7, browser = IE, version < 9, update to IE9
3. If browser = Firefox and version is <6, update to 6
4. If browser = Chrome and version is <13, update to 13
5. If browser =Safari and version is < 5.0 update to 5.1
6. If browser = Opera and version is <11.5, update to 11.51

Links are independent of the specific version and created by the browser vendors. See <https://otalliance.org/browser/updateslinks.html> for links to browser update pages.

Operating System / Browser Compatibility Matrix – as of 10/10/11 ^{5, 6}							
	OS 10.3	OS 10.4 Tiger	OS 10.5	Mac OS > 10.5.8	XP SP1	Vista	Win 7
Google Chrome	Not supported			Chrome 14	Chrome 14	Chrome 14	Chrome 14
Windows IE	Not supported				IE 8 ⁷	IE 9	IE 9
Mozilla Firefox				?	FF 7	FF 7	FF 7
Apple Safari					5.1	5.1	5.1
Opera	9	10	?	11.5	11.5	11.5	11.5

Note: data above does not cover edge cases of operating systems not listed and only applies to Intel-based Mac systems.

⁵ See <https://otalliance.org/browser/updateslinks.html> for the latest updates before coding.

⁶ Note browser vendors use multiple version number schemas and may change frequently

⁷ For users Windows XP with Service Pack 1 they cannot update to IE 9 or newer versions. In this scenario, it is recommended to encourage them to update to IE 8, which affords significant security and privacy features over IE 6 and 7.

APPENDIX C - RELATED RECOMMENDATIONS & RESOURCES

The following is a summary of related best practices all sites and business are encouraged to consider, offering increasing brand, domain and user protection from online exploits.

Email Authentication - In 2003, several industry efforts emerged to help address the rising tide of spam and forged email. These efforts ultimately produced two key email authentication technologies: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), each of which received experimental RFC status from the Internet Engineering Task Force (IETF). Organizations around the world have adopted SPF (including the Sender ID Framework [SIDF]) and DKIM as complementary approaches to aid in the prevention of malicious email. After several years of real world deployment, early adopters have recognized the technical value from the combined implementation of *both* SPF and DKIM.

<https://otalliance.org/resources/authentication/index.html>

Extended Validation SSL Certificates - Extended Validation SSL Certificates (EV SSL) were introduced in 2006 in response to phishing exploits, look-alike websites and fraudulently obtained SSL Certificates. EV SSL requires a thorough verification and audit process that helps to prevent deceptive and illicit entities from obtaining a certificate. EV SSL Certificates provide differentiation and recognition to the organizations that obtain and publish them. This differentiation is highlighted by displaying a green identifier as a visual trust indicator in the browser's address bar. EV SSL is now supported by all leading browsers including Internet Explorer, Firefox, Chrome, Opera and Safari. <https://otalliance.org/resources/EV/index.html>

Data Breach & Data Loss Incident Planning - OTA advocates all that businesses create an incident response plan and be prepared for the likelihood they will experience a breach or data loss in the future. The fact is that breaches happen – and never at a good time. Rather than be lulled into the belief it will not happen to your business, a well-designed breach plan is emerging as an essential part of regulatory compliance, demonstrating that a firm or organization is willing to take reasonable steps to protect data from abuse. Doing so is good business. Developing a plan can help to minimize risk to consumers, business partners and stockholders, while increasing brand protection and the long-term viability of a business.

<https://otalliance.org/resources/Incident.html>

HTTP Strict Transport Security (HSTS) / Always On SSL - HSTS offers full end-to-end encryption (known on the web as HTTPS or SSL) and is an effective deterrent to such threats from wireless snooping or hot spot hacking.

Anti-Malvertising Guidelines - Malvertising is the cybercriminal practice of injecting malicious or malware-laden advertisements into legitimate online advertising networks. It is a growing threat to the integrity of the ad supply chain and vector to distribute malware to unsuspecting users.

<https://otalliance.org/resources/malvertising.html>

ACKNOWLEDGMENTS

This initiative has been made possible with input and advice from numerous individuals and organizations committed to self-regulation on online trust. Special thanks to the leadership of Mike Hammer of AG Interactive, Eric Davis Google, Gus Maldonado of PayPal, Geoff Noakes of Symantec, Dave Lewis of Message Systems, John Scarrow of Microsoft, Joe St Sauver, Ph.D., University of Oregon and Internet2, Sal Tripi of Publishers Clearing House and Richard Weaver of comScore. In addition this effort could not have been possible without the efforts of Mark Goldstein, OTA strategic advisor, OTA staff including Liz Shambaugh, Debbie Mac and Craig Spiegle and to representatives of the browser community.

About The Online Trust Alliance (OTA) <https://otalliance.org/>

OTA's mission is to develop and advocate best practices and public policies which mitigate emerging privacy, identity and security threats to online services, organizations and consumers, thereby enhancing online trust and confidence.

By facilitating an open dialog with industry, business and governmental agencies to work collaboratively, OTA is making progress to address various forms of online abuse, threats and practices which threaten to undermine online trust and increase the demand for regulations.

Formed in 2004 to counter email deception and online abuse, today OTA is the only global organization representing the Internet ecosystem supporting user choice and control, protection of critical infrastructure, privacy and data governance, promoting marketing best practices, balanced legislation, benchmark reporting and self-governance.

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA) nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other advice, please consult your attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit <https://otalliance.org/browser>.

© 2011 Online Trust Alliance. All rights reserved.