OpenDnsAndUribls

I'm using OpenDNS and seeing SURBL or URIBL rules firing on non-spam

OpenDNS is a service that changes the responses to some DNS queries in order to prevent users from visiting spam, phishing, etc., sites. It also has a "typo correction" feature that directs mistyped domain names to custom sites controlled by OpenDNS instead of sites controlled by typosquatters, phishers, etc.

When using SpamAssassin with an OpenDNS nameserver it's important to disable the typo correction feature in OpenDNS, or the responses to non-matching SURBL or URIBL queries will be rendered incorrect. The reason is that the OpenDNS nameservers return an IP address of their own web site in those cases, and that modified IP address will have an incorrect effect on SURBL/URIBL list identification that depends on where the bit patterns happen to be in the modified response.

SURBLs and URIBLs will work with OpenDNS if their typo correction feature is disabled on servers or clients doing SURBL queries. Alternatively, consider using non-OpenDNS nameservers on those systems.

(thanks to Jeff Chan for this text)

UPDATE - 2007-01-30

- The OpenDNS team has automatically turned off typo correction for SURBL and URIBL. See the blog entry at OpenDNS.com for more details.

UPDATE - 2008-01-29

- It's been reported that Verizon is doing something similar, whereby requests for non-existent DNS records are responded to with pointers to Verizon services.