ENISA 2009 spam survey

Measures used by providers to reduce spam

December 09

What Are the Measures Used by European Providers to Reduce the Amount of Spam Received by Their Customers?

Third ENISA Anti-Spam Measures Survey

enisa
European Network and Information Security Agency

About ENISA and this work

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

This report is based on the responses given by anti-spam managers and security managers from European service providers. ENISA would like to thank them all for their excellent contributions and insights.

ENISA would like to thank IDC CEMA (John Gole and Michael Vorisek) for their professionalism and dedication that resulted in this report.

Contact details:

For contacting ENISA on spam-related matters please use the following details:

Pascal Manzano, Expert Network Security Policies, ENISA

Internet: http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Table of Contents

List of figures

Executive Summary

Background

The European Network and Information Security Agency (ENISA) has been designated to aid in the development of resilient public eCommunications networks and services in the European Union through research, sharing of knowledge, stimulation of industry debate, and encouragement of collaboration between public and private sector bodies active in the field.

Since email has become a critical part of the foundation of modern electronic communications for private citizens, governments, companies, and other organizations, and since email systems have been bombarded for several years with huge volumes of unsolicited bulk mail, much of it fraudulent, illegal, and threatening to ICT security, ENISA has long been active in the fight against spam. This survey is the third such survey ENISA has conducted, and the first since 2007. The survey results, presentations, and forums for debate on anti-spam measures constitute key contributions ENISA makes in this effort.

For this survey mail providers have been interviewed throughout the European Union and beyond, with 90 providers submitting their views from 30 different countries. The survey asked providers about the organizational aspects of spam, the technical measures applied, and the effectiveness of these measures.

Key Findings

Organisational Aspects of Spam

Nearly all respondents treat spam as part of security operations, and the average response about the importance of spam in their security operations is that it is "significant".

Spam affects a service provider's business primarily through its impact on the quality of service received by the customer, and on the customer service operations. Some respondents noted that a significant share of helpdesk calls concern spam, though most reported that less than 10% of helpdesk calls concern spam. These results suggest that most providers are currently managing to prevent spam from greatly harming the customer experience, though spam continues to impose costs on helpdesks.

Anti-spam budgets vary greatly, with size of provider being the greatest reason. Even most small providers have anti-spam budgets over EUR 10,000 annually, while the largest providers can have budgets in the millions of Euros.

Respondents generally agreed that spam prevention is a competitive issue. The average responses showed that they think spam prevention is a key selling point for customers, and that it can provide a competitive advantage.

These results suggest that providers tend to view spam as an important business challenge that must be effectively managed, but few respondents indicated that it is of great significance. Spam prevention efforts appear to have made spam manageable, making anti-spam measures a standard part of operations. Spam must be addressed to retain customers, but it is not a critical concern for most providers.

Technical measures

Turning to technical measures, we examined the measures to detect and prevent spam.

Detecting Spam: With regard to detection, nearly all providers track spam, and the most common way of doing so is by tracking complaints. More pro-active measures that are also widely used include monitoring for traffic peaks, as well as real-time analysis of traffic anomalies or signature-based detection methods.

Preventing Sending of Spam: Blacklists were the most commonly used measure to prevent sending of spam, followed closely by limiting high outbound mail volumes (both used by over 60% of respondents). Other common measures include performing outbound virus scanning and blocking or managing Port 25 access.

Preventing Receiving of Spam: To prevent customers from receiving spam, nearly all service providers provide network-based spam filtering, though some charge specifically for the service. The most common network-based measures are blacklisting, content filtering, and sender authentication. The usage of most network-based measures has stayed constant since the 2007 survey, though use of sender authentication and URI blacklisting have increased markedly, while reputation systems and slowing the sender's connection have become less common. The average number of network-based measures applied has also remained consistent at 4.7 per provider.

Sender authentication: SMTP AUTH is the dominant sender authentication method, with SMTP TLS and SPF in distant second and third places. The usage of the various sender authentication mechanisms has remained mostly constant since 2007, except for DKIM, which has increased significantly.

Analyzing The Source of Spam: Three quarters of respondents analyze the source of spam upon receipt of complaints from customers or other ISPs. Far fewer analyze the source of spam based on automated tools, specifically when monitored spam levels reach a threshold.

After Detecting Spam: Most providers take a collaborative approach in their measures after detecting incoming spam. They tend to contact the source ISP, and only block SMTP connections, or IP addresses if that ISP does not solve the problem. Based on the information collected, such collaborative approaches to eliminating spam are the best way to solve the problem without disrupting legitimate traffic.

Sources of Reputation Databases: Since blacklists are the most common network-based anti-spam measures, and other reputation databases are also commonly used, the survey asked about the sources of databases used. The sources of these databases in use vary. Over half of providers use their own databases, and a similar number use a free database. Commercial databases are less common, though they do remain an important part of the arsenal of reputation databases.

Reliability of Blacklists: With blacklists so important in blocking spam, their reliability is crucial. Yet two thirds of respondents, and all of the largest providers, stated that they have had their servers added to blacklists (or retained on them) incorrectly, for example, after spam problems have been corrected. Furthermore, two thirds of respondents believe that major blacklists sometimes incorrectly include servers that do not or no longer send spam. Half of these did say that it is usually easy to have the problem fixed, but the other half felt it is often difficult to get the problem fixed.

This high level of responses citing problems with blacklists incorrectly including non-spamming servers is alarming. This problem may inevitably happen occasionally, but e-mail providers clearly want to be sure that when a spam problem is fixed, that the server can be removed from the blacklist.

Planned Anti-Spam Measures: Close to half of providers stated that they plan to implement new anti-spam measures within six months. Reputation databases were mentioned most frequently with new blacklists most common, followed by greylists[1]. A great variety of other measures were mentioned less frequently.

Anti-Spam Software: A mix of commercial and open-source applications is widely used by respondents. By far the most commonly mentioned application was the open-source SpamAssassin, which combines several different anti-spam measures in a single free application. Dozens of other applications were also mentioned.

Abuse Reporting: By far the most common way to process abuse reports exchanged between providers was manually. Only a few providers process them automatically. There has been little

[1] Greylist: Reject emails at first reception. See annexes for a more complete definition.

change in the last two years in improving this situation, and this looks like one area where spam prevention efforts could gain some ground.

Conflict between Spam Filtering and Obligations to Customer: Close to a third of respondents stated that they think there is a conflict between the need to filter out spam, and their obligations to the customer to deliver the mail and protect privacy. This level has remained the same since the 2007 survey. The most common conflict areas concerned false positives and privacy concerns.

Effectiveness of Measures

The data on aborted SMTP connections and filtered emails seems to show that anti-spam measures are currently highly effective. Nearly 80% of SMTP connections are aborted, most of them due to blacklists. And of the accepted connections, nearly 80% are filtered out, mostly as spam. Thus, the percent of delivered e-mail is only 4.4% of the total. This is an even lower figure than was the case in the 2007 survey. The anti-spam measures are effectively filtering out vast amounts of spam, without allowing false positives to become a major problem.

Segmentation Analysis of Survey Results

Throughout this report, the survey results are segmented by size of provider. In analyzing the results, we also examined the results by different segments, and found that little variation is evident when segmenting by type of company (such as a telecoms service provider that also offers email services, as opposed to a web hosting provider that also offers email services), or by target market of the company. The greatest variation appears when examining the size of the provider, probably due to the larger budgets available to large providers in their anti-spam efforts. Nonetheless, even by size of provider, the variation is usually not great, nor are there often predictable patterns.

Conclusions

Email providers generally take spam seriously as a security challenge, but it is not a critical threat. It is an ongoing management challenge that has important ramifications for customer retention, and it imposes costs on the provider. However, it is a manageable business process that is currently largely effective.

One of the most prominent conclusions is that little has changed over the last two years. Most measures are applied by similar proportions of providers to what was observed in 2007. Usage of the main types of sender authentication mechanisms remains approximately the same. Abuse report handling is still mostly manual. And the percentage of respondents perceiving conflicts between spam filtering and ISP obligations has remained steady. Essentially, few major changes have occurred in the efforts against spam. Less than 5% of the total email traffic is delivered.

Spam prevention is not only a matter of protecting customers from external spammers. Several respondents emphasized the need for a coordinated approach against spam, and a key part of that is for providers to shut down spammers among their own customers, before sending the spam on to other service providers.

Many providers indicated plans to implement new measures in the coming six months, such as new blacklists or greylisting measures, DKIM, and port 25 management. Thus, although usage levels of various measures have remained constant, providers are frequently adjusting or upgrading their measures to ensure that they remain effective.

These results, combined with the moderate significance assigned to spam by providers, suggest that spam prevention has reached a sort of equilibrium, in which substantial efforts are required to manage spam, but the challenges and countermeasures are generally well-understood. The countermeasures are proving effective, when managed and updated properly, so little major changes seem to be required.

Recommendations

Though anti-spam measures are proving generally effective, these efforts could still be improved. For example:

- Email providers should take a more proactive approach to monitoring spam and identifying the source, so that appropriate actions can be taken by originating ISPs.
- Blacklist managers need to ensure that it is easy to remove a server or domain from a blacklist when spam problems have been rectified. And with so many different blacklists in use, collaborative efforts to share data on servers that should be removed from blacklists would help to address the problem. Wider use of whitelists could help in this effort.
- Providers should look to increase the abuse report feedback loops with other providers and aim to automate abuse reporting processes, possibly adopting the Abuse Reporting Format (ARF).
- Providers should seek collaborative solutions to fight spam, as many, but not all, already do. For example, notifying ISPs that originate spam that they are doing so and discussing countermeasures with them will help to cut off spam at the source.
- Policy-makers and regulatory authorities could help spam prevention efforts by further clarifying the apparent conflicts between spam-filtering, privacy, and obligation to deliver, particularly by distributing and promoting awareness of the findings of the Article 29 Data Protection Working Group, which outlines the legal basis for spam-filtering based on the EU legal framework.

- Institutions that aim to aid public and private efforts against spam should promote open collaborative solutions to spam, such as reporting of spam sources to other ISPs and authorities; the Abuse Reporting Format; contribution to collaborative solutions; and sharing of best practices across the industry to aid providers that need to improve their anti-spam measures.

Context

Public eCommunications networks have become fundamental critical infrastructure for the operations of Europe's modern societies, economies and government institutions. However, these networks are under continuous threat from wide-ranging sources and techniques. In an effort to help improve the security of these networks, the European Union created the European Network and Information Security Agency (ENISA). This agency's role is to ensure a high and effective level of network security within the EU. It does so by acting as a centre of expertise working for the EU institutions and Member States, giving expert advice and recommendations, disseminating best practices, and stimulating discussion and cooperation among public and private organizations and experts.

As the Internet has grown to become critical infrastructure for the modern economy, governance, and personal communications, one of the cornerstones of Internet communications—email—has become widely abused by senders of huge volumes of unsolicited bulk mail, or spam. Taking advantage of the negligible costs of sending email, these senders have far surpassed the volume of legitimate email, swamping networks, email servers, and email inboxes, having a detrimental effect on networks, and reducing the usability and efficiency of this critical communications method. Commonly, and even more alarmingly, many of these unsolicited bulk mail messages support illegal activities, often constituting serious security threats in the forms of phishing messages and distribution of viruses and other malware.

In confronting these problems and threats, network operators and email service providers have deployed a wide range of anti-spam measures. With these measures network operators and service providers have achieved significant success in reducing the amount of spam that reaches the end-user or that traverses the network. However, the battle continues, with spammers continually seeking new approaches to evade these measures, and anti-spammers developing new measures to stop them.

ENISA has taken an active role in this battle for several years, conducting research, generating debate, encouraging collaboration, and disseminating knowledge on the anti-spam battle. The first ENISA Anti-Spam Measures Survey was conducted in 2006, and a second survey followed a year later to gauge progress. The third ENISA Anti-Spam Measures Survey aims to again determine how the battle has evolved, and to share the latest anti-spam practices with the public and private organizations and experts that confront the spam challenge in the EU. ENISA selected IDC to conduct the research.

Methodology

The questionnaire for the Anti-Spam Measures Survey 2009 was based largely on the previous 2007 survey questionnaire, with some modifications. The 2007 survey used European Directive 2002/58/EC to create the questions, especially Article 4 (Security) and Article 13 (Unsolicited communications). Some providers' best practices (e.g. from MAAWG, OECD) were also taken into account, with the aim of obtaining feedback on their level of implementation. Retaining much of the original survey enables analysis of results over time.

The survey targeted anti-spam managers at email service providers throughout the EU. The objective was to include a wide range of providers of different types and sizes, and from different countries. Contact details for over 1700 email providers were assembled and they received invitation letters. The letters included a web link to access the questionnaire online.

In addition to the direct mailing, several ISP associations and other associations with ties to email providers were asked to distribute invitations to their members. Furthermore, contacts with many providers via telephone to reach anti-spam managers were initiated and they were invited to participate.

The survey was open from May until July 2009, and 90 respondents participated from 30 different countries. The respondents together manage over 80 million email mailboxes.

Respondents

The survey was completed by 92 respondents, located in 30 different countries. The number of respondents by country is listed in table 1. The respondents were fairly evenly distributed, though there were some concentrations of responses, particularly 13 respondents in Austria. Of the EU member states, 26 of the 27 are represented.

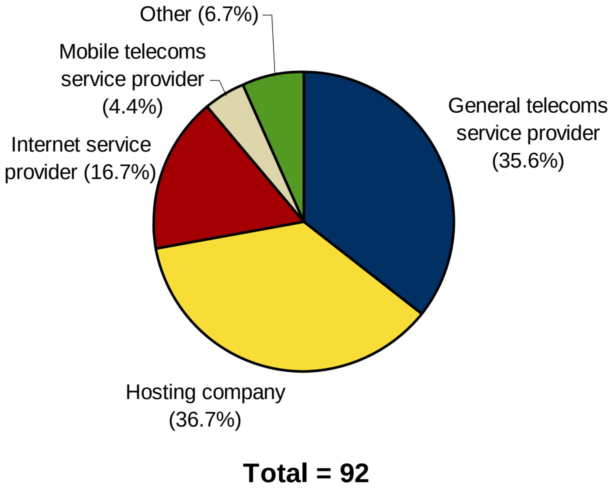
Respondents represented diverse companies. Most were telecoms network operators, while a large portion were hosting companies not operating telecoms networks (see Figure 1).

Table 1: Respondents by Country of Location

Country	Respondents
Austria	13
Belgium	1
Bulgaria	3
Cyprus	3
Czech Republic	6
Denmark	3
Estonia	2
Finland	2
France	2
Germany	3
Greece	3
Hungary	1
Iceland	1
Ireland	3
Italy	4
Latvia	2
Lithuania	2
Malta	3
Netherlands	5
Norway	3
Poland	2
Portugal	2
Romania	7
Slovakia	1
Slovenia	3
Spain	4
Sweden	1
Turkey	1
United Kingdom	5
United States	1
Total	**92**

Source: ENISA anti-spam survey 2009

Figure 1: Respondents by Type of Company



Source: ENISA anti-spam survey 2009

The respondent companies varied greatly by size, and this factor might be expected to be the greatest factor differentiating between how companies address the challenges of spam prevention. The survey featured companies ranging from very small to very large, so the results have frequently been categorized to distinguish their responses. For this purpose, they have been segmented by the number of email mailboxes that they manage. The categories, and the defining ranges of mailboxes managed, are listed in Table 2.

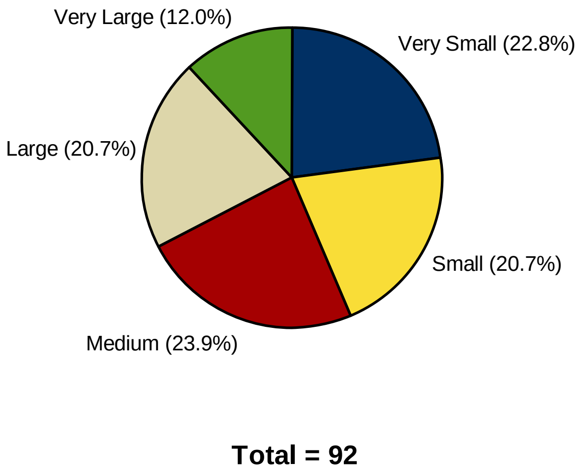
Table 2: Respondent Segmentation by Size of Provider

Segment Name	Number of Email Mailboxes Managed
Very Small	Less than 1000
Small	1,000 to 9,999
Medium	10,000 to 99,999
Large	100,000 to 999,999
Very large	1 Million or More

Source: ENISA anti-spam survey 2009

Based on this segmentation, the respondents are fairly evenly distributed in terms of the numbers of respondents, though there are fewer of the very large companies. The distribution by size is shown in Figure 2.

Figure 2: Respondents by Size (Number of Email Mailboxes Managed)



Source: ENISA anti-spam survey 2009

The largest email providers generally come from the telecoms operator space, especially those general telecoms service providers that offer a wide range of voice and data services on the fixed-line (and sometime also mobile) networks.

The company types are mainly segmented into a few different types of telecoms service provider, as well as hosting companies, and "other". This last category includes only a few respondents, and these include some research institutions and universities that manage large numbers of mailboxes.

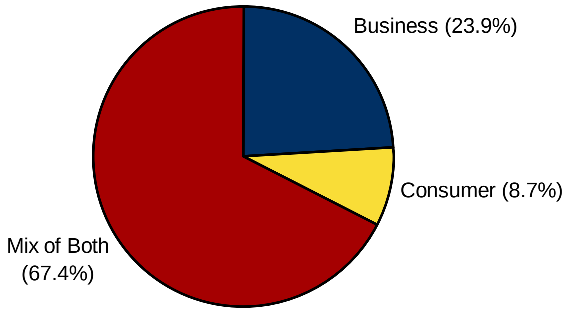
Table 3: Respondents by Type and by Size (Number of Email Mailboxes Managed)

Company Size by Number of Email Mailboxes Managed	General telecoms service provider (n=32)	Hosting company (n=33)	Internet service provider (n=16)	Mobile service provider (n=5)	Other (n=6)	Overall (n=92)
Very Small (less than 1,000)	5	10	3	2	1	21
Small (1,000 to 9,999)	3	7	9	0	0	19
Medium (10,000 to 99,999)	6	8	4	0	4	22
Large (100,000 to 999,999)	8	7	0	3	1	19
Very Large (1 million or more)	10	1	0	0	0	11

Source: ENISA anti-spam survey 2009

Another factor that might be expected to influence the way in which a provider addresses spam is the provider's primary target segment. Businesses, and especially large enterprises, often demand and pay for higher levels of service quality, reliability or security, than do consumers. Some survey responses have been segmented to reveal how the respondent companies may approach some issues differently, due to their target segments. However, because by far most of the respondent companies target both business and consumer segments, the sample size for the those targeting one or the other are small (see Figure 3), limiting the level of analysis possible. Nonetheless, some data are presented along this segmentation to try to enable some general conclusions.

Figure 3: Respondents by Primary Target Market



Total = 92

Source: ENISA anti-spam survey 2009

In analyzing the data by these business-type and target-market segments, the authors found that there is generally little variation in the responses. Some results in the study include these segments, in order to illustrate this similarity. However, due to this similarity, most results are instead presented only in aggregate form, or segmented by size of provider.

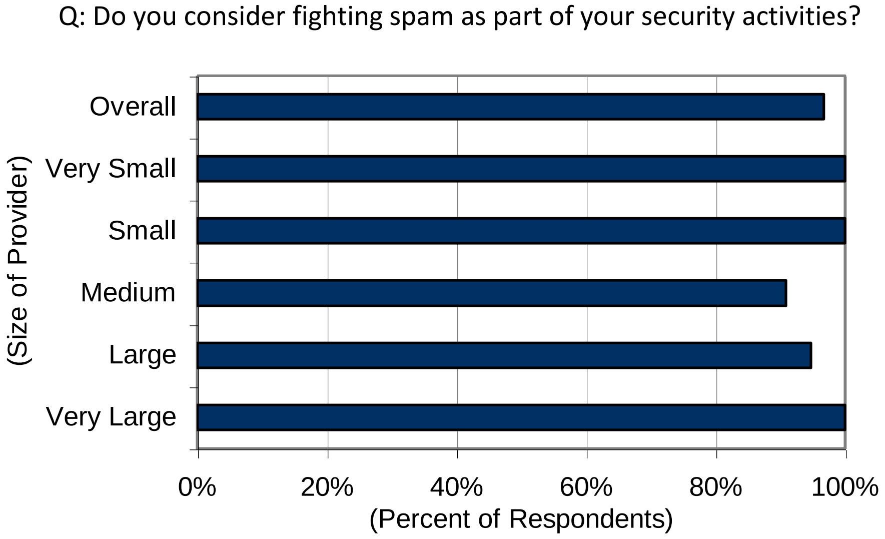
Organizational Measures

The first core section of the survey focused on organizational measures and aspects of the anti-spam efforts. The survey aimed to determine how service providers address the spam challenge, how significant the challenge is, and what impact it has on their operations and results.

Spam as Part of Security Operations

First of all, we asked about what kind of a challenge is spam. Do they consider fighting spam as part of their security activities? Spam can be viewed in some ways as a nuisance, rather than a security threat to the service provider, so we wanted to see what department confronts spam. As it turned out, the responses were almost unanimous in treating spam within the security operations (see Figure 4). This status suggests that service providers consider it an important threat that they must address carefully. Further questions investigate further to verify how seriously service providers evaluate the threat, and how much resources are devoted to it.

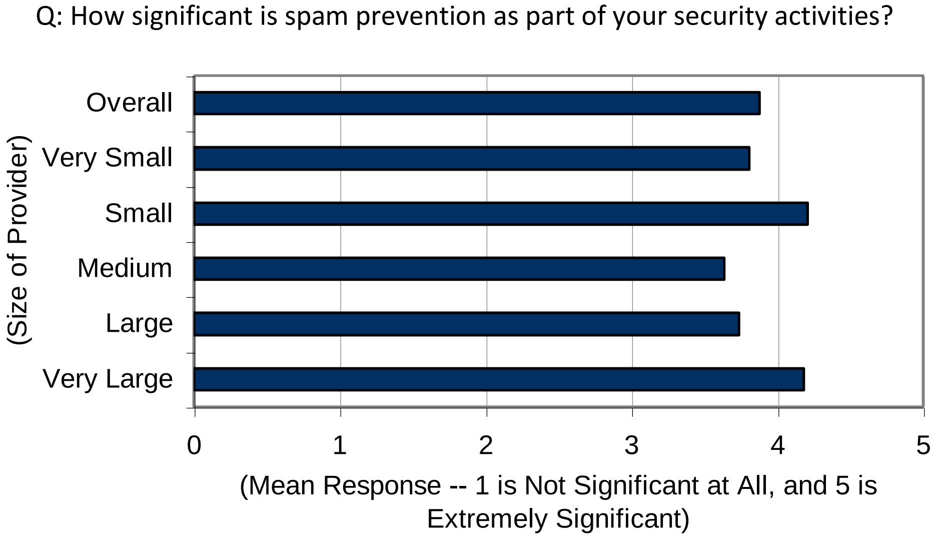
Figure 4: Addressing Spam as Part of Security Operations



Source: ENISA anti-spam survey 2009 (N=92)

When asked how significant spam prevention is within security activities, the average response was that it is significant (see Figure 5).

Figure 5: Significance of Spam in Security Operations by Size of Provider

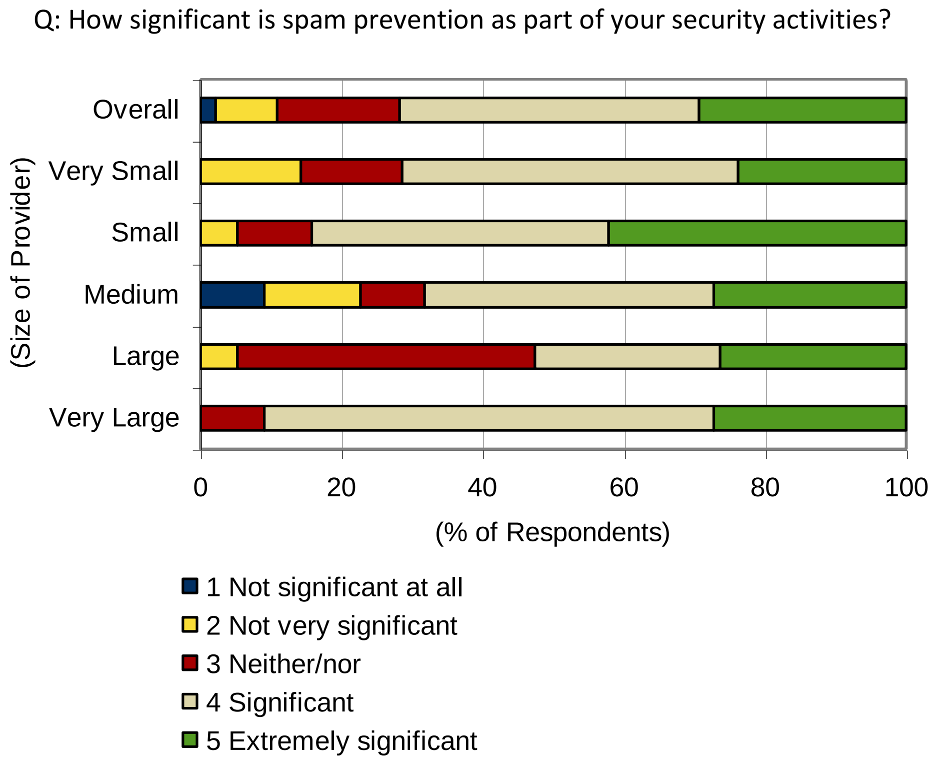


Source: ENISA anti-spam survey 2009 (N=92)

However, averages can hide the extremes, so it is worth seeing the individual responses to see if significant numbers view spam as insignificant. In fact, that is not the case. When looking at the individual responses, we can see that 12% consider spam an insignificant ("Not very significant" combined with "Not significant at all") part of security activities (see Figure 6). Meanwhile, 70% of respondents consider it extremely significant or significant.

When comparing the size categories, there is little consistent trend. Given the small sample size, the variation is not statistically significant.

Figure 6: Significance of Spam in Security Operations by Size of Provider



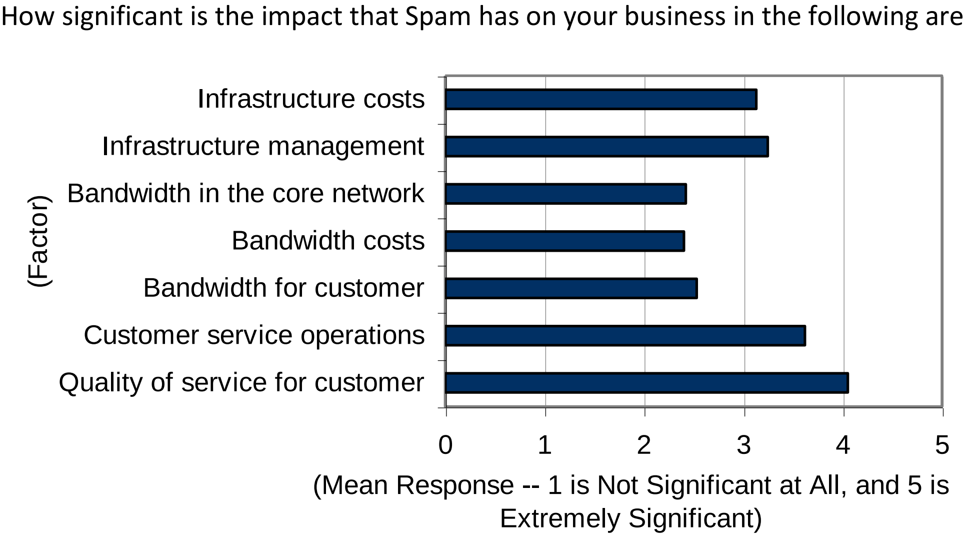
Source: ENISA anti-spam survey 2009 (N=92)

Impact of Spam

Impact on Providers' Business

The survey also asked how significant is the impact that spam has on various aspects of the service provider's business. The most prominent impact is on the quality of service delivered to the customer, while the impact on bandwidth is viewed generally as of low significance (see Figure 7).

Figure 7: Impact of Spam on Respondent's Business



Source: ENISA anti-spam survey 2009 (N=92)

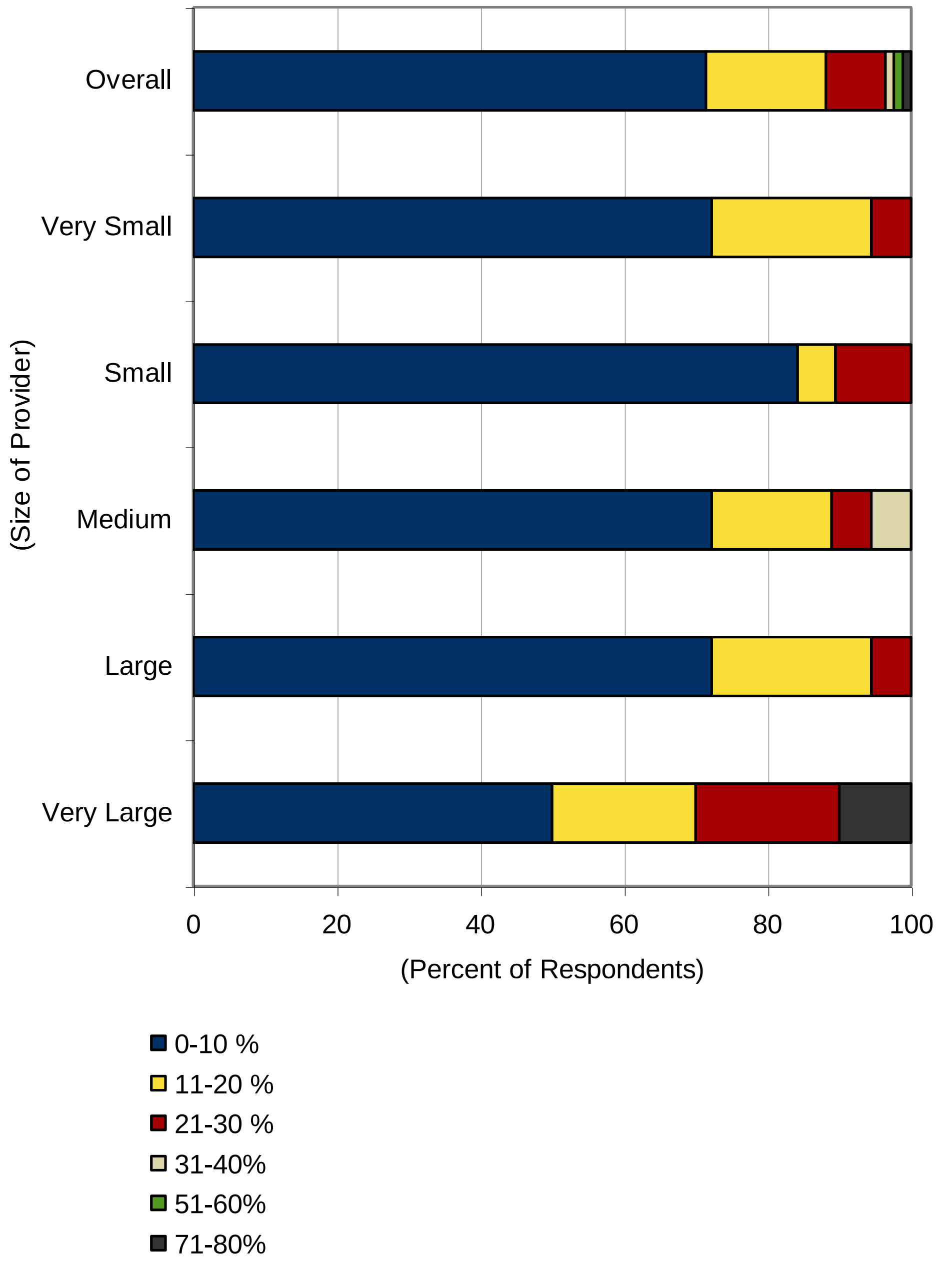
Helpdesk Calls Concerning Spam

With spam's impact on the customer experience being identified as so significant, the survey investigated this subject further. The survey found that most service providers report only a moderate amount of helpdesk calls are connected to spam (see Figure 8), though over a quarter of respondents noted spam accounting for over 10% of helpdesk calls. This finding may indicate that most service providers have been largely effective in their efforts to prevent spam from harming most customers' experience. However, some providers clearly must devote a large amount of helpdesk resources to the issue.

It is interesting to note the slightly higher percentages of helpdesk calls concerning spam for the largest service providers. Due to the small sample size, we must be cautious with such data, but it may reflect the fact that these service providers include large mass-market customer segments that can generate a large volume of helpdesk calls.

Figure 8: Helpdesk Calls Concerning Spam

Q: What percent of your helpdesk calls concern spam?



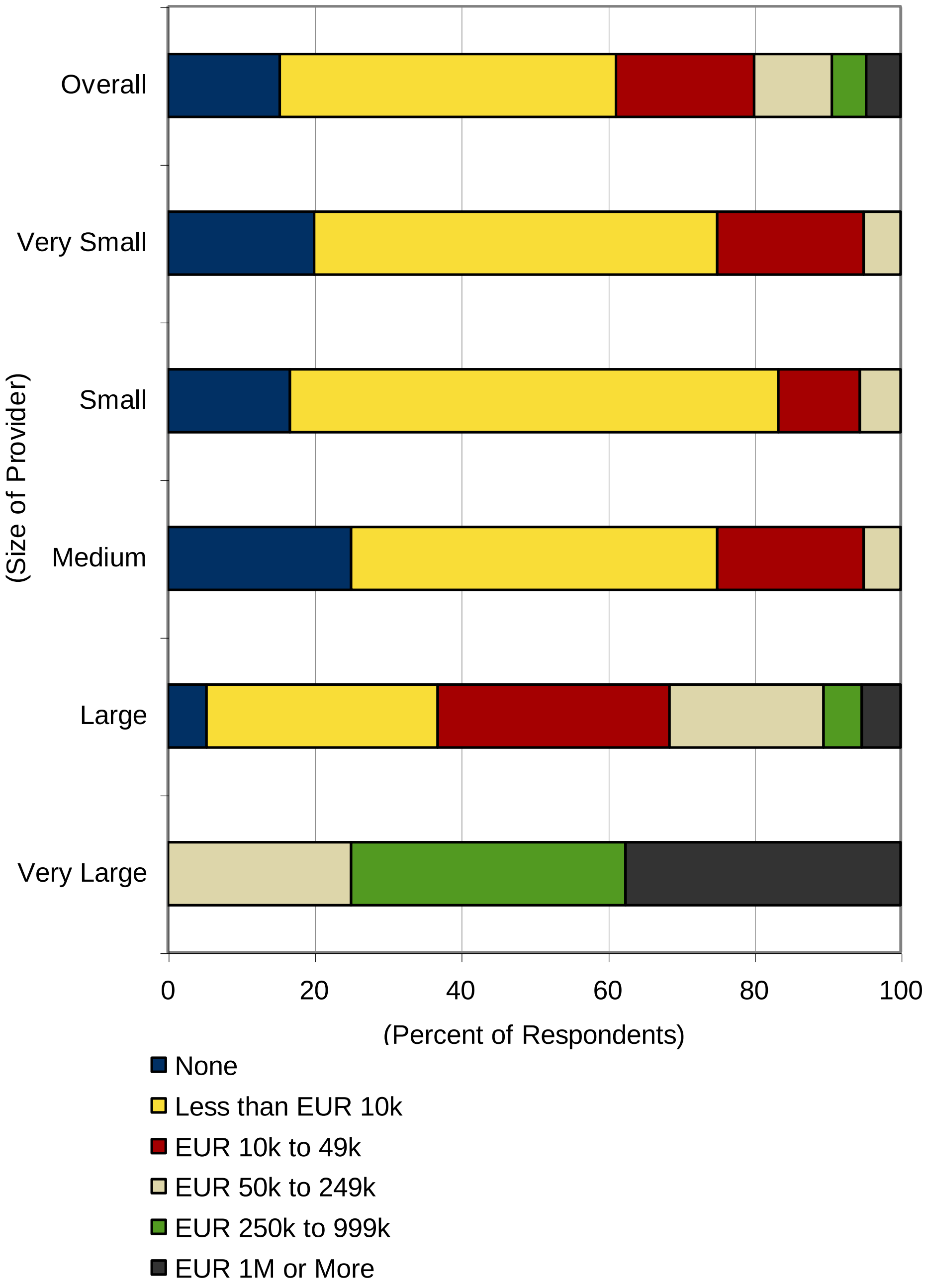
Source: ENISA anti-spam survey 2009 (N=84)

Anti-Spam Budget

Given the significance of spam for the service providers, spam may generate considerable costs for service providers. Anti-spam budgets can indeed be considerable. Among the very small providers, for example, a quarter of respondents stated that their anti-spam budgets are over EUR 10,000 per year, with one even over EUR 50,000 per year (see Figure 9). And among very large providers, a third pointed to anti-spam budgets over EUR 1 million annually. This financial measure truly highlights the costs of the anti-spam efforts. But note that this does not reflect all spam-related costs. For example, the customer-service call costs of spam-related calls can be significant.

Figure 9: Annual Anti-Spam Budget

Q: What is your annual budget for anti-spam measures and operations?



Source: ENISA anti-spam survey 2009 (N=85)

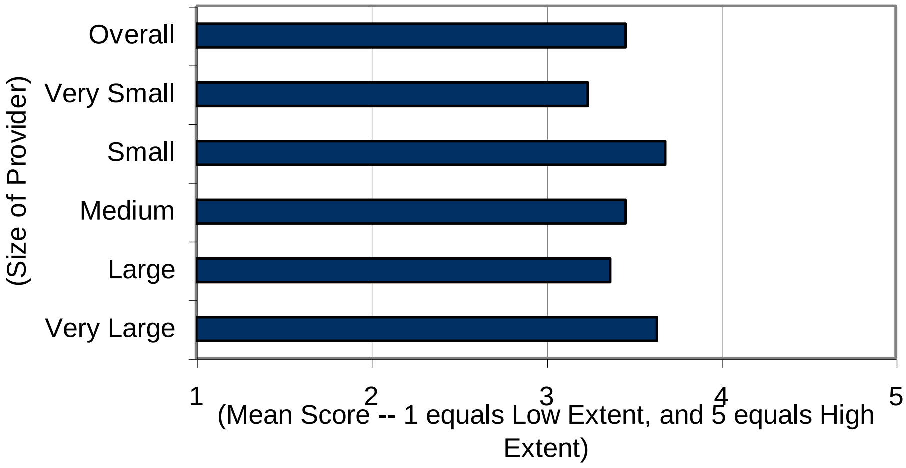
Spam Prevention as a Competitive Factor

Key Selling Point for Customers

But the impact of spam is not only on costs. With customer service directly affected by spam, service providers pointed to spam as a competitive issue. When asked to what extent is spam prevention "a key selling point", the average response was closer to "high extent" than to "low extent" (see Figure 10).

Figure 10: Anti-Spam Measures as a Key Selling Point for Customers, by Size of Provider

Q: To what extent do you consider spam prevention as a key selling point?



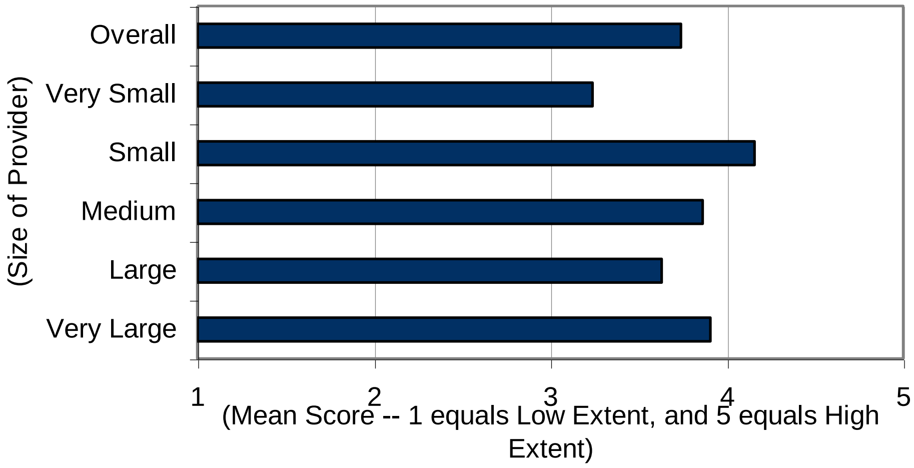
Source: ENISA anti-spam survey 2009 (N=92)

Competitive Advantage for Providers

Similar results emerged when providers were asked whether anti-spam measures provide a competitive advantage (see Figure 13). Responses were again consistent by size and type of provider and by target market, suggesting that generally all providers consider it necessary to have effective anti-spam measures for the sake of attracting and retaining customers.

Figure 11: Anti-Spam Measures as a Competitive Advantage for Providers

Q: To what extent do you consider spam prevention as a competitive advantage?



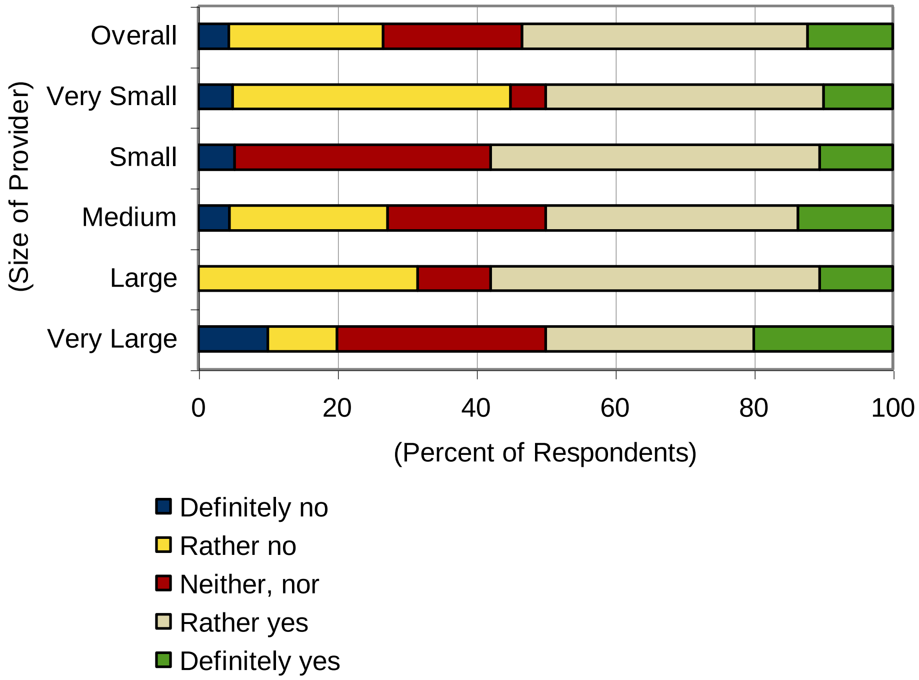
Source: ENISA anti-spam survey 2009 (N=92)

Does Spam Prevention Factor into the Customer's Choice of Provider?

Another question addressed this point more directly. When asked if spam prevention is a factor in the customer's choice of provider, over half said yes, while less than a third said no (see Figure 14).

Figure 12: Spam Prevention as a Factor in Customer's Choice of Service Provider

Q: Do you think that spam prevention is taken into consideration by end-users when choosing a service provider?



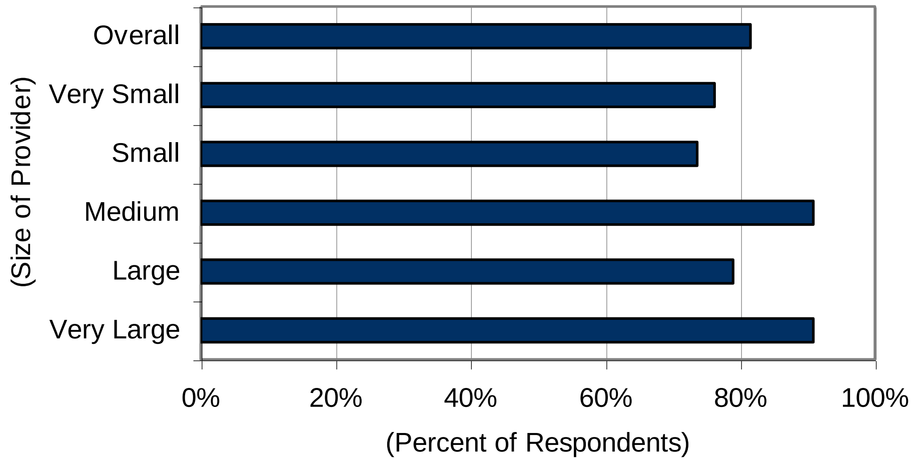
Source: ENISA anti-spam survey 2009 (N=90)

Contact Details for Reporting Email Abuse

With such consistent answers about spam prevention's role in competition and attracting customers, it is no surprise that service providers also were consistent in stating that most of them provide clear contact details for customers to report email abuse (see Figure 15).

Figure 13: Contact Details for Reporting Email Abuse

Q: Do you provide your customers with clear contact details for reporting e-mail abuse?



Source: ENISA anti-spam survey 2009 (N=92)

Conclusions about Organizational Issues

Based on the above data, it is clear that email providers consider spam to be a significant operational challenge, and one that is important in attracting and retaining customers. But the data also do not express major alarm at the spam threats. Most of the responses noted spam as having a moderately significant impact on the business, but few providers indicated that this impact is critical or urgent. These responses suggest that spam prevention is currently mainly an operational challenge, but not a strategic one. It is a challenge that absorbs some resources, creates problems for anti-spam managers, makes provision of email services complicated, and can be a competitive factor if a provider fails to deliver satisfactory email service. But the responses also give the impression that there is no current crisis in spam prevention. Have spammers and anti-spam measures reached a bearable equilibrium? And if so, how?

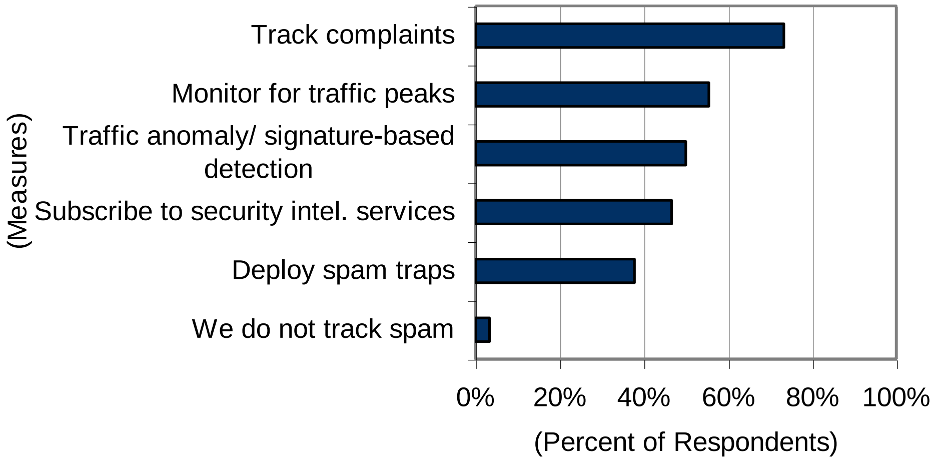
Technical Measures

Measures to Detect Spam

The next section investigates the technical measures that providers implement to combat spam. First, we asked about the measures to detect spam. The most common method is to track complaints, a method applied by about three quarters of respondents (see Figure 16). This is probably the simplest measure to apply, but also a useful one if complaints can be tracked and addressed quickly. Other common measures are to monitor traffic peaks and conduct real-time anomaly and/or signature-based detection. These real-time monitoring measures give the ability to take action quickly against spammers and to minimize the impact on customers. Encouragingly, only very few respondents do not track spam.

Figure 14: Measures to Detect Spam Problems

Q: What measures do you take to become aware of spam problems?



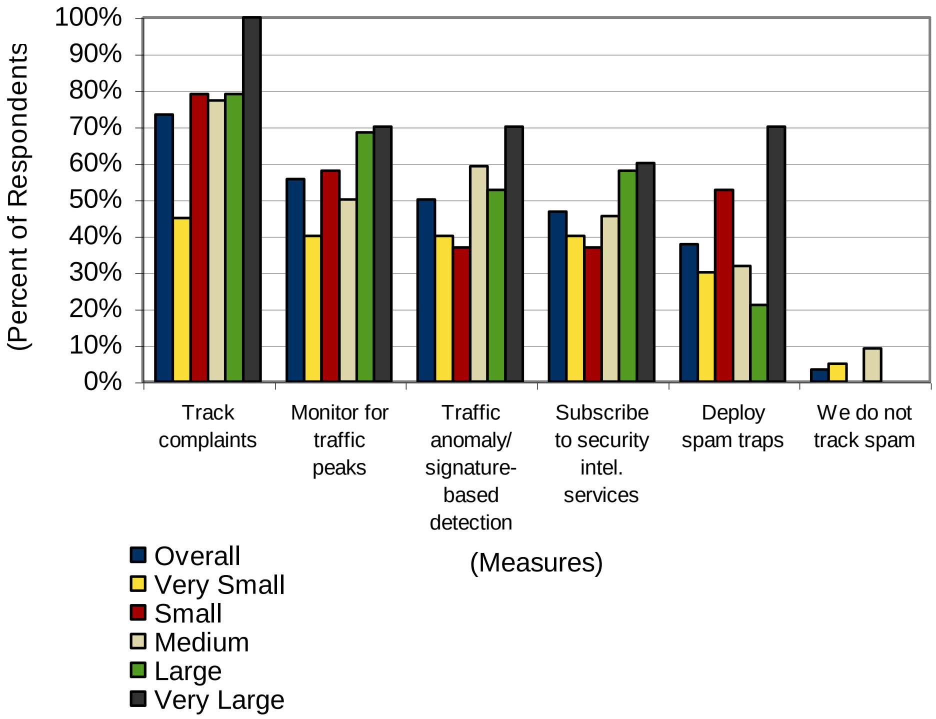
Note: Several respondents also noted other measures, including monitoring anti-spam software and server logs, and limiting SMTP usage.

Source: ENISA anti-spam survey 2009 (N=90)

Examining the data by size of provider yields some interesting differences (see Figure 17). Significantly, the largest providers apply all of the measures more frequently than do the smaller providers, generally by a wide margin. This is perhaps to be expected, as large providers tend to have more staff and larger budgets to apply to spam prevention, and they typically also have more formal procedures around their business operations, than do small providers, which can achieve some objectives with less formal procedures. This variance between measures applied by large and small providers can be seen in many examples of anti-spam measures.

Figure 15: Measures to Detect Spam Problems, by Size of Company

Q: What measures do you take to become aware of spam problems?



Source: ENISA anti-spam survey 2009 (N=90)

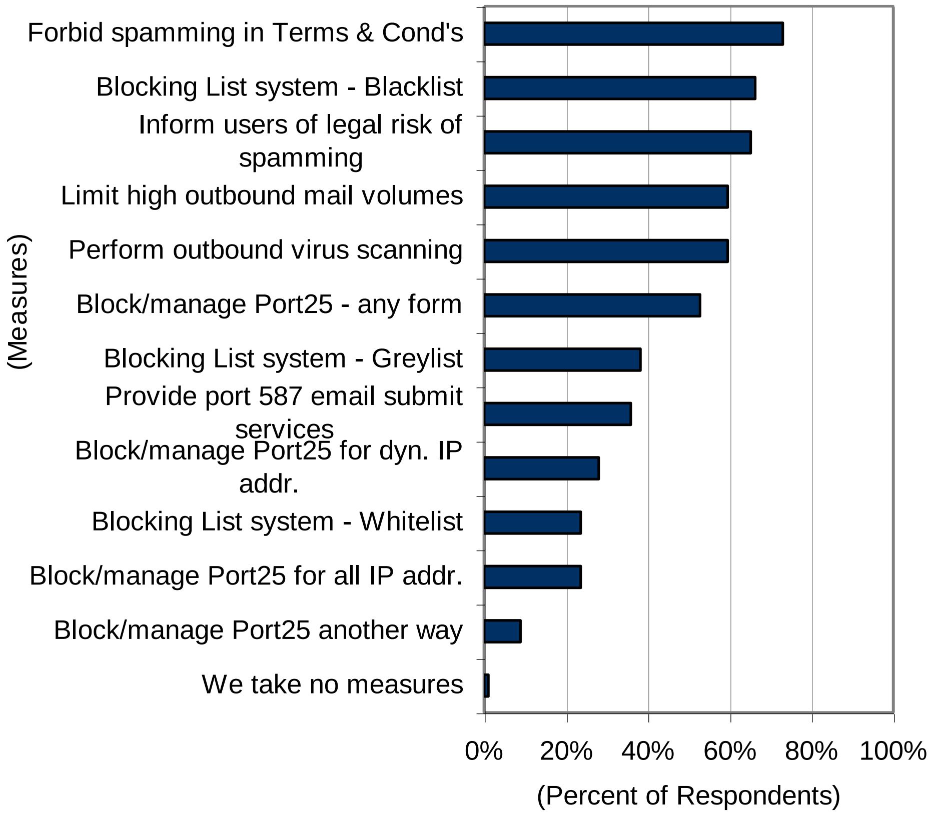
Measures to Prevent Customers from Sending Spam

Spam prevention is not only a matter of protecting customers from external spammers. Several respondents emphasized the need for a coordinated approach against spam, and a key part of that is for providers to shut down spammers among their own customers, before sending the spam on to other service providers.

When looking at the measures providers apply to prevent customers from sending spam, the most common (three quarters of respondents) is to forbid spamming in the terms and conditions (see Figure 18). This measure in and of itself may not be very effective, but it can support and justify other measures. And other measures are indeed common, including blacklisting violators, and other blocking list systems. Also common is to inform them of legal consequences of spamming, limiting high outbound mail volumes, performing outbound virus scanning, and blocking or managing port 25 access in some way. Less common technical measures include providing port 587 email submission services and specific variants of blocking or managing of port 25. Almost none of the respondents stated that they do not take any measures to prevent customers from sending spam, and those that did were among the smallest providers.

Figure 16: Measures to Prevent Customers from Sending Spam

Q: Which of the following measures do you take to prevent your subscribers from sending unsolicited communications (spam)?



Note: Those blocking or managing port 25 access another way indicated such tactics as manually restricting specific IP addresses and requiring authentication.

Note: Some respondents also listed some other tactics, such as investigating complaints and suspending an account if abuse can be verified, monitoring bounce rates, and performing outbound spam scanning.

Source: ENISA anti-spam survey 2009 (N=89)

Other variation by size of provider is harder to assess. There is no obvious trend across all measures (such as one size of provider always deploying all measures more frequently than the others). In fact, very small and medium-sized providers tended to have the lowest level of deployment of measures.

Meanwhile, small providers show the highest deployment of some measures, such as outbound virus scanning and whitelisting, and one of the lowest for others (informing violators of legal consequences, and managing port 25 access for dynamic IP addresses). Generally, the largest providers do show somewhat higher deployment of these measures.

In any case, nearly all of the measures could be more widely applied by all of the size categories, though a provider will generally want to choose the measures to apply carefully, selecting a combination that is efficient and effective.

Measures to Prevent Customers from Receiving Spam

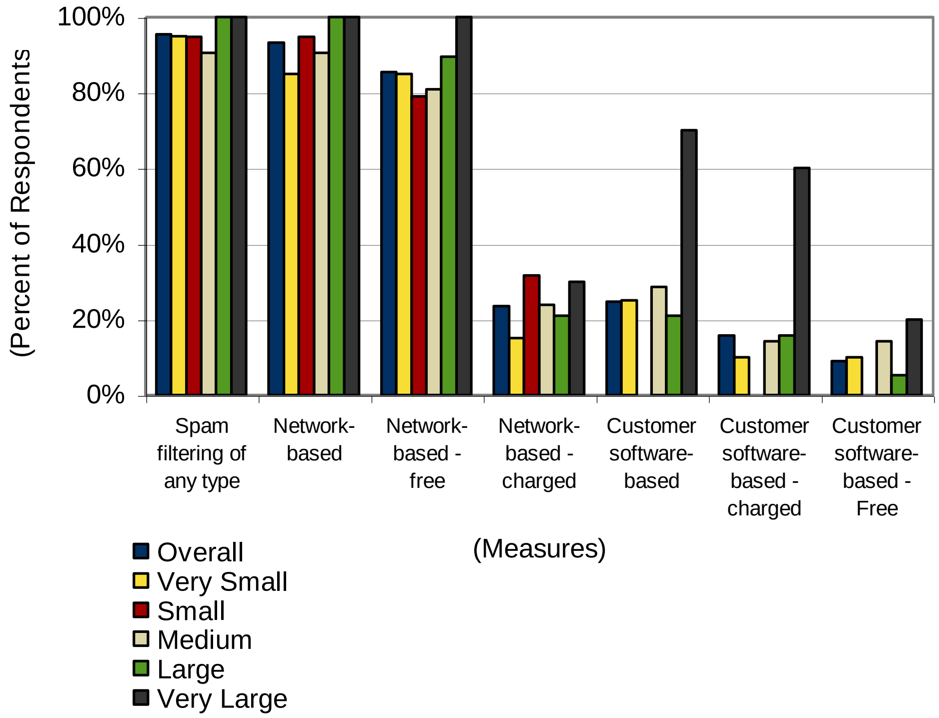
Turning to inbound email, what measures do providers take to prevent customers from receiving spam? In general, nearly all providers provide some form of spam filtering to their customers. A very high percentage of respondents offers spam filtering on their networks (see Figure 19), and the vast majority of these offer it for free.

Spam filtering software for customers to install is much less common, though most of the largest providers offer it. It is more common for such services to be offered for a fee, rather than free, though the difference is not great.

In sum, the largest providers all offer network-based, and mostly offer customer software-based filtering. But even among the other categories, nearly all providers offer some kind of filtering. Only a small number offer no filtering at all, and either these providers have customers that prefer to do it themselves, or else they may need to improve their efforts to remain competitive.

Figure 17: Measures to Prevent Customers from Receiving Spam

Q: Which of the following measures do you take to protect your subscribers from receiving unsolicited communications (spam)?



Source: ENISA anti-spam survey 2009 (N=89)

Spam-Filtering Measures on the Network

The specific spam-filtering measures on the network vary greatly in usage. The providers deploy on average 4.7 measures each. The most common measure is blacklisting (see Figure 20), with nine tenths of respondents using this method. Content filtering is also very widely used, followed by sender authentication. Much less common are measures such as whitelisting, checksum analysis, and slowing the sender's connection.

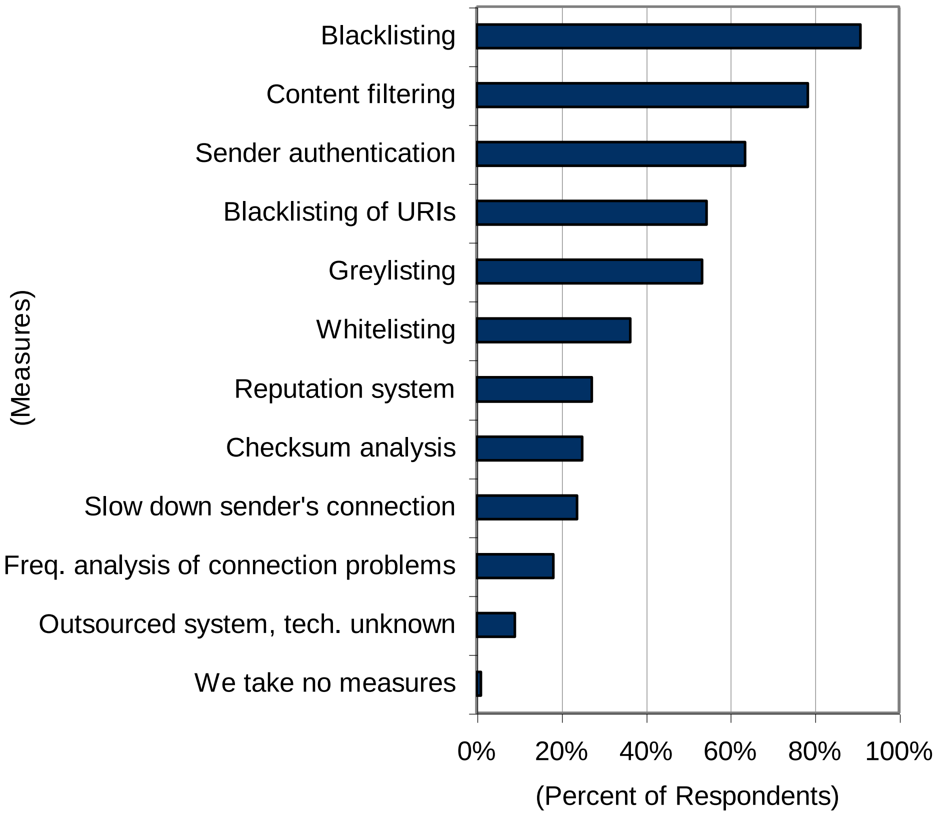
When comparing the results to the 2007 survey, one significant finding is that very little has changed in terms of adoption of these measures. In particular:

- The use of many measures has remained effectively constant since two years ago. These include blacklisting, content filtering, greylisting, and frequency analysis.

- The one measure to increase significantly in that time is sender authentication, which increased from about 50% to 64%.
- Two measures decreased significantly: reputation system fell in usage from about 35% to 26%, and slowing down the sender's connection fell from about 45% to about 25%.
- The average number of measures per provider has also remained steady at 4.7 both in 2007 and now.

Figure 18: Spam-Filtering Measures on the Network – Overall

Q: Which of the following spam-filtering measures do you take on your network?



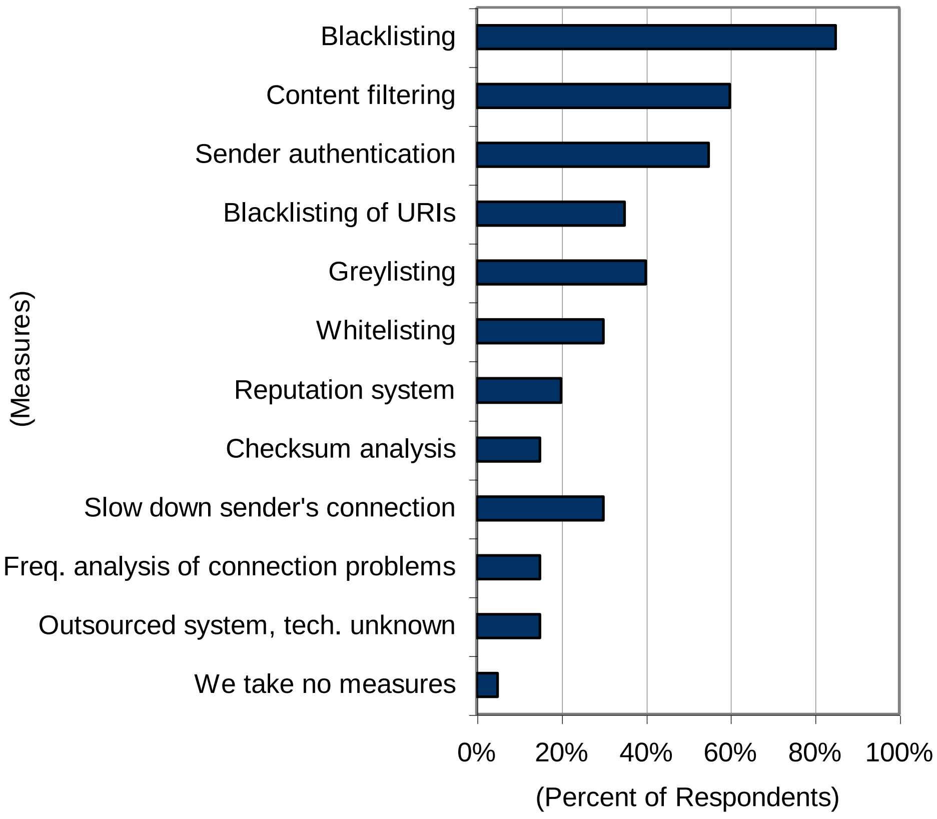
Note: Some other measures mentioned included manually blocking spam servers, automated content analysis, connection count limits, volume limits per minute, and checking reverse lookup of IP addresses.

Source: ENISA anti-spam survey 2009 (N=88)

With regard to the deployment of measures by size of provider, again there is little consistent trend, apart from a tendency for the smallest providers to have slightly lower levels of usage, and the largest to have slightly higher levels of usage (see Figures 21 to 25).

Figure 19: Spam-Filtering Measures on the Network -- Very Small Providers

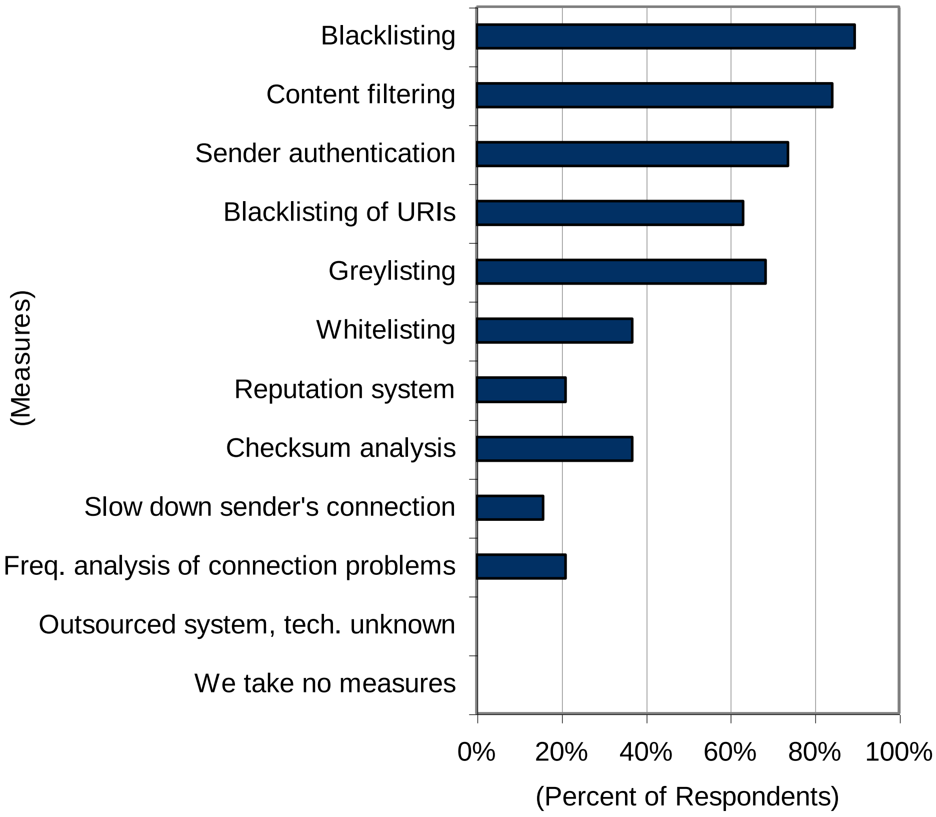
Q: Which of the following spam-filtering measures do you take on your network?



Source: ENISA anti-spam survey 2009 (N=20)

Figure 20: Spam-Filtering Measures on The Network -- Small Providers

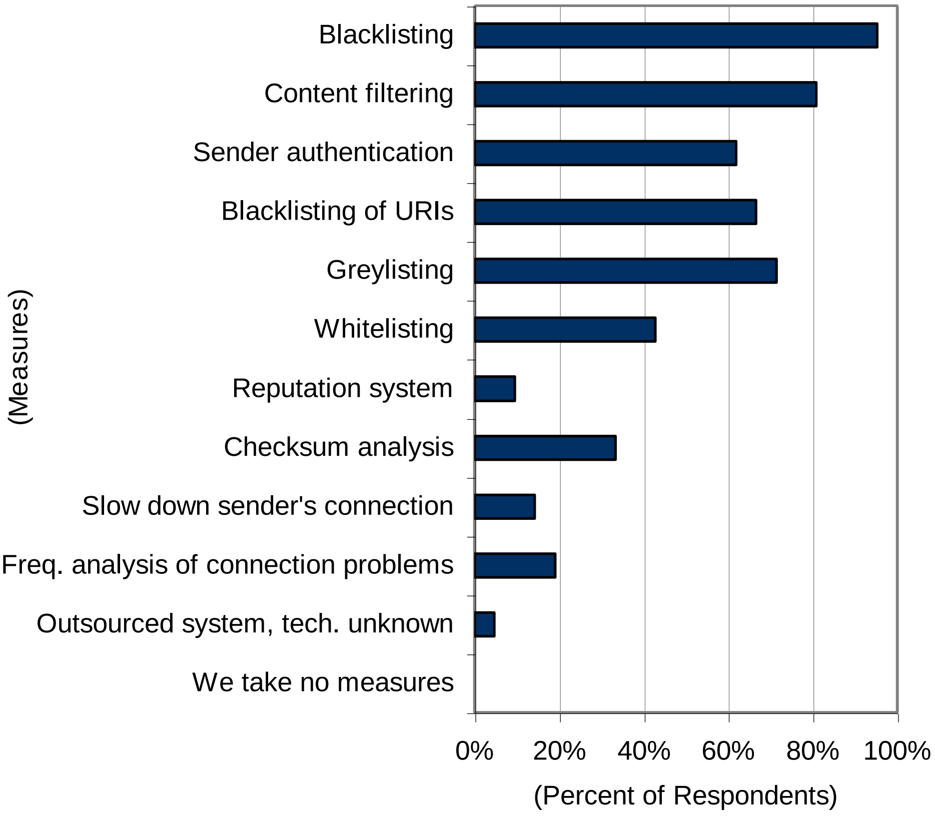
Q: Which of the following spam-filtering measures do you take on your network?



Source: ENISA anti-spam survey 2009 (N=19)

Figure 21: Spam-Filtering Measures on the Network -- Medium-Sized Providers

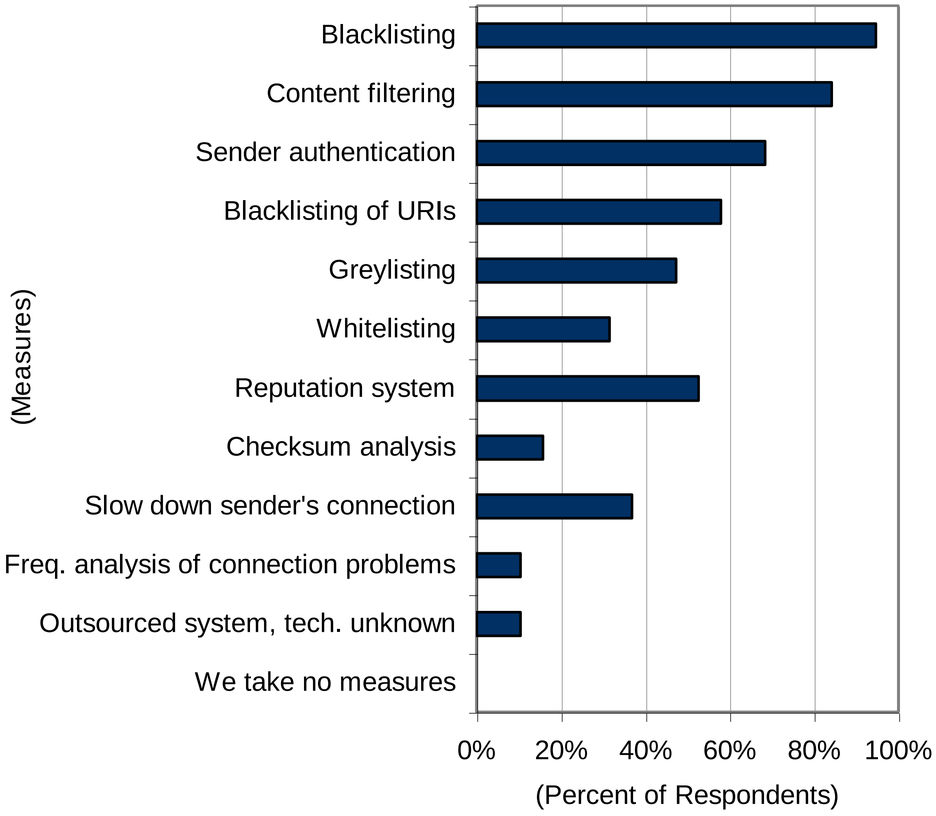
Q: Which of the following spam-filtering measures do you take on your network?



Source: ENISA anti-spam survey 2009 (N=21)

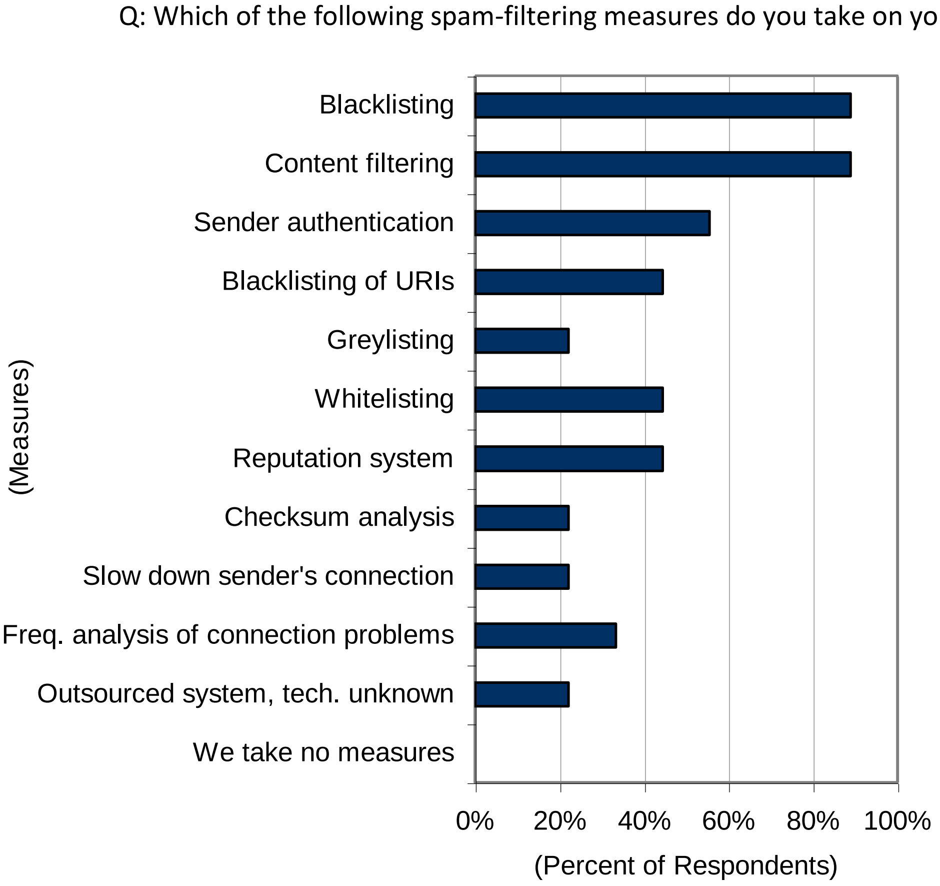
Figure 22: Spam-Filtering Measures on the Network -- Large Providers

Q: Which of the following spam-filtering measures do you take on your network?



Source: ENISA anti-spam survey 2009 (N=19)

Figure 23: Spam-Filtering Measures on the Network -- Very Large Providers



Source: ENISA anti-spam survey 2009 (N=9)

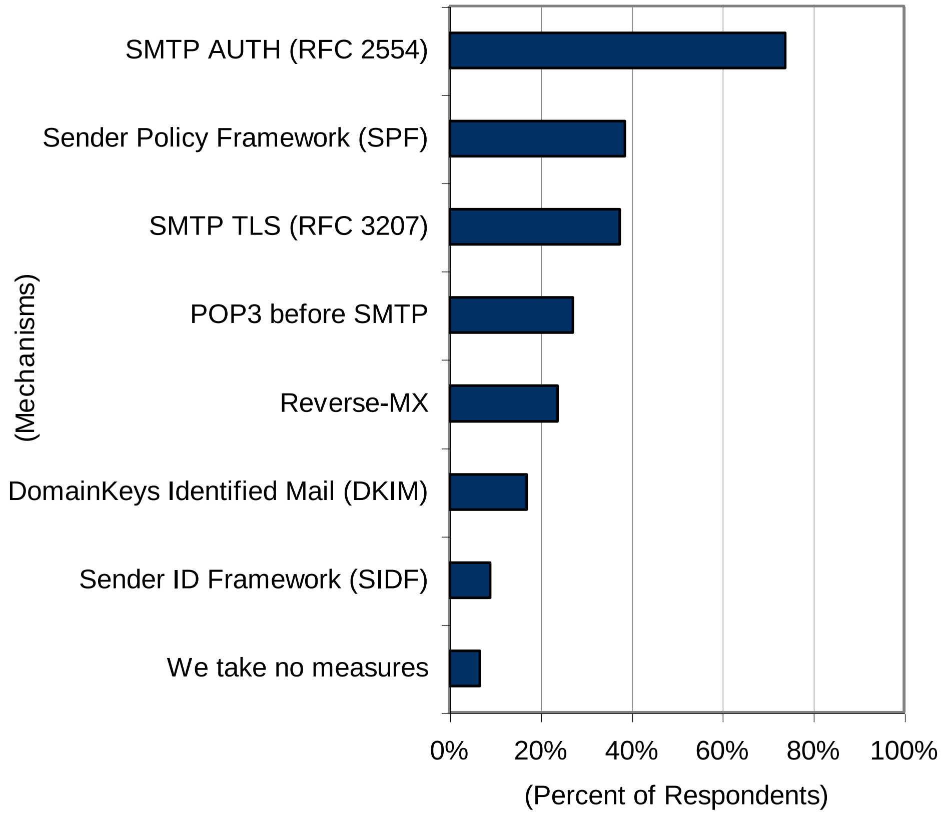
Sender Authentication Mechanisms

Sender authentication mechanisms have also remained consistent over the past two years. As before, SMTP AUTH is the dominant authentication method, used by 74% of respondents, down slightly from 2007. SMTP TLS remains next most common, followed by Sender Policy Framework (SPF), which has dropped a bit in usage and now is third-most common.

Two technologies that have gained ground are Domain Keys Identified Mail (DKIM—up from about 5% to 17%), and Sender ID Framework (SIDF—up from about 5% to 9%).

Figure 24: Sender Authentication Mechanisms

Q: Which of the following sender authentication mechanisms do you implement?



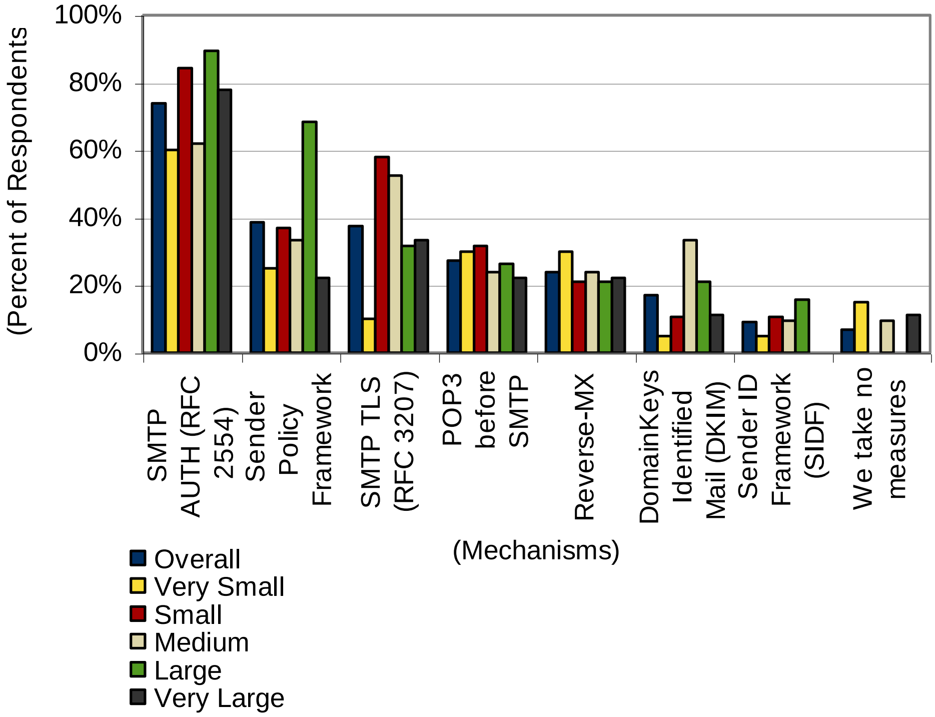
Note: One additional measure mentioned was Simple Authentication and Security Layer (SASL)

Source: ENISA anti-spam survey 2009 (N=88)

There is not great variation by size of provider except that SPF is particularly common among large providers, while DKIM stands out among medium-sized providers (see Figure 27). Generally, though, size is not a major correlating factor.

Figure 25: Sender Authentication Mechanisms, by Size of Company

Q: Which of the following sender authentication mechanisms do you implement?



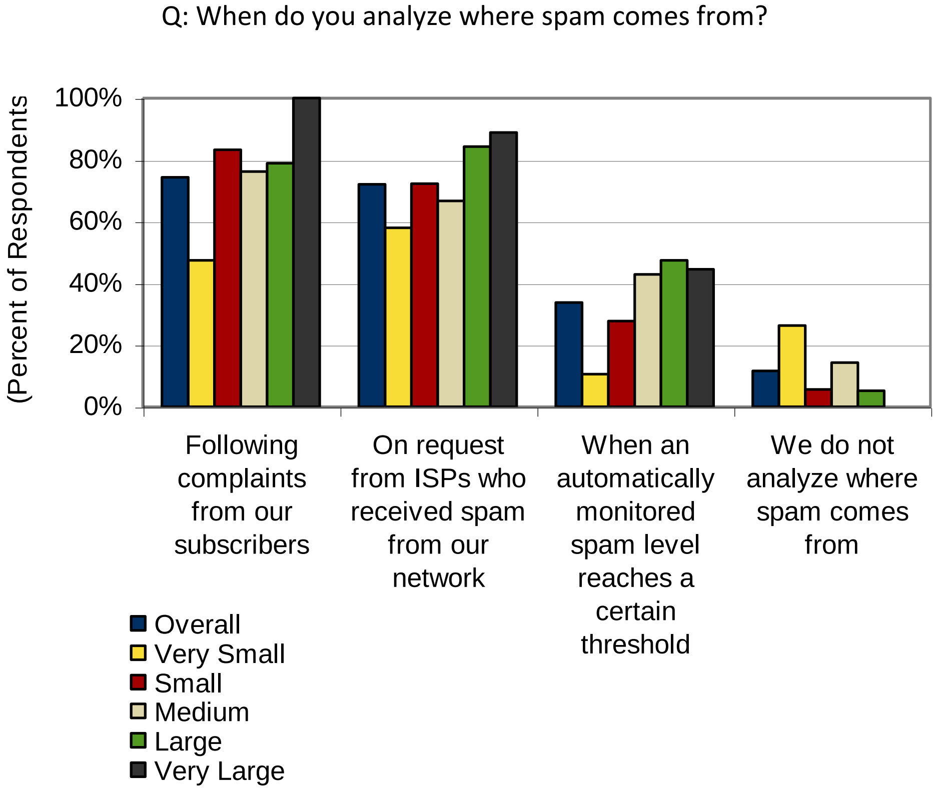
Note: One additional measure mentioned was Simple Authentication and Security Layer (SASL)

Source: ENISA anti-spam survey 2009 (N=88)

Identifying Sources of Spam

Usually, providers analyze the sources of spam when notified by a customer or by another ISP of a problem that they need to investigate (see Figure 28). A smaller but significant percentage of providers analyze the source when automatically monitored spam levels reach a certain threshold. Very few providers said that they do not analyze the source of spam.

Figure 26: Identifying the Source of Spam



Note: Other responses included continuous monitoring of spamtraps, log files and other data.

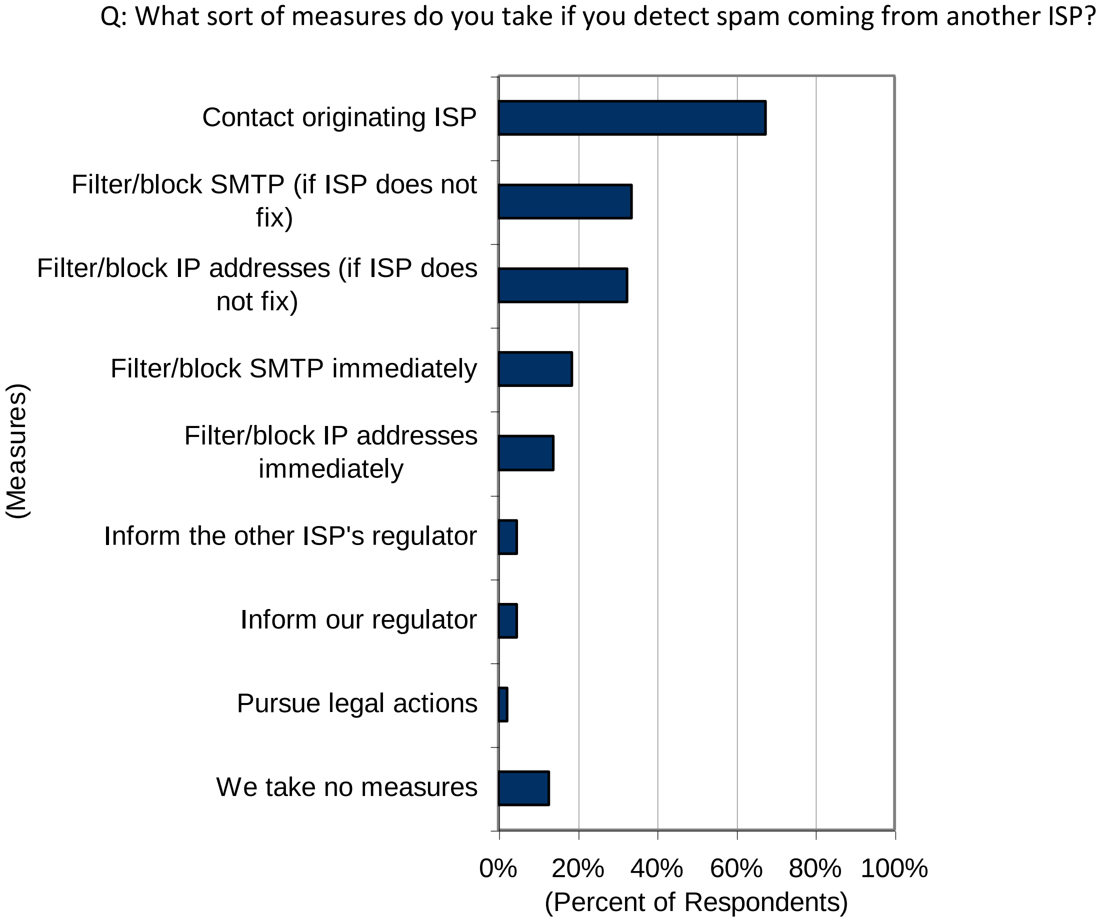
Source: ENISA anti-spam survey 2009 (N=86)

Measures after Detecting Spam from another ISP

Once spam is detected, two thirds of providers contact the originating ISP to discuss measures that they can take (see Figure 29). The next-most common actions are to filter or block the originating SMTP connections or IP addresses, if the source ISP does not solve the problem. Thus, most of the responses are collaborative and constructive.

A much smaller number immediately block SMTP connections or IP addresses, without waiting for notification and the other ISP's actions to take effect. In a very few cases, providers stated that they notify either their own National Regulatory Authority, or that of the originating ISP, or pursue legal actions.

Figure 27: Measures after Detecting Spam from Another ISP



Note: Several respondents also mentioned reporting the abuse to a reputation black list.

Source: ENISA anti-spam survey 2009 (N=86)

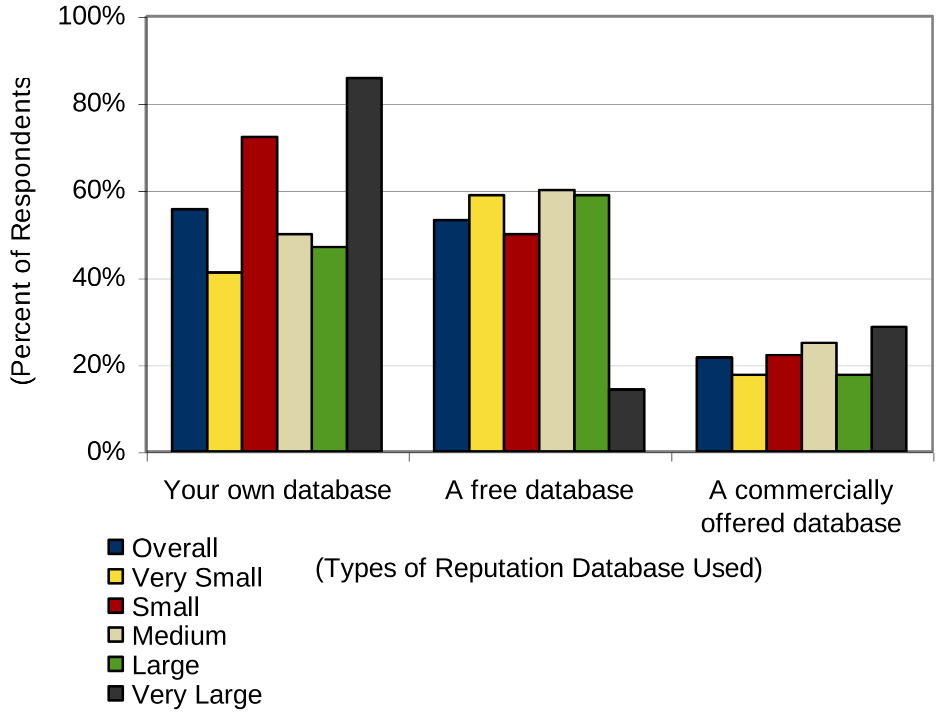
Reputation Databases

Types of Reputation Database Used

For those providers that use reputation databases, we asked what kind of database they use. Results varied. Over 50% use their own databases, while a similar number use a free database (see Figure 30). Less than a quarter use a commercially offered database. Usage by size of provider varies, though not consistently. Very large and small providers tend to use their own databases more frequently than the average, while large and very small lean more toward free databases. Commercial databases are the one less-preferred category. As in the case of software applications to combat spam (see below), clearly some providers value the services provided commercially, while some others strongly prefer open-source or free solutions.

Figure 28: Types of Reputation Database Used

Q: To maintain blacklists and other similar lists, what kind of reputation database do you use?



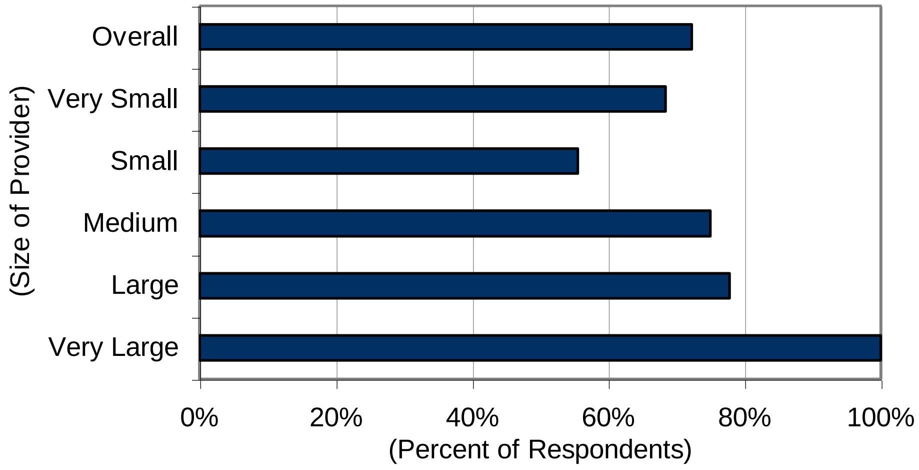
Source: ENISA anti-spam survey 2009 (N=79)

Accuracy of Blacklists

While blacklists are some of the most commonly used and important tools in the anti-spam arsenal, they do attract some criticism. In the survey, we asked providers if they have ever had their servers incorrectly added or retained on a blacklist, and nearly three quarters said yes (see Figure 31). Especially the largest providers reported this problem, with 100% having had such an experience.

Figure 29: Experienced Accuracy of Blacklists

Q: Have you ever had your servers wrongfully added to a blacklist, or wrongfully retained on a blacklist after spam problems were corrected?



Source: ENISA anti-spam survey 2009 (N=83)

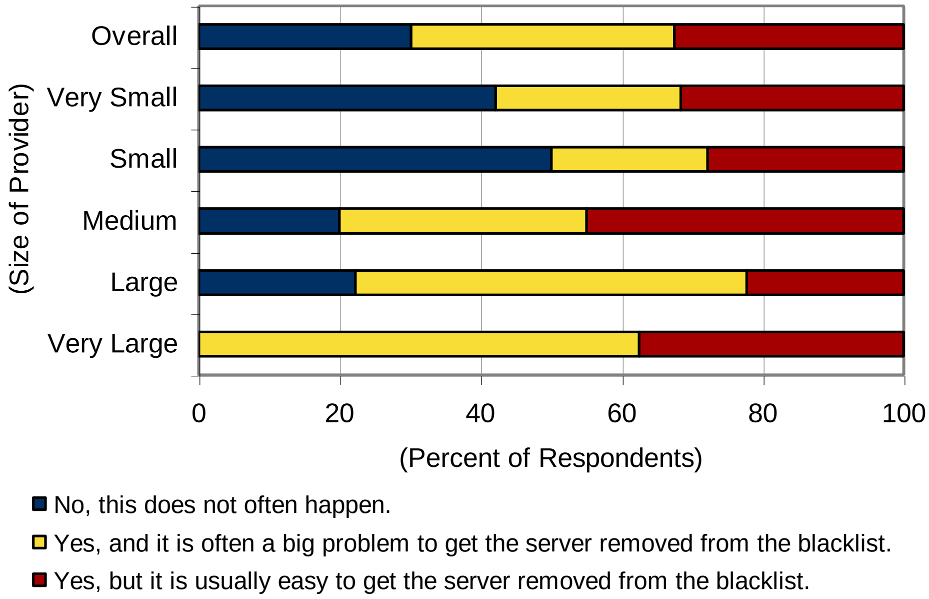
Similarly, when asked if they think that major blacklists sometimes include servers that need not be blacklisted, all of the largest providers, and most of the total said "yes" (see Figure 32). If these, about half said that the problem is usually easy to fix, though. Still, about one third of respondents said that it does happen and that it is often a problem to get the error corrected.

This criticism may be unavoidable when the definition of spam, and the measures that each operator should take to prevent the sending of spam from their networks, are undefined. Similarly, with such large volumes of data on the blacklists, and with spammers seeking to use (often fraudulently) the computers and servers on legitimate providers' networks, it is not surprising that blacklists may add legitimate servers at times, or that disputes can occur. And with so many different blacklists in use, including many developed by providers themselves internally, removing a server from a blacklist may not always be a clear-cut process.

Blacklists are the most effective anti-spam tool in use (as will be seen below), but many providers clearly hope to see greater responsiveness from blacklist providers/developers in terms of evaluating servers that should be removed from the list.

Figure 30: Perceived Accuracy of Blacklists

Q: Do you believe that major blacklists sometimes incorrectly include servers that are not (or are no longer) responsible for spam?



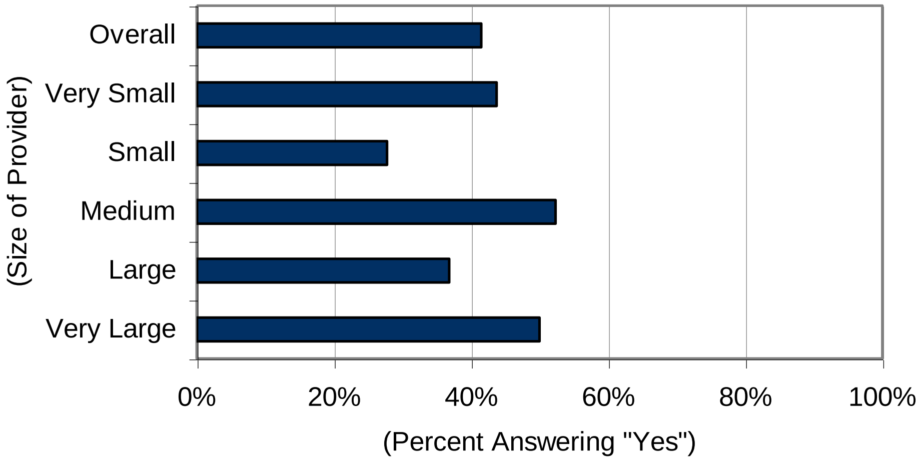
Source: ENISA anti-spam survey 2009 (N=83)

Planned Anti-Spam Measures

Looking ahead, over two fifths of providers plan to implement new anti-spam measures within the next six months (see Figure 33).

Figure 31: Planned Anti-Spam Measures in the Next Six Months

Q: Do you plan to install or implement an anti-spam method in the next six months?



Source: ENISA anti-spam survey 2009 (N=82)

A variety of measures was mentioned as being planned for the next six months. Reputation databases were mentioned at least nine times, far more than any other category. Most of these are plans to deploy new blacklists, but some also mentioned greylists. Some other topics mentioned multiple times include Port 25 blocking or management, which was mentioned three times; DKIM issues mentioned three times; and many different software applications, both opensource and commercial, were mentioned once or twice each.

Others mentioned plans to increase transparency of the system, improve management, outsourcing spam filtering, checksum analysis, URI filtering, SPF protocol, and others.

Anti-Spam Software Solutions

When asked about software applications used to combat spam, many respondents emphasized that open-source software plays a prominent role in fighting spam. By far the most commonly mentioned software was SpamAssassin, a free open-source application that uses a combination of anti-spam measures, including DNS-based and checksum-based spam detection, Bayesian filtering, blacklists and online databases. No other application was mentioned nearly as many times, though dozens of other commercial and open-source applications were also mentioned, though usually once or twice each. The variety of choices, and the frequency of selection of both commercial and open-source applications, reflect the important role that both the open-source and commercial anti-spam activities play in the fight against spam.

Processing Abuse Reports

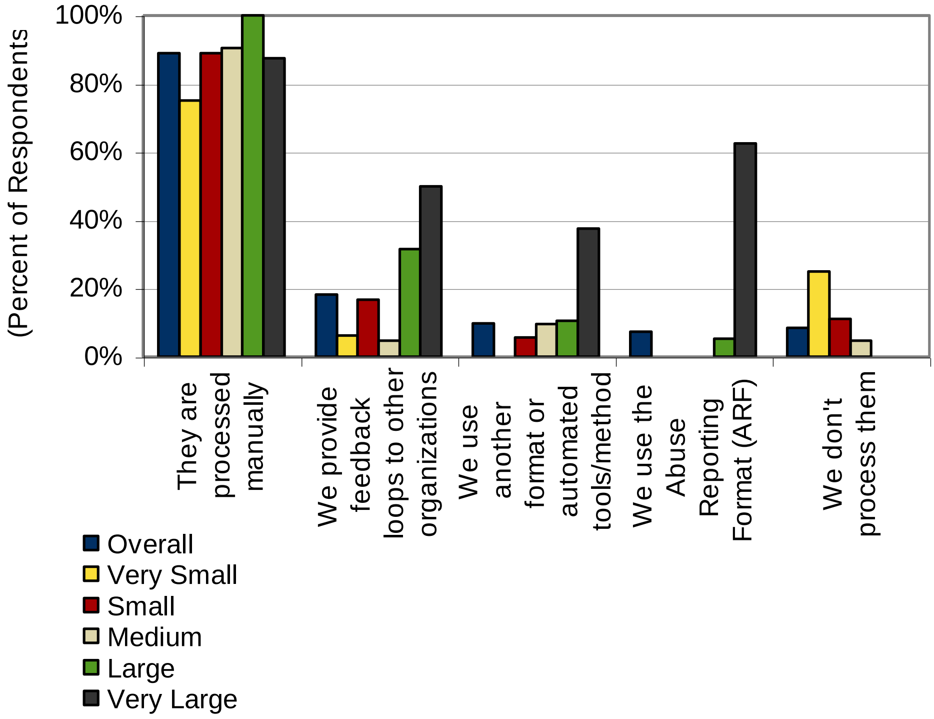
In most cases, abuse reports are processed manually. In the 2007 survey, 73% processed them manually, and that proportion has now increased to 89% (see Figure 34).

Only a small percentage of respondents (16%) provide feedback loops to other organizations. By contrast, in the 2007 survey, nearly half reported contacting an ISP directly when receiving spam from their network. This seems to be a sharp drop in notification to originating providers.

Only 8% of respondents reported using the Abuse Reporting Format (ARF), though all of these are very large or large providers, which account for most of the market. This 8% level has remained stable since 2007.

Figure 32: Processing Abuse Reports

Q: How do you process abuse reports?



Note: Most of those mentioning other reporting formats, tools or methods stated that these are developed in-house.

Source: ENISA anti-spam survey 2009 (N=82)

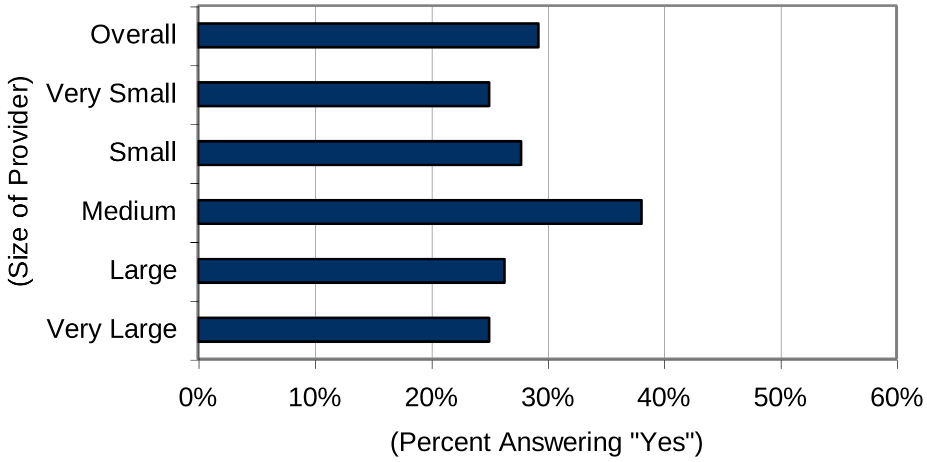
Conflicts between Spam Filtering and Obligations to Deliver and Protect Privacy

Nearly a third of providers reported that they think there are conflicts between the use of spam filtering and the ISP's obligation to deliver messages and to protect privacy (see Figure 35). This figure remains essentially unchanged since the 2007 survey, despite efforts to clarify the situation from some agencies and international bodies. In particular, the European Commission created the Article 29 Data Protection Working Party to review this question and advise on the legality of spam filtering. The Working Party found, in a 2006 publication of its findings (see Additional Resources below), that spam-filtering can be justified under the EU's legal framework for privacy and communications, based on the requirement to provide secure communications. The findings further stated that service providers should take certain steps to ensure that their spam filtering is fully compliant, including informing the users about the filtering, and giving the users flexibility and tools to decide what kinds of messages should be filtered out or delivered, or to opt out altogether.

The Working Party's findings should satisfy many anti-spam managers about the legality of spam filtering. Yet three years after the Working Party's findings, there is still a significant share of respondents expressing concern and uncertainty about this issue. The authors of this study recommend greater publicity of the Working Party findings in the anti-spam community by ENISA, other EU institutions, national data protection agencies, and other organizations that regularly participate in the anti-spam dialogue.

Figure 33: Potential Conflict between Spam Filtering and ISP's Obligations to Protect Privacy and Deliver Mail

Q: Do you think that there is a conflict between the use of spam filters that block some messages and the ISP's obligations to deliver messages and protect privacy?



Source: ENISA anti-spam survey 2009 (N=82)

Of those stating that there is a conflict, the most common problem cited was false positives. Eleven of the 26 respondents cited false positives-- and associated factors-- as the most important conflict. Some respondents noted in particular the threat of legal action by, and compensation for, customers, as a result of false positives.

The next most common conflict area concerned privacy. For example, several respondents noted legal risks around the analysis of email content. One respondent pointed to the need to filter out spam in order to preserve the service, but what to do about customers that do not give consent to this filtering? Similarly, when an email is potentially a false positive, the content must be analyzed, requiring customer consent.

Another problem mentioned multiple times concerned the grey area between clearly legitimate messages and clearly spam messages. One respondent pointed out that one customer's spam may be another customer's legitimate email. Another noted that badly configured mail servers can be blocked as spam by others, despite being legitimate.

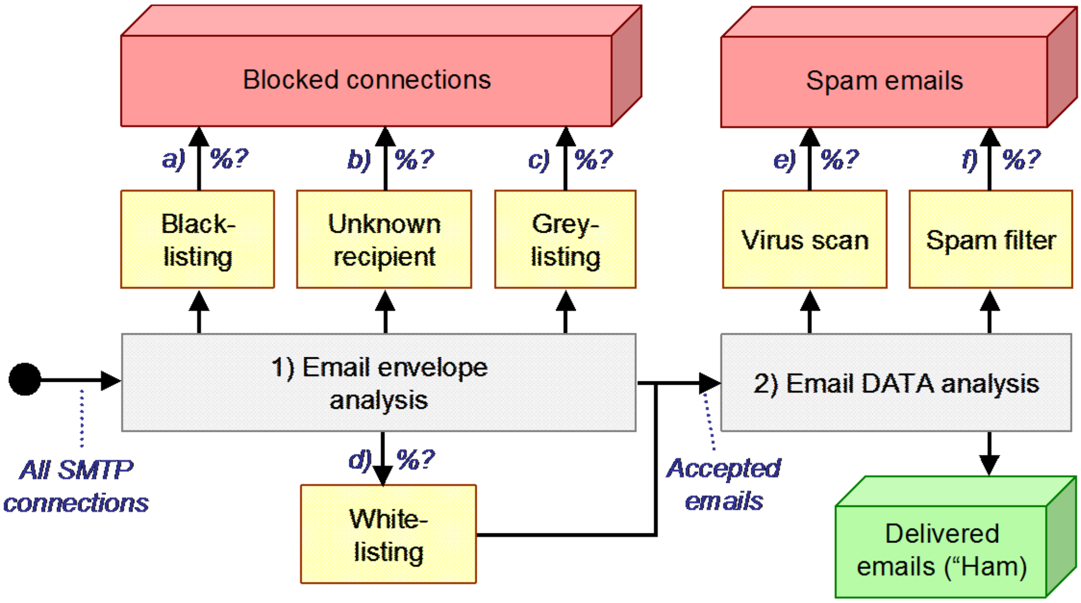
Clearly, many providers are concerned about this apparent conflict, suggesting that regulatory authorities may need to clarify the issues and untangle the conflict.

Effectiveness of Measures

Examining the percentage of email traffic that is blocked or filtered by different mechanisms can shed some light on the effectiveness of those measures and the overall battle against spam. At the same time, it also can give some indication of the scale of the spam problem.

We asked providers to estimate the percent of SMTP connections that are blocked or aborted due to blacklisting, greylisting or unknown recipient, as well as the percent accepted due to whitelisting, and those accepted after passing through these filters. And then of the accepted SMTP connections, we asked respondents what percent of emails are filtered out as virus-infected or spam. Figure 36 provides a diagram to visually display the process.

Figure 34: Effectiveness of Anti-Spam Measures: Diagram of Connections and Messages Blocked, Filtered, or Delivered



Source: ENISA anti-spam survey 2009

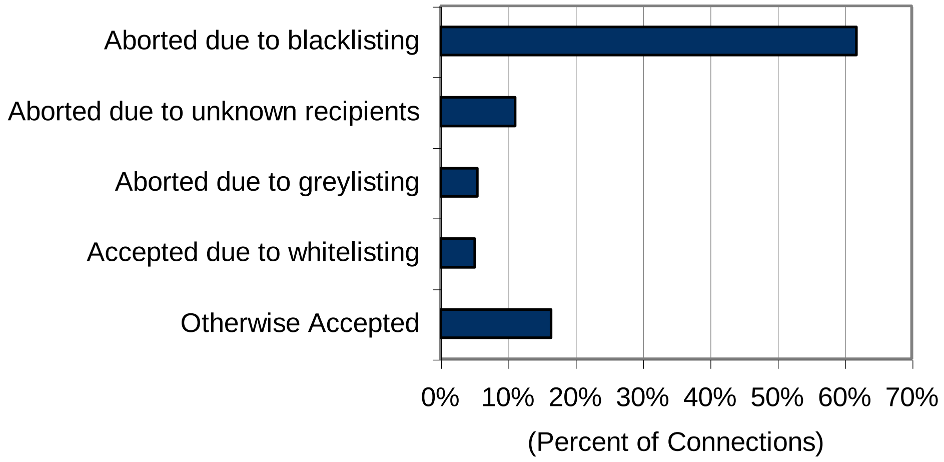
Not all respondents were able to answer, noting that, for example, the data is simply not available from the tools they use, in some cases. Nonetheless, we received answers from the majority of respondents, with a total of over 70 million mailboxes under management.

In the SMTP analysis, blacklisting accounts for the vast majority of aborted spam (see Figure 37). Aborts due to unknown recipients and greylisting also accounted for significant shares, though far below the level of blacklisting.

Whitelisting ensured the acceptance of a small share (5%), leaving a total of nearly 22% accepted.

Figure 35: SMTP Connections Aborted or Accepted

Q: Could you provide us the following information about your anti-spam system? Percentage of SMTP connections …?



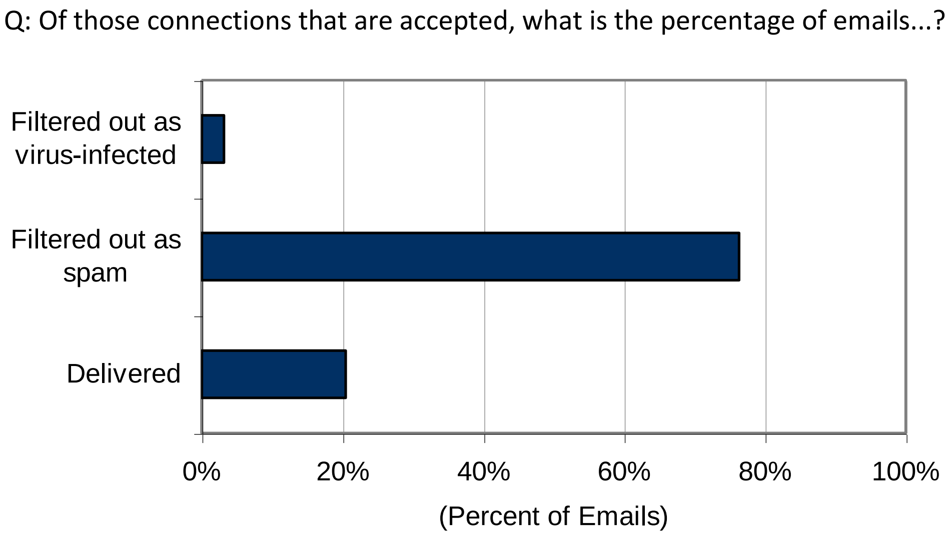
Note: The figures were obtained using a weighted average of responses, with weighting based on the number of mailboxes managed.

Note: The respondents answering this question represented over 70 million email mailboxes.

Source: ENISA anti-spam survey 2009 (N=58)

Once the messages are accepted, they are then analyzed by virus scanners and spam filters. Virus scans eliminate only a small share (3%), while three quarters are filtered out as spam. The remaining 21% of messages are actually delivered (see Figure 38).

Figure 36: Accepted SMTP Connections Resulting in Blocked or Delivered Email



Note: The figures were obtained using a weighted average of responses, with weighting based on the number of mailboxes managed.

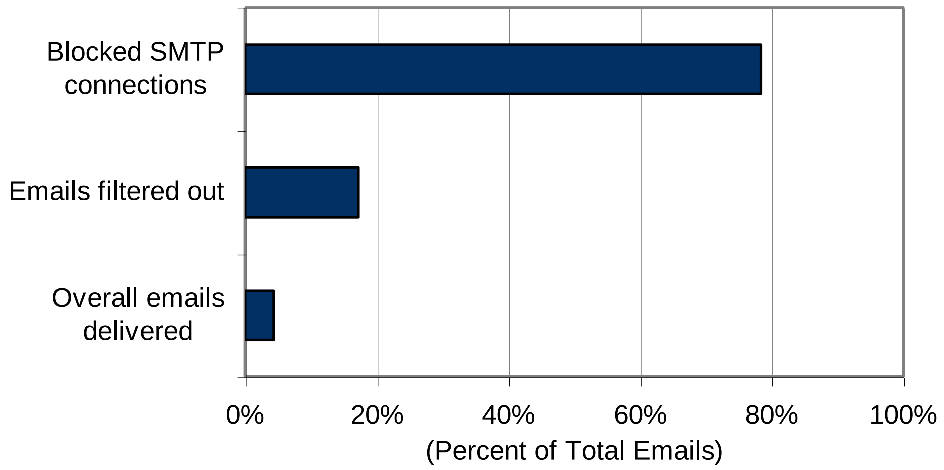
Note: The respondents answering this question represented over 70 million email mailboxes.

Source: ENISA anti-spam survey 2009 (N=58)

As a result of these various steps, very little of the total email traffic is delivered. Only 4.4% is delivered (see Figure 39), with 95.6% blocked by the various anti-spam measures. These figures are similar to data published by the Messaging Anti-Abuse Working Group (MAAWG) in its quarterly analysis of abusive email blocked by its members worldwide (see Additional Resources below), though the MAAWG data tends to show a slightly higher percentage of mail is delivered.

With only a small portion of email traffic being delivered, the anti-spam measures in use appear to be cumulatively effective. Each of the various anti-spam measures plays an important role in the process, preventing email systems from being swamped by spam, and preventing users from being exposes to most of the fraudulent email that poses security and privacy threats.

Figure 37: Overall Email Traffic Blocked or Delivered



Note: Emails filtered out and overall emails delivered are calculated by multiplying the percentages for each by the percent of accepted SMTP connections.

Note: The figures were obtained using a weighted average of responses, with weighting based on the number of mailboxes managed.

Note: The respondents answering this question represented over 70 million email mailboxes.

Source: ENISA anti-spam survey 2009 (N=58)

Conclusions

Email providers almost unanimously treat spam as a security issue to be handled by the security department. This step alone suggests that spam is considered to be an important technical threat that must be addressed carefully and correctly. Yet providers generally feel that it is a significant, but not critical, part of security operations. The reason is that spam's impact on the business has been greatly reduced through effective anti-spam measures.

These measures currently filter out over 95% of email traffic, using a variety of methods, greatly reducing the volume of spam that customers receive, without causing significant problems with false positives. Anti-spam measures are doing their job, reducing the threat of spam to a manageable security process. This process still requires focus, expertise and resources, but it is arguably predictable.

The major tool categories of the anti-spam manager have not changed greatly over the past two years. Generally, the same measures are applied by roughly the same percentages of providers, though these measures themselves have evolved and improved, such as constantly improving blacklists and software solutions. Providers employ a combination of these tools to filter out spam, though the precise combination varies by provider.

Spam prevention is not only a matter of protecting customers from external spammers. Several respondents emphasized the need for a coordinated approach against spam, and a key part of that is for providers to shut down spammers among their own customers, before sending the spam on to other service providers.

There are still some gaps in the anti-spam efforts. In particular, abuse reporting to other ISPs and authorities could be improved and automated, while blacklist providers need to ensure that their lists do not incorrectly include some domains that are not (or no longer are) spamming. Generally, collaborative approaches are developing and proving successful, but there is much more that can be done to collaboratively address the problem of spam.

Recommendations

Though anti-spam measures are proving generally effective, these efforts could still be improved. For example:

- Email providers should take a more proactive approach to monitoring spam and identifying the source, so that appropriate actions can be taken by originating ISPs.
- Blacklist managers need to ensure that it is easy to remove a server or domain from a blacklist when spam problems have been rectified. And with so many different blacklists in use, collaborative efforts to share data on servers that should be removed from blacklists would help to address the problem. Wider use of whitelists could help in this effort.
- Providers should look to increase the abuse report feedback loops with other providers and aim to automate abuse reporting processes, possibly adopting the Abuse Reporting Format (ARF).
- Providers should seek collaborative solutions to fight spam, as many, but not all, already do. For example, notifying ISPs that originate spam that they are doing so and discussing countermeasures with them will help to cut off more spam at the source. Additionally, reporting spam sources to authorities can help them to take legal action or to develop appropriate policies to address such sources.
- Policy-makers and regulatory authorities could help spam prevention efforts by further clarifying the apparent conflicts between spam-filtering, privacy, and obligation to deliver. Promotion of the findings of the Article 29 Data Protection Working Group would help this effort.

- Institutions that aim to aid public and private efforts against spam should promote open collaborative solutions to spam, such as reporting of spam sources to other ISPs and authorities; the Abuse Reporting Format; contribution to collaborative solutions; and sharing of best practices across the industry to aid providers that need to improve their anti-spam measures.

Appendix

Additional Resources

There are many additional resources that can be useful in further investigating, tracking, and participating in the anti-spam dialogue. Selected examples are highlighted below.

The Article 29 Data Protection Working Party, "Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services", 21 February 2006 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf). In this document, the Working Party explains its view on the legal basis for spam filtering.

ETIS, a global association of telecommunications service providers, has an Information Security Working Group that contributes to anti-spam efforts, along with other security initiatives. More information is available at http://www.etis.org/activities/Information_Security_Group.asp

EuroISPA, the European ISP Association (http://www.euroispa.org/). EuroISPA represents European ISPs, participating in industry discussions and publishing position papers on issues relevant to its members.

The Verband der Deutschen Internetwirtshaft e. V. (eco) is very active in the anti-spam dialogue, including hosting regular anti-spam summits. The most recent summit information can be found at http://www.eco.de/antispamsummit2009.

The Messaging Anti-Abuse Working Group (MAAWG) regularly publishes findings on the abusive emails blocked or filtered by its members. A study can be found at http://www.maawg.org/about/MAAWG_2008-Q3Q4_Metrics_Report.pdf. Much more information about global anti-spam efforts can be found at the MAAWG website at http://www.maawg.org.

The disconnection of the **McColo server farm** in California in November 2008 temporarily reduced the amount of spam being sent worldwide and yielded useful insight into both spam's origination and the effectiveness of anti-spam measures. Richard Clayton of the University of Cambridge, UK, published one study of the anti-spam measures during that period, called **"How much did shutting down McColo help?"** that can be found at http://www.ceas.cc/papers-2009/ceas2009-paper-16.pdf.

Additional insight into the impact of the McColo server farm on spam can be found in **Symantec's** monthly reports called **"The State of Spam"**, which can be found at http://www.symantec.com/business/theme.jsp?themeid=state_of_spam.

Definitions

The list below illustrates ENISA's understanding of some more specialized terms that are used in the context of this study and the survey. Definitions by external parties (e.g. Wikipedia) have been checked and sometimes adjusted by ENISA.

ARF: Abuse Reporting Format, see http://mipassoc.org/arf/

Bayesian filtering: Bayesian filtering is a statistical technique of e-mail filtering based on the probability of word occurrences.

BC(P): Business Continuity Planning (BCP) is a methodology used to create a plan for how an organization will resume partially or completely interrupted critical function(s) within a predetermined time after a disaster or disruption. BCP may be a part of a larger organizational effort to reduce operational risk associated with poor information security controls, and thus has a number of overlaps with the practice of risk management. – Source: Wikipedia

Blacklist: A blacklist is a list or register of entities who, for one reason or another, are being denied a particular privilege, service, or mobility. –Source: Wikipedia

Content Filtering: Content filtering is the most commonly used group of methods to filter for security problems (e.g. viruses). Content filters act either on the content, the information contained in the mail body, or on the mail headers (like "Subject:") to either classify, accept or reject a mail. – Source: Wikipedia/ENISA

DDoS: A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. – Source: Wikipedia

DNSSEC: DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System (DNS) used on Internet Protocol networks. It is a set of extensions to DNS, which provide origin authentication of DNS data, data integrity, and authenticated denial of existence (i.e. authenticated non-existence reply). DNSSEC was designed to protect the Internet from certain attacks such as DNS cache poisoning. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the info on the authoritative DNS server. – Source: Wikipedia, based on RFC 4033-4035

DomainsKeys Identified Mail (DKIM): DKIM provides a method for validating an identity that is associated with a message, during the time it is transferred over the Internet. That identity then can be held accountable for the message. In most cases the signing MTA acts on behalf of the sender by inserting a DKIM-Signature header, and the verifying MTA on behalf of the receiver, validating the signature by retrieving a sender's public key through the DNS. – Source: Wikipedia, http://www.dkim.org

Greylist: A mail transfer agent which uses greylisting will "temporarily reject" any email from a sender it does not recognize. If the mail is legitimate, the originating server will try again to send it later, at which time the destination will accept it. If the mail originates from a spammer, the spammer will probably not resend it. – Source: Wikipedia, shortened

Real-time anomaly detection: Anomaly detection tries to discover malicious behaviour by comparing current behaviour to learned normal models of behaviour. An anomaly detection approach usually consists of two phases: a training phase which defines what is normal and a working phase which compare new data to the learned model. – Source: Long Fei (Purdue University)

Reputation system: A reputation system is a type of collaborative filtering algorithm which attempts to determine ratings for a collection of entities, given a collection of opinions that those entities hold about each other. In detail, these systems can be used to exchange characteristics of spammers (e.g. IP, domain). – Source: Wikipedia, ENISA

Sender ID: Sender ID is an anti-spam proposal from the MARID IETF working group that joined Sender Policy Framework (SPF) and Caller ID. – Source: Wikipedia

Sender Policy Framework (SPF): Sender Policy Framework (SPF) is an extension to Simple Mail Transfer Protocol (SMTP), the standard Internet protocol for transmitting email. SPF makes it easier to counter most forged "From" addresses in e-mail, and thus helps to counter email spam. – Source: Wikipedia

SMTP Authentication: SMTP authentication allows a requested authentication mechanism, which performs an authentication protocol exchange to authenticate and identify the user. The authentication mechanism can be for example ESMTP AUTH LOGIN / PLAIN, TLS, Kerberos, GSSAPI. – Source: RFCs 2554, RFC 2222, ENISA

Spamtraps: Spamtraps are usually e-mail addresses that are created not for communication, but rather to lure spam. Since no e-mail is solicited by the owner of this spamtrap e-mail address, any e-mail messages sent to this address are immediately considered unsolicited. – Source: Wikipedia

Whitelist: A whitelist is a list of accepted items or persons in a set. This list is inclusionary, confirming that the item being analyzed is acceptable. – Source: Wikipedia