OTA
Online Trust Alliance

OTA members have developed the following draft of Online Trust Principles with input from OTA affiliate organizations as well as representatives of U.S. and international regulatory agencies. This joint undertaking exemplifies industry and government collaboration and a shared commitment to both consumer protection and self-regulation.

OTA will work with its industry partners and these partners' related organizations to secure endorsement of these Principles. It will also utilize these organizations to help drive awareness and adoption of the Principles worldwide. OTA welcomes input from ALL interested parties and organizations. Comments should be sent on letterhead to staff@otalliance.org. Unless requested by the submitter, OTA may at its discretion, make all submissions public.

After a 30-day comment period and subsequent review, OTA will publish these Principles and call on leading ecommerce and banking sites to implement them within nine months.[1] In addition, OTA will encourage ecommerce sites of all sizes to implement the principles most appropriate to the protection of consumers and their employees.

OTA's position is that these Principles should be mandatory for all public and private companies engaging in ecommerce and online banking, unless otherwise stipulated by their respective regulatory agencies. The draft Principles are consistent with FTC and European mandates and guidelines that stipulate that businesses apply "reasonable security" in protecting sensitive personal information.

The draft Online Trust Principles are broken down into three categories:
1) Infrastructure, including protection of servers, web sites, desktops and mobile devices;
2) Data that includes both sensitive and Personally Identifiable Information (PII);
3) User Choice, Control and Privacy.

Infrastructure:

1. Maintain and audit all corporate IT systems and desktops including:
    a. Adhering to compliance policies as stipulated by regulatory agencies and / or those required by organizations which they are members of.
    b. Regularly scaning for vulnerabilities, End-Of-Life (EOL) software, and updated security patches for operating systems, applications, browsers and browser plug-ins / add-ons. It is understood that the installations of such updates may be deferred pending security and compatibility testing.
    c. Ensure implementation of protection against phishing, spam, viruses and malware including but not limited to anti-spyware, anti-malware, takedown services and fraud monitoring programs.
2. Upgrade existing Secure Socket Layer (SSL) certificates to Extended Validation SSL Certificates (EV SSL) for all ecommerce or online banking sites. EV SSL Certificates are designed to provide consumers increased confidence and trust of the sites they visit by providing a green identifier in a browser's address bar. Any site interested in providing users a stronger assertion on their identity and their authenticity is encouraged to adopt EV certificates upon the expiration of their existing SSL certificates.

[1] As denoted by the top 100 online retailers as posted by Internet Retailer, financial institutions and Fortune 500. Ecommerce sites are those in which credit cards are utilized.

3. Establish a domain name registration and Domain Name System (DNS) management and monitoring program with incident handling procedures. These measures help prevent consumer deception and detect brand infringement, before deceptive sites are deployed.[2]

4. Complete a security audit of all third party code, plug-ins, applications and scripts prior to implementation. These audits shall include ongoing exploit monitoring. In addition, analyze and monitor any third party site that tightly integrates into their site for transactions or other direct-to-customer services.[3] Such code and linkages are widely used, yet continue to be one of the leading attack vectors, exposing users to malware, click-jacking, cross-site scripting and related exploits.

5. Implement email authentication across all corporate and product domains, including those not used for email yet recognizable to the consumer. Senders and domain holders must implement production Sender Policy Framework (SPF) / SenderID (SIDF) records and/or Domain Keys Identified Mail (DKIM) signatures.[4]

6. Recommend and encourage users of transactional web sites (ecommerce and banking) to upgrade to the most current browser version. Such updated offer enhanced security and privacy controls. Sites should help educate users by providing information, alerts and links. Furthermore sites and ISPs are urged to discontinue support for end-of-life browsers.[5] To help assist and aid domain holders, OTA will provide sample landing and referral pages for sites to incorporate or point to users to.

Data:

7. Recognizing the likelihood of potential data loss, sites shall create and implement proactive measures including the monitoring of data moving through the network (such as, email, copying off the network, or onto USB drives). In addition sites shall create and broadly publish for all employees a data loss contingency plan including mechanisms to contact impacted users in a timely fashion to help prevent and detect identity theft. It is recommended that such plans be shared with employees and data partners in advance and updated on an annual basis.

8. Encrypt all customer data files that include PII, including but not limited to email, opt-out and unsubscribe lists, data on external devices and or data transmitted to partners and service providers.

[2] Threat of “drop catching” http://www.cadna.org/en/newsroom/press-releases/drop-catching-study

[3] Examples include but are not limited to shopping carts and event registration services.

[4] Production SPF records do not include “?all” records as by design they are disregarded and ignored by receiving networks and frequently utilized by spammers and deceptive mailers.

[5] The following is an example of the user experience when visiting a site which no longer supports the End-Of-Life (EOL) browser being used. User will be presented with a landing page providing a “teachable-moment”, informing them of the risks of using an outdated browser and provide links for upgrading. Sites may wish to disallow login for such users with EOL browsers. While it may not be permitted without user consent, sites may consider offering the ability of providing users a scan of their systems for such vulnerabilities as outlined in Principle #1.

User Choice, Control and Privacy:

9. Require first party site privacy obligations and data policies be honored by all third party content and ad providers. For example, it is reasonable to provide users the assurance that upon visiting a site, any use of data shared retained, tracked and profiled by third party content providers is consistent with the data and privacy policies of the site the users choose to visit.

10. Provide consumers comprehendible and discoverable notices of any privacy, email, data and opt-in policies including their data sharing policy with third parties and affiliates. Such notice should be on the first screen or page of the site's policy and linked as appropriate to expanded policies. It is suggested such polices follow a common format and be written for the 6th grade reading level to maximize readability across all user segments.

11. Provide consumers an expectation on the frequency and content (subject and relevancy) of email they will be receiving upon signup or registration. As an example, a customer would be informed upon registration a range of the number of emails they will receive monthly related to the product or service they enrolled to.

12. Adopt third-party security, privacy and opt-out seal and certification programs, providing consumers an identifiable mechanism to understand the privacy assertions of the sites they visit.[6]

Updated versions of this document will be posted at
https://www.otalliance.org/resources/principles.html

Comments should be sent on letterhead to staff@otalliance.org. Unless requested by the submitter, OTA may at its discretion, make all submissions public.

[6] Such programs are offered by the Better Business Bureau, TRUSTe and VeriSign as well as other third parties.