FAQs to the third ENISA Anti-Spam Measures Survey “What Are the Measures Used by European Providers to Reduce the Amount of Spam Received by Their Customers?

What is the reason for ENISA to do a report on spam?

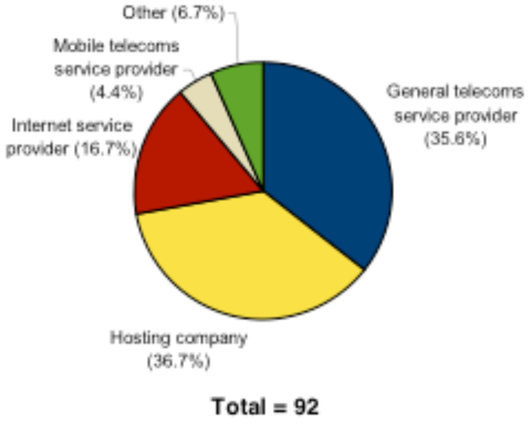
ENISA has long been active in the fight against spam and this is the third survey ENISA has conducted on spam. The reason for this is that email has become a critical part of the foundation of modern electronic communications and since email systems have been bombarded for several years with huge volumes of unsolicited bulk mail, much of it fraudulent, illegal, and threatening to ICT security.

The survey results, presentations, and forums for debate on anti-spam measures constitute key contributions ENISA makes in this effort.

How was this report conducted and what is included in the report?

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.

Respondents by type of company



What are the operational aspects of spam?

When looking at the operational 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. The survey results show that most providers are currently managing to prevent spam from greatly harming the customer experience, though spam continues to impose costs on helpdesks.

What are the anti-spam costs for the service providers?
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.

Don't all of the email providers now have spam prevention to their customers?
The spam prevention efforts appear to have made spam manageable, making anti-spam measures a standard part of operations. Spam is an important business challenge that must be addressed to retain customers, but it is not a critical concern for most providers.

What are the measures to detect spam?
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.

What are the other technical measures to prevent spam?
Besides detecting spam, some of the technical measures to prevent spam are

- **Preventing Sending of Spam**
  Blocklists were the most commonly used measure to prevent sending of spam, followed closely by limiting high outbound mail volumes

- **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 blocklisting, content filtering, and sender authentication.

- **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.

- **Sources of Reputation Databases**
  Since blocklists 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.

- **Reliability of Blocklists**
  With blocklists so important in blocking spam, their reliability is crucial.

- **Planned Anti-Spam Measures**
  Close to half of providers stated that they plan to implement new anti-spam measures within six months.

- **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.

- **Abuse Reporting**
  By far the most common way to process abuse reports exchanged between providers were manually. Only a few providers process them automatically.

- **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.

Are these measures taken enough?
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 blocklists. 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.

Does the segmentation analysis of survey results show any difference between the different providers?
When analyzing the results of the survey ENISA examined the results by different segments. There was little variation when looking at different types of companies (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.

What are the conclusions and what is the difference compared to the findings of the previous spam surveys?
The survey shows that spam is an ongoing management challenge 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.

Another finding is that many of the providers are, although usage levels of various measures have remained constant, upgrading their measures to ensure that they remain effective.

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.

What are ENISA's 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.

- Blocklist managers need to ensure that it is easy to remove a server or domain from a blocklist when spam problems have been rectified. And with so many different blocklists in use, collaborative efforts to share data on servers that should be removed from blocklists 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.

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

For press release:
http://www.enisa.europa.eu/media/press-releases/spam-survey-2009-the-fight-against-spam

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

For further details, contact:
Pascal Manzano, Expert Network Security Policy, ENISA, tel: +30 2810 391366
Ulf Bergstrom, Spokesman, ENISA
press@enisa.europa.eu, Mobile: +30 6948 460143