

The Solution to Unsolicited Commercial Email (“UCE”)

Background

The Internet started as a small network of trusted individuals in academia, where peer pressure and professionalism governed its use. The mechanisms developed within this environment became vulnerable as a result of market forces introducing opportunity to marketers, since there are no facilities to enforce accountability or trust.

Due to the early Internet architects' open design, a single sender can send copies of a single message to an unlimited number of recipients. The result put the recipients and third party servers under a heavy load, introducing hardware and bandwidth costs. This has created a false economy, which currently drives the UCE problem.

Given that the abuse of the public network is a social problem, the solution must comprise legal, self-regulatory, and technical solutions. There are legitimate uses of the public infrastructure for the delivery of commercial email and protecting these should be a requirement for any solution.

Legal Framework Recommendations

Any legal solution must set the guidelines between what is acceptable use and what is abuse of the public infrastructure. With the cost of delivery borne by the recipient (or ISP), the abuse of others' infrastructure without prior permission must be discouraged by the threat of legal liability.

The marketing industry needs to present self-monitoring regulations. These regulations must "have teeth" and meet the requirements of the large Internet Service Providers (ISPs). Any self-regulations that allow the use of opt-out (messages sent without prior consent) should not be acceptable by law.

Even with a strict legal framework and effective industry self-regulation, some illegitimate senders will simply move to more lax jurisdictions and continue operations (as has happened with online casinos and gambling operations). For these cases, prophylactic anti-spam software will still be required.

Technology Framework Recommendations

Technical solutions must provide the recipient (such as an ISP, an enterprise, a government agency, or individual) with the ability to "own" their inbox, and assert the trust and accountability that was once a part of the small Internet culture, and has now been diluted by growth. To this end, software should enforce the preferences of the recipient and allow them to discard messages which they choose not to receive. A comprehensive approach is the most effective in combating spam, with combinations of advanced text classification, message heuristics, and sender identity emerging as the basis of the technical solution. These are explained further below:

* Text Classification - Algorithms that allow a machine to determine whether a set of text belongs to a specific class (such as "spam" or "good" mail) based on its similarity to previous samples. So-called Bayesian classifiers are becoming increasingly accurate at identifying spam and non-spam, using techniques developed for machine learning.

* Message Heuristics - Tests against messages that identify obfuscations used by spammers to hide the message content, with the intent of bypassing Text Classification systems. Messages containing obfuscations are never of value to a recipient.

* Sender Identity –Recipient-created "friend lists", which will bypass any other form of filtering, require strong systems to prevent the sender from forging their identity. Currently, there are technical proposals that leverage the Internet's existing infrastructure to provide these services; these are expected to roll out in 2003.

Once the inbox owner is suitably empowered, the marketing industry must offer enough value to the recipient to make their content relevant to the recipient and to allow their communications to be delivered. This is a market dynamic which will enforce the cost-shifting element of the solution, as only relevant messages will be received.

Future Trends

As the combined force of legislation, empowered recipients, and self-regulation take effect, an effective model will emerge for legitimate commercial emailing. The hardcore "spam gangs" will move to unregulated jurisdictions, and the problem will settle into the same model as anti-virus. This move will make identifying UCE easier, and the problem will become a minor annoyance, instead of a major disruption.

This model will see ISPs competing on their ability to enforce their recipients' receipt preferences, while potentially generating revenue by providing a marketing channel to legitimate email marketing firms (i.e. ones who only send with consent).

About ActiveState

ActiveState enables IT professionals and enterprises to increase productivity and organizational efficiency. The Company's PureMessage product empowers organizations to take control of their email communications to protect against spam and viruses, and to enforce email policy. Additional information on ActiveState's industrial strength anti-spam software for enterprises and professional tools for programmers is available at: www.ActiveState.com.

