Actrix Networks Ltd
Wellington
NZ

ISP SPAM code of Practice
May 2007
Version 0.95

Comments

Definitions – Sender Policy Framework is not well adopted; what will change behaviour here?

Section 4.1 part F talks about providing a "non-technical overview" of the Spam filter which is pretty vague. Too little information and it's not much use, too much and Spammers can read it and try to devise ways of getting around filters. I presume how much info we choose to provide is at our discretion as long as we clearly state Spam filtering is on by default and provide at least some generic information on how it works?

Section 4.1 part F (g) – False Positive is a geeky term; why not use something the public understands or define the technical terms somewhere; (guess depends on the audience?)

Section 7.3 talks about disconnection or suspension due to open proxy's and relay's whether it is with the customers knowledge or not but there is no mention of zombie / botnet / infected PC's which isn't an "open" relay or proxy as such but which do allow remote access to particular individuals and can be used to send Spam (among other things)? The example AUP does have a generic clause regarding 'hosting a device or service that allows E-mail to be sent' that would cover open proxy's, relay's and more but it's only in the example? Or is the open proxy / relay wording covered in these circumstances?

Section 9 regarding best practices states "Service Providers should not distribute Customer Premises Equipment...that is so configured by default as to be susceptible to being remotely administered..." Does this mean routers etc that allow remote access by default but how would this be interpreted for equipment that has a design / security flaw revealed that allows remote access with a little persuasion? By default it's not configured to allow remote access but due to a flaw it is still susceptible? The ISP has to rectify the situation? The manufacturer? Both? Neither? Irrelevant?

Section 9 regarding best practices also states we need to prevent accounts from being registered without direct human intervention…Does this mean the customer must be human? If this means the ISP must have human intervention, then it won't happen?

The example AUP section X.6 describes the companies right to terminate the service and talks of a pro-rata refund for pre-paid charges and the right to levy a reasonable fee for costs incurred as a result of the conduct that resulted in suspension but how does this affect other customer obligations such as term contracts, disconnection fees, contractual / rental / HP equipment provided to the customer, etc? Assume T&C kick in?

What happens if we state we comply with the ISP Spam Code of Practice but end up in breach in some way?

Our 2c worth.
Cheers
George

George Reedy
Group Managing Director
ACTRIX INTERNET (ISP)