

Dear Sir,

We are a domestic software vendor who provides anti-spam and anti-virus managed service to the market. Regarding the consultation paper of "Proposal to Contain the Problem of Unsolicited Electronic Messages", we should like to submit our comments to the following points.

Point 34.

As we are providing managed service of anti-spam and anti-virus, we have collected the figures regarding spam mails from our servers. We believe that these figures could give a solid statistic to measure the impact of the anti-spam problem. The figures are taken every month from the statistic reports of our anti-spam servers. The figures shows that on average, 46% of incoming mails are spam mails, and 23% network traffic is for spam mails.

Point 68.

We agree to have the codes of practice, but we are doubt on the result of the codes of practice. In general, the codes of practice can only be applied to the registered organizations, such as operators. In case of the violation of the codes of practice, these organizations could be held responsible for their mistakes. Nevertheless, spammers are not registered and are transparent in the internet. It is very difficult and costly to get the spammers. Not saying spam mails, we are still receiving junk faxes everyday. Therefore, the effectiveness of proposed solution - point 68, is not good enough.

Point 69.

We agree to encourage the industry players to take actions to stop spam mails. However, the core problem will be who is going to pay for it. Before we could identify the source of money, industry players may find it difficult to take such actions. Even we could get the funding for it, it turns out to the next question of who is going to monitor if the actions are taken properly. Therefore, having the solution in the way of "encouragement" could not solve the problem.

Point 70.

Having the industry players to get together and take some actions to stop spam mails is a commercial act. Obviously, the effectiveness of the commercial act depends on the profitability of the market. In that case, such alliance will be appeared or not be appeared based on the natural rule in the business world.

Point 78.

The following are the available technical solutions that used in anti-spam solutions. Based on our R&D experience, we have marked the effectiveness of each solution. The legend of the mark is (1-Good, 2- Normal, 3-Poor).

Spam Mail Scoring Card (1)
Two Score Threshold (1)

Spam Quarantine Individual Control Message (1)
Challenge/Response Approaches (2)
International Anti-Spam Networks Integration (1)
Content Analysis, Keyword and Pattern Matching (3)
Heuristic Filtering (2)
Signature and Hash-Based Filtering (2)
Bayesian Filtering (3)
DNS Blacklist Filtering (1)
Blacklisting and Whitelisting (1)
Open Relay Database (1)
Open Proxy Database (1)
Known Spammer Database (2)
Spam Policy Abuse (3)
IP Based Detection (2)
Domain Based Detection (3)
Real-time Blacklist Lookups (2)

In addition, we have listed the International Anti-Spam Networks that most of the spam solutions are using.

Vipul's Razor
DCC – Distributed Checksum Clearinghouse
Pzorz
ORDB - Open Relay Database
MAPS – Mail-Abuse Prevention System
SpamCop
DSBL – Distributed Server Boycott List
SpamHaus
NJABL – Not Just Another Bogus List
RFCI – RFC Ignorant

Point 83.

We think having legislative approach to combat spam is a necessary approach. With the legislation, government can at least trace the spammers and hold them responsible. However, there are a number of limitations in such legislation. First of all, most of the spammers are not in HK. Secondly, it is very difficult to define if the mail is spam or ham. In fact, some mails are spam to you, but it may be the ham mail to others. The legislation cannot prevent the e-marketing activities. Therefore, we think it is necessary to have legislation on anti-spam. However, just like the computer virus, it cannot solve the spam problem entirely.

*** The email has been scanned by AxiScan ***