MEMORANDUM

“Characterisation of actions to combat spam”

Analysis of responses to questionnaire

INDEX

1. Background to questionnaire

In May 2008 an inquiry was launched to make a characterisation diagnosis of actions taken by Internet service providers and providers of email services combating unsolicited communications (spam).

It was intended that this questionnaire be extended to all ISPs registered[1] with ANACOM. Of a total of 36 companies, responses were received from 18[2], on which the present report is based.

The questionnaire form in annex was published on ANACOM's website[3]. Requests to participate and respond were also made by official notice.

Because this is the first time that ANACOM has done this questionnaire, it was decided to use open questions without restricting the possible answers. While this method can contribute to some divergence as a result of the necessary interpretation of responses, in order to group them so conclusions could be drawn, the alternative option, where fixed options are given for the responses, might be seen as inappropriate to the reality and experience of the national companies.

The questionnaire form was based on the questionnaire promoted by ENISA[4]. Besides the level of confidence that this fact brings, the questionnaire form received positive evaluations by some of the operators which were contacted previously.

The diagnosis resulting from the inquiry is intended as a first step in setting out, in conjunction with the ISPs, a course of action for combating spam.

[1] Operational Internet access Service providers 1st quarter 2008 Service provider of Internet Access Broadband Fixed 1st quarter 2008 Providers offering Mobile Broadband Services Mobile 1st quarter 2008

[2] Companies that responded to the survey: Bragatel, Cabovisão, PT Comunicações, PT WiFi, PT Prime, ReferTelecom, SemCabo, Tvtel, Vodafone, Cyclopnet, TMN, Connex, Fleximédia, Sonaecom, NSFI, Zon TV Cabo, Nortenet, Claranet

[3] Home: Electronic Commerce: Spam Combating unsolicited communications: Questionnaire on combating unsolicited communications - http://www.anacom.pt/render.jsp?categoryId=275882&languageId=1

[4] Provider Security Measures - ENISA 2006

This inquiry was also held with the objective of formulating a basis for ISP contacts, allowing improved interaction for future actions to be taken in combating spam.

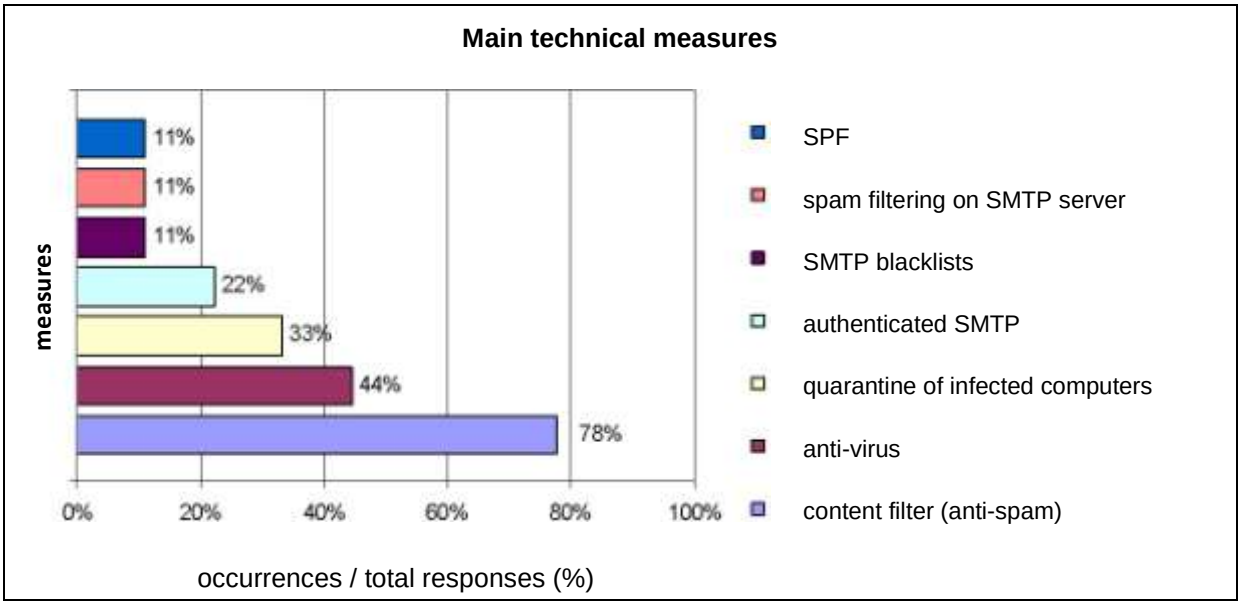
2. Analysis of responses to questionnaire

Given that the questions were open, multiple answers were possible (various aspects indicated in the same answer). As a result, the sum of the percentages referred to during the analysis are not 100%.

2.1 Question 1 - What measures have you taken with a view to promoting the security of the services provided?

The responses were divided into two types of action - technical measures and organisational measures.

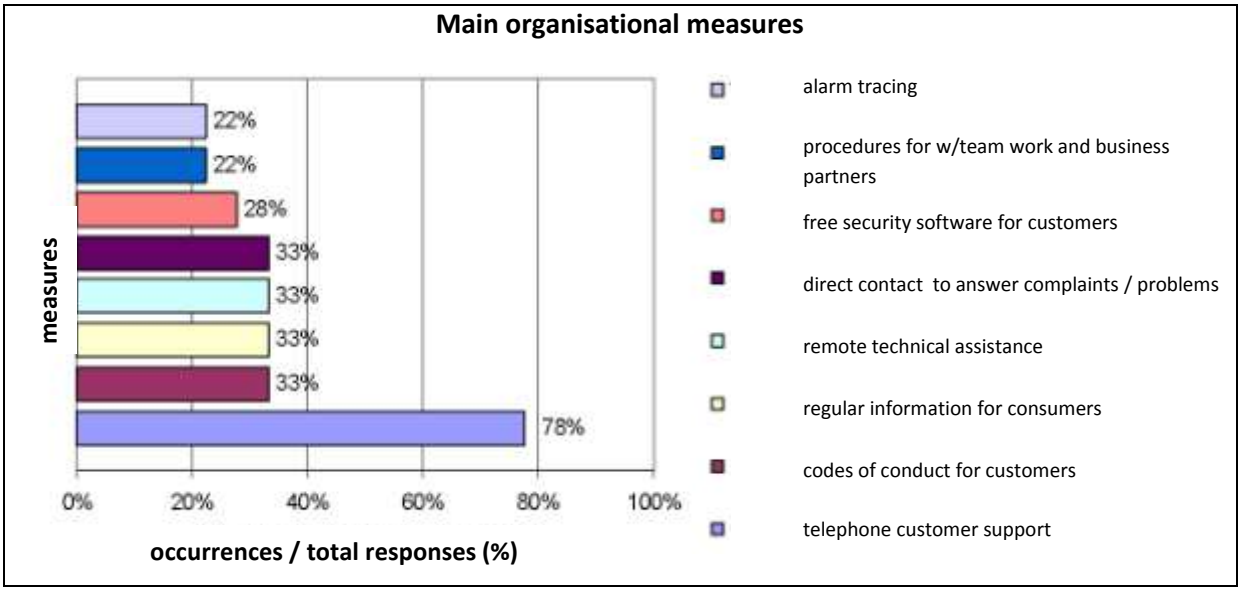
With respect to the technical measures, emphasis is given to anti-spam and anti-virus filters, with 78% and 44% of the companies referring to these measures respectively.



SPF Sender Policy Framework[5]
SMTP Simple Mail Transfer Protocol[6]

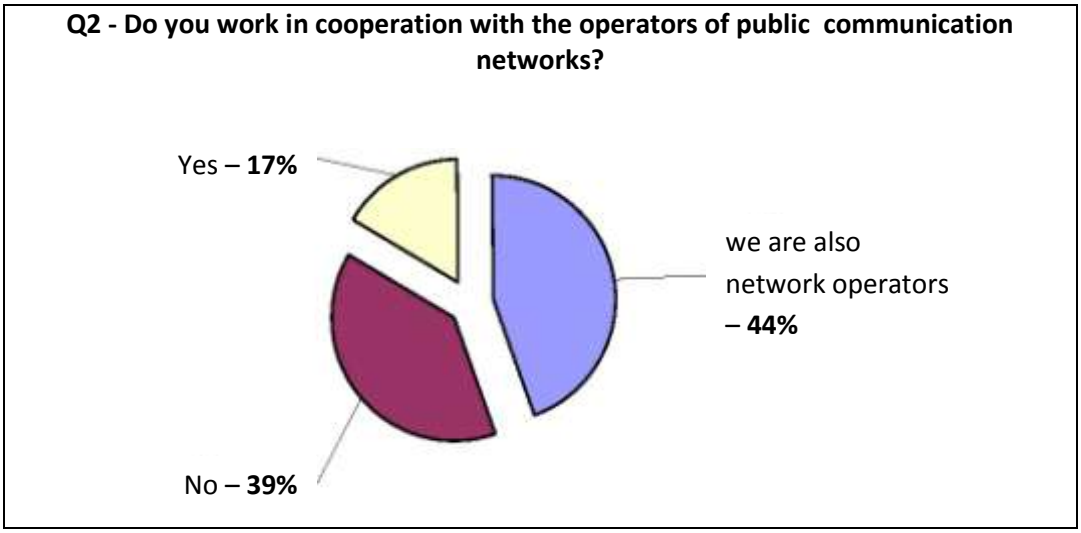
[5] Sender Policy Framework or SPF is a system that prevents other domains (the Internet address) from sending unauthorised emails in the name of a domain.
[6] Simple Mail Transfer Protocol or SMTP is the standard protocol for sending and emails over the Internet.

In terms of organisation measures, of particular relevance are the provision of technical support to customers over the telephone (78%) and the existence of codes of conduct or rules for the use of services, with reference to the question of spam (33%).



2.2 Question 2 - In executing these measures, do you work in cooperation with the operators of public communication networks?

44% of respondents affirmed that the provision of Internet access and e-mail is combined with the management of the network, whereby it follows that the action is concerted. Of the others, the majority (7 companies out of 18 respondents) act in a manner that is not coordinated with the network operators.



2.3 Question 3 - How do you keep updated with respect to developments in security and costs inherent in the adoption of an appropriate level of security?

78% stated they acted primarily according to legislation, including reference to European standards.

The second most significant factor cited was "standard industry practices" (61%) and third the "best international practice" (39%).

Reference was also made to "listening to customers and partners" (22%) and specialty websites (17%).

It may also be inferred that the combat of spam is encompassed by legislation that is clear to all stakeholders and by cooperation in terms of disclosure and adoption of "best practices".

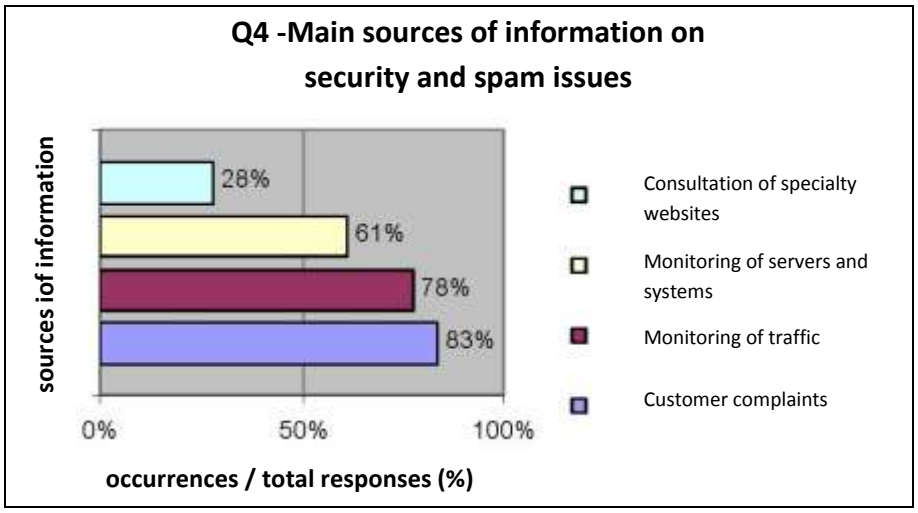
national and international legislation (including European standards)	**78%**
standard industry practices	**61%**
international best practices	**39%**
"listening" to customers and partners	**22%**
specialty websites	**17%**
knowledge resulting from actual experience in the activity	**6%**
protocols with national and international bodies	**6%**

2.4 Question 4 - How do you keep informed about security issues and SPAM?

The key factors of information on the issues of computer security and spam are:

- Customer complaints (83%)
- Monitoring of traffic and systems (78% and 61% respectively)
- Consultation of specialty websites (28%)

Complaints from customers provide the main source of information on security issues. It is also noted that ISPs are active in ensuring security through the monitoring of traffic

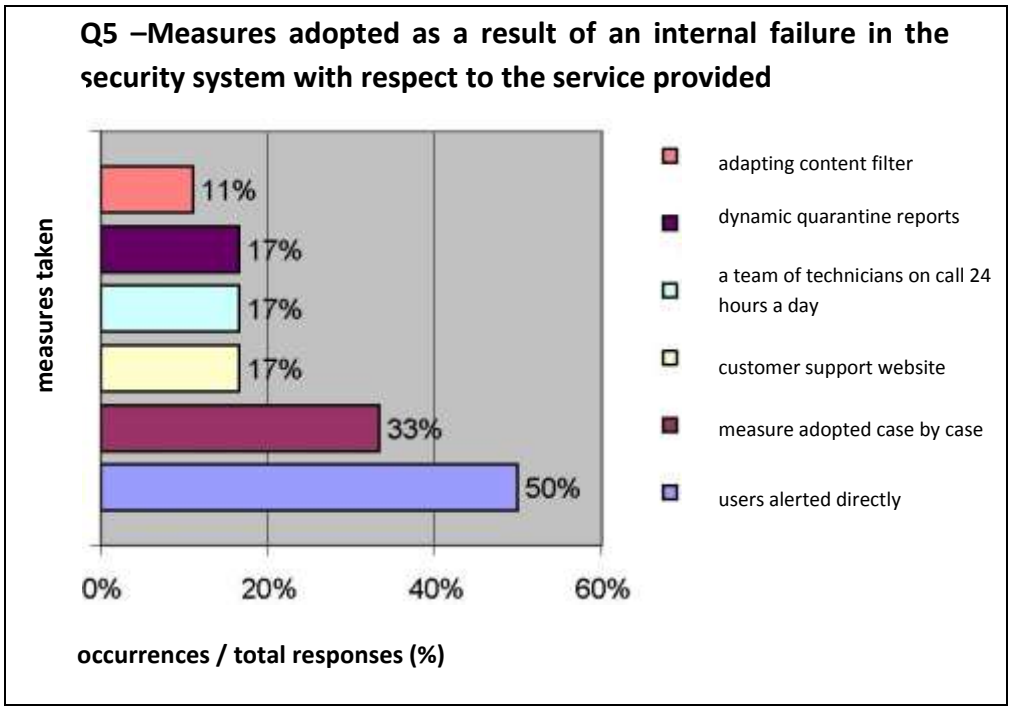


2.5 Question 5 - What measures do you take when a failure is detected in the security system with respect to the service you provide?

The responses give the perception of there being some difficulty in interpreting this and the next question, because in some way one complements the other. The aim is to gauge with respect to this question what the ISP would do as a result of failure originating in their own system and in question 6 what they would do in cooperation when failure originates in the system of a third party. Given these facts, and with respect to this question and question 6, the responses have been set out according to the aim of each question.

The action resulting from an internal failure, leads the ISP to:

- Alert users directly (50%)
- Provide support through a team of technicians on call 24 hours a day (17%) or through information on the website (17%)
- Maintenance of dynamic quarantine reports with the occurrences (17%) and adaptation of the content filter (11%)

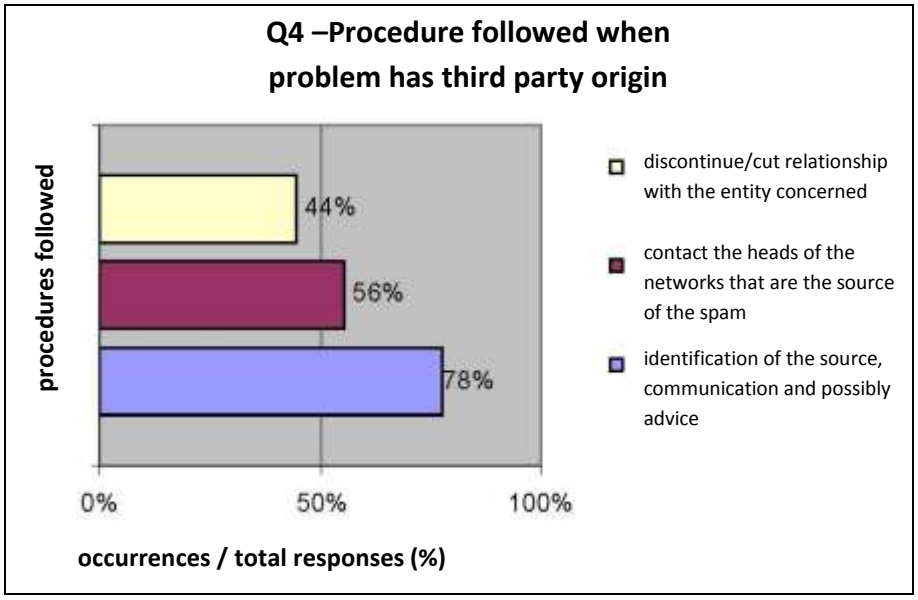


2.6 Question 6 - What procedure is adopted, when the adoption of suitable measures do not depend on your company?

The first measure taken by the ISP when the security breach has external origins is to identify the source, communication and possibly advice (78%). Sometimes ISPs contact the heads of the networks that are the source of the spam (56%). The severest measure, adopted in extreme cases, is the discontinuing service with the entity concerned (44%).

It can be concluded that the route adopted in most cases is dialogue and advice. However this course of action is not always possible and the entity that is the source of the spam may be cut off when it appears on blacklists. From this it can be inferred that it is positive to promote white lists for companies which engage in serious

marketing and that sometimes, when such lists are not feasible, these companies are confused with "spammers".



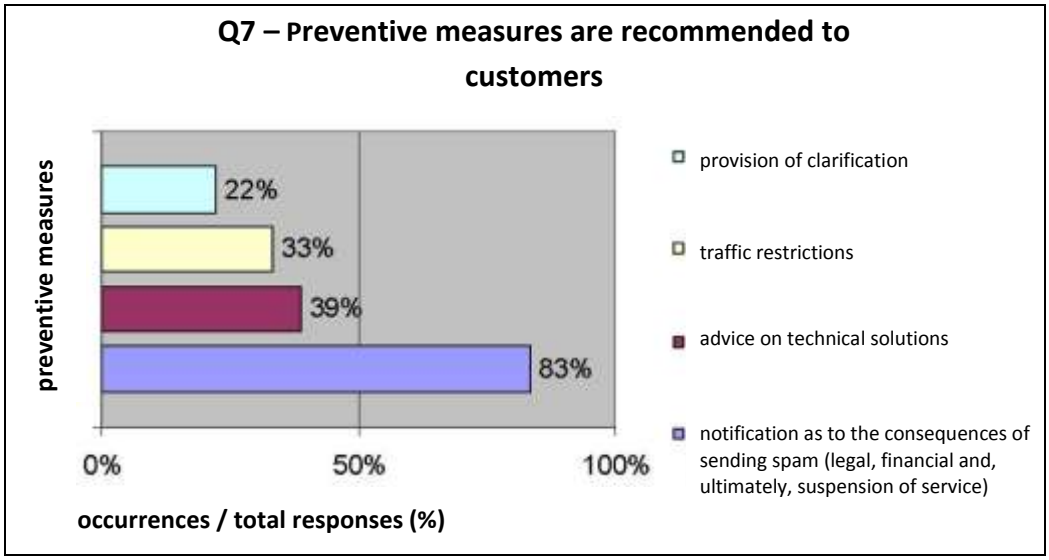
2.7 Question 7 - What preventive measures are recommended to customers with respect to the sending of SPAM?

Spam prevention work is based mainly on the promotion of codes of conduct or of good practice in the use of services. When spam is detected, the first initiative is to give notification as to the consequences of this practice (83%), these consequences may be legal, financial and, ultimately, suspension of service.

The ISPs also opt to give technical advice (39%) and for the provision of clarification of information (22%).

In 33% of cases restrictions are placed on traffic, which means making use of blacklists.

From the responses received, note should be made of the positive effects that the codes of conduct can have as a measure which deters engaging in spam.



2.8 Question 8 - What measures are taken to help customers from receiving SPAM?

Note is made of the role of ISP self-regulation with respect to protecting customers from spam.

Accordingly, 16 of the 18 respondents claim to provide spam filters free of charge as part of their e-mail service.

Of the 18 respondents, 7 reported offering anti-virus and 5 gave advice on good practices in order to avoid spam.

This result points to evidence that there is room for more initiative in advising on the adoption of best practices to avoid the spam, given that this measure does not yet figure very significantly in the overall raft of the measures taken to protect customers.

Moreover, it can be concluded that there is a "reluctance" to promote black, white and gray lists. Accepting that these must be constantly updated to be useful, an exchange of information between ISP which kept these lists updated could benefit the action in the fight against spam.

Q8 - Main measures taken to protect customers from receiving spam

offer of free spam filter	**89%**
offer of anti-virus software	**39%**
advice on good practice to avoid spam	**28%**
blocking with use of blacklists	**17%**
customer technical support	**11%**
monitoring of the performance and quality of services and network	**11%**

2.9 Question 9 - What preventive measures are taken to combat cases of identity fraud? Is a mechanism for authentication implemented?

5 companies admit not implementing any authentication mechanism. 12 companies perform SMTP authentication and 5 publish SPF information.

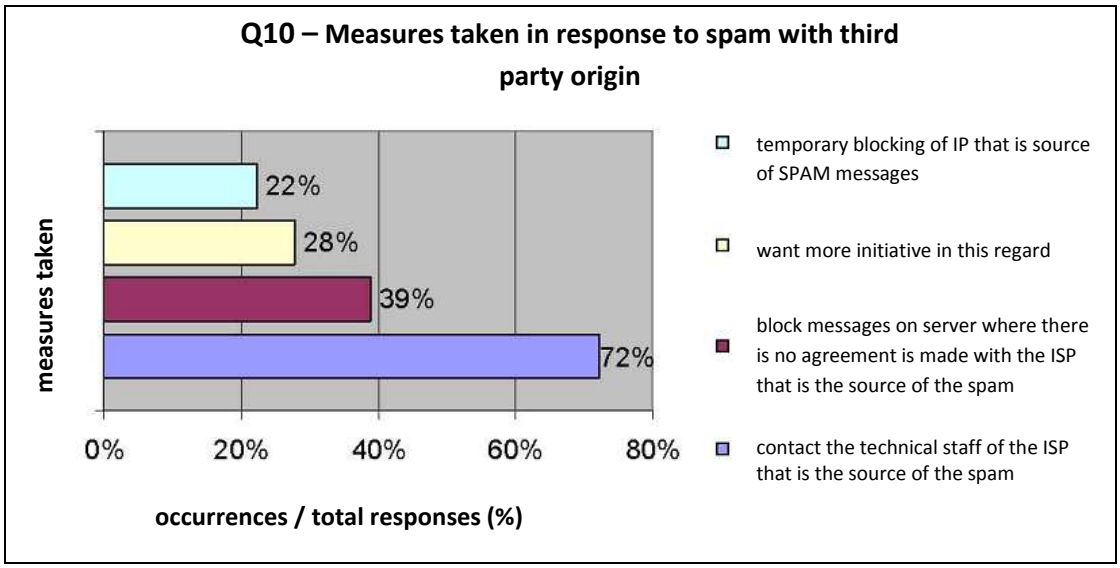
Q9 - Preventive measures taken to combat identity fraud

SMTP authentication	**67%**
no authentication mechanism implemented	**28%**
publication of SPF information	**28%**
SIDF	**11%**
single sign-on (SSO)	**6%**
DKIM for outbound email	**6%**

2:10 Question 10 - What measures are taken when it is found that SPAM messages originate from service providers of access Internet based in the country? And if they come from service providers based in Europe? And also from service providers based outside the European Union?

Virtually none of the respondents defined courses of action with distinction in terms of the geographic source of the spam. Even without this distinction, 72% reported that they contacted the technical staff of the ISP that is the source of the spam. 11 of the 18 reported blocking messages in the event that no agreement is made with the ISP that is the source of the spam. It is shown that 28% want more initiative in this regard.

This data is indicative of the important role that ISPs have in combating spam. In fact traffic is routed through them, so that the fact that they desire more initiative should be taken as an opportunity for concerted action.



3. Principal Conclusions

- The establishment of codes of conduct or rules for the use of services is one of the main organisational measures taken to promote the security of provided services.
- The measures taken to promote the security of services are not always coordinated among service providers and network operators.
- Legislation appears to be the main point of reference when it is necessary to define the level of security; The second and third factors which are cited as forming the basis of this decision are the standard practices of industry and international best practices.
- The main sources of information for the identification of computer security and spam issues are, in descending order of importance, complaints from customers, traffic monitoring and consultation of specialist websites.
- When there is a failure of internal security, particularly related to spam, the ISPs take measures as follows:
    - Alert users,
    - Support through a team of technicians, sometimes operational 24 hours / day,
    - Adapt content filter and quarantine reports adapted to the incidents.

  This action shows that the ISPs have a proactive and attentive attitude.
- When the security failure has its origin with third parties, the most common action is to identify the source, alert it and possibly provide it with advice. Sometimes ISPs contact the heads of the networks that are the source of the spam. In extreme cases, i.e. when the failures endanger the operation of the system and / or the heads of networks do not cooperate, ISPs choose to discontinue the service which gave origin to the security failure.
- Some of the respondents indicated that they made use of blacklists. The discontinuity of service in extreme cases, reveal the contribution, in addition to blacklists that identify the offenders, that white lists have in identifying those who are examples of good practice.
- Spam prevention work is based mainly on the promotion of codes of conduct or of good practice in the use of services. When spam is detected, the first initiative is to give notification as to the consequences of this practice; these consequences may be legal, financial and, ultimately, suspension of service.

- Most ISPs offer anti-spam and anti-virus for free, which reflects an attentive and active position with regard to security.
- There are still ISPs which do not implement any authentication mechanisms as a way of combating cases of identity fraud.
- The answer to the question on measures taken as a consequence of spam messages shows that ISPs want greater initiative in this regard, Sometimes, when there is a lack of understanding with the ISP that is the origin of the spam, the practice is to block traffic. From this conclusion it can be deduced that there is scope for concerted action between the ISPs to identify and combat "spammers".