Task Force on Spam

EDUCATION AND AWARENESS RAISING
FOREWORD

The OECD Task force on Spam discussed this document during its meeting in March 2005, and recommended it for declassification to the CCP and ICCP Committees through a written procedure, which was completed on 28 July 2005.

The report was prepared by Ms Mina Park, of the OECD Secretariat. It is published under the responsibility of the Secretary-General of the OECD.

Copyright OECD, 2005.

Applications for permission to reproduce or translate all or part of this material should be made to:

Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.
TABLE OF CONTENTS

ELEMENT 5: EDUCATION AND AWARENESS RAISING ............................................................... 5

1. Introduction ......................................................... 5
2. Why do we need education and awareness-raising as part of an anti-spam strategy? .............. 6
3. Raising awareness .................................................. 7
   3.1 Media Coverage .................................................. 7
   3.2 National Campaigns .......................................... 7
   3.3 Industry cooperation and educational initiatives ................................................................. 8
   3.4 Websites ............................................................ 9
4. Education on Spam .................................................. 10
   4.1 Targeting Student, Children, and Parents ................................................................. 10
   4.2 Targeting Individuals ........................................... 11
   4.3 Targeting ISPs/ESPs ............................................. 12
   4.4 Targeting Business Entities, especially SMEs .............................................................. 12
   4.5 Targeting Direct Marketers .................................. 12
5. Anti-spam tricks and tips: What needs to be communicated to Internet users? ......................... 13
   What is spam, and what are the dangers? ............................................................... 13
   How to avoid spam ................................................ 13
   How to react and to file complaints when one receives spam ................................................. 14
   What preventive measures may be taken? ................................................................ 14
   Where to find more information ............................................................. 14

ANNEX I. AWARENESS AND EDUCATION ACTIVITIES IN OECD MEMBER COUNTRIES... 15

Australia ......................................................................................................................... 15
Belgium ............................................................................................................................ 15
Canada ............................................................................................................................ 16
Czech Republic ............................................................................................................. 16
Finland ............................................................................................................................ 16
France ............................................................................................................................ 16
Germany ......................................................................................................................... 16
Greece ............................................................................................................................. 17
Ireland ............................................................................................................................. 17
Italy .................................................................................................................................. 17
Japan ............................................................................................................................... 17
Korea ............................................................................................................................... 17
Mexico ............................................................................................................................. 18
Domestic actions .......................................................................................................... 18
International activities ................................................................................................. 18
Private sector activities ............................................................................................... 19
Netherlands .................................................................................................................... 19
New Zealand ................................................................................................................ 19
Norway ........................................................................................................................... 20
Spain ............................................................................................................................... 20
Sweden ........................................................................................................................... 20
Switzerland ..................................................................................................................... 20
United Kingdom ................................................................................................................................. 21
United States ..................................................................................................................................... 21

ANNEX II. SPAM MATRIX .................................................................................................................. 22

NOTES ................................................................................................................................................. 27
ELEMENT 5: EDUCATION AND AWARENESS RAISING

1. Introduction

1. Element 5 of the OECD Anti-Spam Toolkit aims to create an on-line repository (webpage) for a range of resources and education and awareness publications that have been or are being developed across a range of languages, targeted at educating and raising awareness about spam and related topics. This will include information targeted for consumers, ISPs, government agencies, and business, covering such issues as:

- Understanding spam and other malicious codes, and how to avoid them.
- What is “phishing” and how to recognize it?
- What is “spyware” and how to avoid it?
- Computer hijacking and zombie machines, how they work, and measures to avoid being hijacked.
- General information resources about the nature and extent of the spam problem in individual countries.
- How to avoid unintentionally sending what could be considered spam.
- How to report spam or take action against spammers.

2. These resources will support the work of other private or public bodies that are willing to undertake similar initiatives - in particular in developing economies - and which would benefit from already available material. In addition, by identifying ongoing and planned initiatives around the world, this element will facilitate agencies with similar requirements to work together and develop collaborative output, minimizing duplication of effort and reducing the cost of deliverables. The website will also promote the development of best practices and highlight success stories.

3. The paper, and the relating website, focuses not only on spam-specific educational and awareness-raising initiatives, but includes also information material about scams perpetrated through spam, as happens in the case of “phishing” and “spyware”, i.e. malicious code distributed to a large number of people through spam messages.

4. Some initiatives which are being taken in the area of education and awareness are as mentioned below.

5. For the purpose of this paper, “awareness-raising” and “education” initiatives are defined as follows:¹

6. **Awareness-raising initiatives** are any initiatives that help targets to obtain knowledge of the subject and improve their ability to react to situations and increase their level of alertness.
7. **Education initiatives** are any initiatives that generally aim to create an understanding of various concepts and perspectives which promote critical thinking. They emphasize interconnection and integration between theory and practice. Programmes for children are some examples.

8. **Training initiatives** are any initiatives that transfer knowledge and know-how that is required for successful performance in a job, occupation, or profession. Security training for network administrators is one example.

9. As education and training are similar concepts, the word education will be used to indicate both education and training.

2. **Why do we need education and awareness-raising as part of an anti-spam strategy?**

10. Educate users not to buy or respond to spam messages: One of the reasons why spammers are successful is that a certain number of e-mail recipients are still responding to spam, purchasing advertised products or services, visiting websites advertised by spammers, or being tricked into responding to requests for personal information from ‘phishing’ scams. Considering the low cost of sending spam, it is sufficient that even a very small percentage of users respond by purchasing from spammers to allow them to make a profit, and therefore to provide an incentive to continue spamming. OECD countries have recognised through their discussions that part of the solution to eradicate spam consists in reducing the spam revenue flow. Increasing education and awareness is therefore an important part of a comprehensive anti-spam strategy as it helps in reducing the potential “market” of spammers and consequently their financial incentives.

11. Provide clear information on the limits of legitimate online marketing and spam: Education and awareness-raising can also help diminish spam which is sent by legitimate online operators and direct marketers who are unaware of laws and regulations regarding unsolicited electronic communications. This can be done by providing a check list clearly identifying which types of electronic communications are illegal, while at the same time underlining the sanctions that may be applied for breaching the law.

12. Educate users to improve their computer security: An increasing number of unsolicited messages are being transmitted through intermediaries who are unaware that this is taking place. This could take place through open relays and open proxies which allow a computer to route e-mail to other Internet mail addresses, or through “zombie computers”, i.e. machines which have been infected by Trojans programmes, and are under the control of a malicious hacker without the knowledge of the computer owner. Zombies can be used to send spam messages or launch DoS attacks.

13. Spam, viruses and spyware are just a part of the broader problem of information security: Education and awareness-raising in the context of spam is a broader concept than just dealing with the purchase of goods and/or services advertised in spam. The issue also deals with information security in general, to educate users on how to protect their computers and their personal information, and avoid being the victims of computer crimes. In this context education and awareness needs to cover individual consumers as well as corporate users and companies.
3. Raising awareness

14. Many users of the Internet and of e-mail who receive spam on a regular basis have not been given sufficient information on how to avoid getting spammed, how to react to spam and often are not aware of the harm that can result from opening spam. It is important that these users are provided with the basics of Internet “hygiene” to ensure that they do not take actions which may stimulate further spam, or result in their computers becoming infected by either viruses or Trojans.

3.1 Media Coverage

15. Offline media coverage can play an important role in raising awareness and providing links to informative cyber security websites.

16. In northern European countries, the SAFT (Safety, Awareness, Facts and Tools), is a consortium of governmental bodies, NGOs, ICT industry and research professionals created with the support of the European Commission Internet Action Plan, which aims to create a safe and useful Internet environment for children. The consortium has launched TV advertisements, using well known SAFT cartoon characters. The consistency and persistency of the SAFT characters on TV programmes coupled with online educational resources featuring the same characters have caught children’s attention in those countries, allowing them to easily associate with the message (“pay attention to spam”) in their daily Internet activities and habits.

17. In Switzerland’s TSR 1 transmitted a documentary on spam and its security implications. Documentaries leave a strong impression on viewers and motivate them to take specific actions.

18. Some companies have their own internal TV network for their employees. Still more have internal newsletters and bulletins, and a security package is often distributed to new employees. Making best use of these media to broadcast information on spam will not only increase employees’ awareness on spam but also help secure company network. In OECD, for example, a four page leaflet of OECD Security Tips & Tricks is handed out to new employees.

19. Awareness campaigns in newspapers and IT magazines which have a large circulation, also contribute to the diffusion of information about spam, online fraud and viruses. In May 2005 a free newspaper distributed in all underground stations in Paris reported news on phishing attacks and zombie computers on its cover page, providing some basic information on how they work, and how users can avoid becoming victims of such practices.

3.2 National Campaigns

20. Some countries have launched a national day especially for internet security and safety. National campaigns tend to stimulate organisations to create activities to highlight given problems, and are usually picked-up by the news media, resulting in a wider coverage of the problems which need to be tackled and potential solutions.

The Safer Internet Day is now celebrated in 30 countries across Europe and worldwide, and involves more than 65 organizations, including ISPs and software providers.

Finland held a National Data Security Day to enhance awareness on computer security basics targeting especially the home users, the small and home offices, children and students.
Korea also holds a national e-Clean campaign every year since 2003 to boost Internet safety awareness. This e-Clean campaign harnesses government, the IT industry, children protection groups, industry, and media to promote a clean internet, and the post office and educational organisations provide the means of promotion. Telecommunication ethics courses for children, parents, and teachers are also set up. In the long run, the campaign is devoted to developing an individual telecommunication ethics index for measurement.

The United Kingdom launched IT Safe, a new programme mainly aimed at network security, but also dealing with spam. The programme aims at providing warnings about damaging viruses, software vulnerabilities and weaknesses on devices such as mobile phones. Alerts will inform people how the threats affect them and what they can do to avoid protect themselves. The service will be free and those who sign up can get e-mail or text alerts. The scheme is aimed at home users and small businesses.

In Canada, the Fraud Prevention Forum launched in February 2005 a month-long campaign titled Fraud Awareness Month to educate Canadians on how to protect themselves against fraud. More than 40 private and public sector organisations participated to this initiative and contributed in reaching out to Canadians.

3.3 Industry cooperation and educational initiatives

21. Co-operation among different organisations is a must in order to deliver a consistent, well-informed message to a target audience. Industry co-operation is one example. Different parties in an industry sector can develop a programme of self-regulation among members and may develop a programme which can be used to educate their customers on how to fight against spam.

22. Internet Service Providers (ISPs) at the national level, and even at the international level, could develop codes of conduct to deal with spam. ISPs need to cover their clients who send outgoing e-mail in such codes of conduct. In this context the sharing, and adoption, of best-practice acceptable use policies by customers plays an important role.

23. In addition, ISPs can play a role in educating their customers who are recipients of spam and teach them the basics of good Internet practice. As an example, in Japan, six mobile operators and the Ministry of Internal Affairs and Communications established the “Working Group against Spam” and, in Korea eight major ISPs and ESPs, the Ministry of Information and Communications, and the Korea Information Security Agency (KISA) co-developed a “Best Practices Guideline” for ISPs and ESPs.

24. Many Direct Marketing Associations across Europe, North America, and Australia have implemented Codes of Conduct for members to follow. These have been put into place to ensure that their members comply with marketing legislations and to prevent direct marketers from becoming spammers unwittingly.

25. Some positive synergies have also developed as a result of networking among different organisations. For example, SAFT (mentioned above) established national professional networks where governments, NGOs, research and industry stake holders meet and share information and experiences. CAUCE (Coalition Against Unsolicited Commercial Email) is an all volunteer advocate group for responsible Internet commerce; it has spread across different regions and includes a range of professionals and others concerned with creating a safer Internet and reducing spam.
26. Phishing has been identified as a growing problem area resulting in high financial losses to industry as well as individuals. In this context the Anti-Phishing Working Group (APWG), an industry association of software producers, service providers, and online operators, has been created to address the problem of identity theft and fraud, providing updated information on ongoing phishing attacks, and sharing best practices on how to eliminate or limit this phenomenon. The web site of the Anti-Phishing Working Group is www.antiphishing.org and it serves as a public and industry resource for information about the problem of phishing and e-mail fraud, including identification and promotion of pragmatic technical solutions for protection against phishing attacks.

3.4 Websites

27. What better place to launch a war against spam than websites? Many organisations have come forth with innovative and proactive ways to fight against spam online as well.

28. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organisation. Its programs are aimed mainly at security professionals, but also provide information for businesses on spam, phishing and other on-line vulnerabilities. SANS develops, maintains, and makes available at no cost, a large collection of research documents about various aspects of information security, and it operates the Internet's early warning system – Internet Storm Centre. Its web site is at: http://www.sans.org.

29. The Canadian government has formed a Task Force on Spam, and the Task Force has initiated an Internet-based education and awareness campaign through a “Stop Spam Here (Arretez le pourriel ici)” icon that has been posted on all the web sites of major ISPs and leading information service providers. This icon provides a link to a website providing tips for consumers and small business that highlight steps they can take to limit and control the volume of spam in their in-boxes as well as how they can protect themselves from the more dangerous elements associated with spam. The value of this initiative is that it provides both a consistent message and broad dissemination. Up to March 31, 2005, the website had over 500,000 visits and nearly 4,000,000 hits from 148 countries.

30. The SpamCon Federation in the United States is a non-profit agency that has created banners, text, and buttons with links to its web site and these resources are available for any internet user to use in their e-mail and websites. It has also invited users to help create banners and texts that may be posted and used by others.

31. The Korea Information Security Agency (KISA) provides free online software that allows users to protect themselves from spam. The following software is made available:

- Alert Program that monitors any malicious events on the network and alerts individuals in real-time with instructions and information.
- SpamCop: software that enables users, once downloaded, to easily report spam mails.
- NeverSpam: software that allows users to iconize their e-mail address.

32. The organisation also provides free online spam relay tests for ISPs. It identifies online if servers of a requesting ISP may be used as a spam relay, and if so, instructs it on how to protect and secure the server.

33. The Federal Trade Commission (FTC) in the US has educational material on its web site for consumers and for businesses. Examples of web pages devoted to spam, spyware, and security issues
include www.ftc.gov/infosecurity and www.ftc.gov/spam. In addition, in conjunction with 35 agencies from 20 countries, the FTC has launched a programme called “Operation Spam Zombies” aimed at educating ISPs and network operators on how they can help to reduce the problem of hijacked home computers being used to send spam. Now the FTC is taking a broader look at its education materials and tactics related to cybersecurity, online privacy, and Internet fraud, and updating its messages and outreach strategies to better educate computer users about these important issues. In the fall of 2005, the FTC will unveil a new website at OnGuardOnline.gov with general information about online safety, as well as modules with specific information on such topics as phishing, spyware, zombie drones, and P2P file-sharing. The FTC will add to the site as new topics arise. Each module will include the most current information, as well as interactive features, such as videos and quizzes. The FTC is coordinating with public and private sector partners to include additional content appropriate for the site.

34. The web site of PC World has a section on spam, called Spam Watch\(^{12}\), providing news, tips, and tools on junk e-mail. A surfer may get updates on spam while she/he surfs through the site for news. One section, devoted to spam, emphasises the importance of the issue while providing detailed information.

4. Education on Spam

4.1 Targeting Student, Children, and Parents

35. Students and children are the so called “online generation”, \textit{i.e.} those who have grown up with the Internet. They often have multiple net identities and spend a lot of time on online. It is therefore very important for them to learn the dangers of the Internet, acquire the capability to distinguish good content from illegal content, and act accordingly. For these reasons it is extremely important to develop appropriate programmes and material targeting younger users, and teaching them how to safely explore the Internet, protect their privacy, secure their terminals and overall enjoy the benefits of new ICTs... Consequently it seems that schools would be well placed to provide educational tools to children, so that the concept of online security and privacy will be assimilated as an integrating part of Internet surfing or e-mail utilization. However, public institutions are often not providing enough information and do not always have the resources to create such information. Therefore, teachers, parents, and students may have to rely on educational material created by the private sector, governments or non-profit organisations.

36. In Japan, the Ministry of Economy, Trade, and Industry (METI) had distributed educational material on mobile spam, in the form of videos and brochures, to 50% of high schools and college students by September 2004. The material for high school students used cartoons to describe situations students may find themselves in, and provide them with examples of actions they could take.

37. In France, the CNIL\(^{13}\) has “Espace Juniors (Junior Space)” for children where information is displayed in simple words, and games and quizzes are provided to provide lessons on internet security. It also provides e-cards with CNIL cartoon characters and links to the website so that children may send cards to friends to learn about the site.

38. The National Research Council of the National Academies of United States produced the NetSafeKids website\(^{14}\), providing essential information and practical tips that help parents and adults make more informative decisions on how children may spend time online. The FTC also has a web page devoted to children’s privacy issues. It can be found at www.ftc.gov/kidzprivacy.

39. “In Germany, the Federal Government in cooperation with partners from industry launched the campaign “Look ! What your kids do !” (“Schau hin ! Was Deine Kinder machen”)\(^{http://www.schau-hin.info}\). The campaign submits suggestions and services for parents and teachers to improve their
education-responsibility in handling modern electronic media. Moreover the “Federal Department for Media Harmful to Young Persons” (Bundesprüfstelle für jugendgefährdende Medien) http://bundespruefstelle.de/bpjim/bpjim/generalinf.php, the agency: “jugendschutz.net” http://www.jugendschutz.net and the German awareness node “klicksafe.de” http://www.klicksafe.de/common/english.php provide interested parties with information and useful recommendations concerning the use of the internet by children.”

40. The National Research Council of the National Academies of United States produced the NetSafeKids website\(^\text{15}\), providing essential information and practical tips that help parents and adults make more informative decisions on how children may spend time online.

41. SAFT has created a comprehensive education program for 8-12 year olds and their parents and teachers. This module-based interactive education program comes with both classroom and home activities and a teacher’s guide. The education materials are sent out to all schools in CD-ROM format, and are also available online. The material includes information, games, quizzes, workshops, activities and much more. At the moment, SAFT is continually expanding with new modules, and is currently working on a spam module. Some of the existing modules include:

- “Learn to surf”
- Source criticism
- Safety-quiz
- Mailbox: children receive a SAFT diploma and answer safety questions from other children
- Commercial gaming and privacy in interactive computer game format

SAFT has also designed a programme for junior high school on privacy rights.

42. The University of Calgary is offering students a course in writing spyware and the tools for sending and propagating spam. The logic behind this is that ‘the right skills taught in a controlled environment will prove a useful addition to security industry’. On the other hand, some are concerned that the ‘saleability of spam tools may create a financial temptation’ for some students.

4.2 Targeting Individuals

43. Just relying on increased awareness and expecting that individuals will search for information on spam on their own is not likely to get sufficient results. It is difficult and costly to try and target and educate individuals. It is much simpler to target groups of individuals. For example, one can target company employees and require mandatory Internet security courses for employees. Once they are trained to protect themselves online, they will take the knowledge and implement it at home. Another example would be to include Internet security sessions in Internet courses for senior citizens who learn computing. Learning e-mail security while learning to e-mail; can ensure that the habit of security will come naturally and easily.

44. A comprehensive and thorough website with information explaining what spam is, how to avoid it, how to complain, etc., along with perhaps several sample tests to check individual’s level of knowledge on spam, phishing, and internet security should also be made available. As the intermediary of e-mail communication, ISPs and ESPs can make such information available to their customers readily and
efficiently. Such information should be obvious when an individual first signs up for service, and should be always easily accessible.

45. Many ISPs and ESPs do provide information on spam, and also provide anti-spam protection for members. Anti-spam and anti-virus filters are often included in enhanced (paying) service packages, or provided for a fee. It is worth noting that all ISPs in New Zealand provide anti-spam technology for free. However, there are still too many providers that do not include any information on spam on their home page, or do not display it on their home page where it would be most visible.

4.3 Targeting ISPs/ESPs

46. More ISPs and ESPs have come to realize that they can play major role to stop spam. Several national ISP Associations have drafted Codes of Conduct which all members are encouraged to implement. These codes include usually provisions regarding the prohibition to send spam e-mails, viruses or illegal content. This form of self-regulation is reflected in ISP Acceptable Use Policies. Some examples of ISPs associations which have developed a code of conduct would be EuroISPA, US ISPA, CAIP (Canada), and IIA (Australia).

47. The RIPE (Réseaux IP Européens) Anti-Spam Working Group aims to tackle the spam problem from a non-technical perspective. The Working Group is developing a Code of Conduct which ISPs may adopt. It is also making recommendation as to the feasibility and usefulness of a “Centre for European Network Abuse Resolution (CENAR)”. This centre would aim to provide a conflict resolution procedure if ISPs are unable to resolve issues regarding abuse complaints bilaterally.

48. The “Operation Spam Zombies” project mentioned in paragraph 28 is another example of an international effort to educate ISPs on the problem of hijacked home computers being used to send spam.

4.4 Targeting Business Entities, especially SMEs

49. Small and Medium Enterprises (SMEs) are much more exposed to the danger of spam compared to large enterprises because many SMEs are unable to afford dedicated network administrators or invest heavily in network security. For example, most Australian SMEs are now online (86%) (Sensis eBusiness Report, July 2004). Over half are on broadband or intend to do so soon and 82% receive spam, while 69% report that spam is a problem for them. Major issues are productivity based; 39% say they are concerned about related virus threats, yet over one in four reporting a major spam problem admits to having done nothing about it.

50. The entities in best position to help the SMEs would be the ISPs or the security software/product companies by providing solutions at a discount. KT, the largest internet service provider in Korea, provides a relatively cheap anti-spam and anti-virus solution for SMEs.

4.5 Targeting Direct Marketers

51. Direct marketers can be both a victim of spam, as well as become spammers themselves. They may be the victim when their marketing efforts are regarded as being spam, and may not reach their customers. They also become the victims of spam when recipients of their e-mail delete it automatically because they are inundated with commercial e-mail, most of which is spam. On the other hand, they may become spammers when they do not abide by anti-spam national laws and regulations. While it can be difficult to adhere to domestic legislation, it may be more difficult for a company to comply with foreign laws, in case their messages are directed to users in other countries (provided that they know the user is situated in another country, which is not always easy to ascertain when generic top level domains, such as .com and .net, are used).
52. Providing education and awareness-raising material to direct marketers can enable direct marketers to:

   i) Sharpen their skills in marketing and differentiate themselves from spam.
   
   ii) Better target customers who are interested in receiving information on their products.
   
   iii) Avoid the pitfall of becoming a spammer.

53. Direct marketing associations share information and tools on spam for their members. Many have also developed Codes of Conduct on e-mail marketing (see Annex). The Interactive Advertising Bureau, a trade association for internet advertising in the UK, has launched a project to develop guidelines for consumers, materials for employers and managers to educate their employees and staff, and review e-mail marketing codes developed in the past.

5. Anti-spam tricks and tips: What needs to be communicated to Internet users?

54. Different countries have different laws, and different advice may be given in these countries. However, Internet is a common resource where no distinct national boundaries exist, so the basic information that needs to be communicated to users should be the same, although cultural and language differences may require slight modifications to adapt to these differences. Through awareness raising and education, the following message needs to be sent out to all internet users.

What is spam, and what are the dangers?

55. One of the major findings of the “Spam Box” experiment by CNIL was that, people had different definitions for spam. For example, there were some who were more sensitive to the problem and would consider e-mails from acquaintances as spam if it was of no relevance or interest, whereas some people would only consider e-mails which were linked with a scam or with pornography as spam.

56. Perhaps when describing the dangers of spam, they can be categorized into different types and in particular highlighting spam that includes fraud, pornography, viruses and Trojan programmes and is aimed at identity theft\(^{16}\). Additional or separate information on how to handle each danger should also be provided.

How to avoid spam

57. The best advice to users to avoid spam is not to post e-mail address on websites. If it is absolutely necessary to post it, it is advised

   i) to mask e-mail addresses by posting in html script and CGI, or graphic image, or ASCII or JavaScript encoding, or PERL script, and/or
   
   ii) To use multiple disposable e-mail addresses from free web mail providers.

58. As with all information, it is important to update regularly solutions as technology evolves. For example, “munging\(^{17}\)”, the e-mail address, \(i.e.\) type it in a manner that could easily be recognized by a human, but not by a robot, is one of the current methods for masking an address. However, spammers may easily implement coding to detect e-mail addresses from “munged” ones if the practice becomes more common. Once “munging” is not effective any more, it should be readily substituted by other practices and recommendations.
How to react and to file complaints when one receives spam

59. In opt-in countries, one is advised to simply delete spam, or forward to concerned parties to file a complaint. In opt-out countries such as Korea, it is advised to opt-out first, and if the sender is persistent, then file a complaint with the mail requesting opt-out as proof.

60. Legislative bodies or ISP/ESP complaint centres should be informed, with detailed explanations and procedures to file complaints.

What preventive measures may be taken?

61. A list of available spam filters (free and paying) should be provided to users, together with useful anti-spyware software and virus protection. A link to easy and comprehensible guidelines to internet security should be included in all ISPs websites.

Where to find more information

62. Provide links to other anti-spam websites. Once an internet user takes interest in the subject, the person will be willing to hunt for further information. Make it easy for them. Guide people to take action right away.
ANNEX I. AWARENESS AND EDUCATION ACTIVITIES IN OECD MEMBER COUNTRIES

Australia

1. One in four Australians has no current anti-virus protection (Symantec, 2004). Due to early actions of the Australian government and non-profit organisations toward spam, this number is higher than most other countries, but there is plenty of room for improvement.

2. Government bodies have provided much information including the electronic commerce guidelines for business, “Building Consumer Sovereignty in Electronic Commerce (A Best Practice Model for Business)”. It provides additional guidelines to be used by businesses and organisations developing industry codes. The guidelines are designed to promote practices that increase consumer confidence in online transactions.

3. Industry codes, including those of the Internet Industry Association and the Australian Direct Marketing Association, also provide rules relevant to marketing by electronic mail. The Internet Industry Association is the national, non-profit, industry organisation representing internet businesses in Australia. It has launched the IIA National Spam Initiative aiming to empower all Australians on the internet, from corporate employees to home users, to better control their usage of internet. It has created a code of practice for internet and email service providers. The Australian Direct Marketing Association has created a code of practice among the members of the association when marketing in email.

4. Many non-profit organisations are fighting spam, including CAUBE (Coalition Against Unsolicited Bulk Email) and NetAlert. NetAlert is Australia’s Internet safety advisory body, a not-for-profit community organisation providing free practical Internet safety advice, information and resources to Australian families and community.

Belgium

5. Federal Public Service Economy GD Market Regulation & Organisation distributes “Le spamming en 24 questions et réponses” brochures to a wide range of audiences. The main objective is to explain spam and applicable spamming regulations in simple words. The brochure uses question & answer formats to increase understanding.

6. The Secretary of State for the Computerization of the State provides consumers with a check list of minimum safety guarantees to consider when buying a PC or software. The check list is distributed through web pages, workshops and seminars, newspapers, radio, and TV. A consumer may try and comply with the check list by requesting products that meet up to the security and safety requirements on the check list. A current Belgian draft law requests both the internet service providers and the software providers to take any necessary measures to guarantee web safety and offer to their customers effective security services in order to prevent all forms of undesired electronic communication.
7. The Secretary of State for the Computerization of the State also has developed a comic strip, Suske & Wiske, to raise awareness of the dangers of the digital world. The comic focuses on the dangers and risks of the digital world from viruses, hackers, spyware, and phishing and provides practical advice.

8. The Federal Public Service Economy informs users and designers of internet sites on existing information society rules through its guide. The guide aims at providing practical advice and rights and responsibilities for both the internet users and site designers. The guide was distributed at roadshows in year 2001 and updated versions are still distributed at fairs and exhibitions.

Canada

9. The government of Canada had a Task Force on Spam to develop recommendations against spam. The Task Force launched an internet-based communications campaign, including a common logo and web site, to raise public awareness on steps that users can take to limit and control the volume of spam they receive. Also as an effort of the Task Force, Canadian internet service providers and other network operators agreed in December 2004 to block e-mail file attachments with specific extensions known to carry infections, or filter e-mail file attachments based on content properties. Such industry-wide practices of this kind were a world first.

Czech Republic

10. The Consumer Defence Association of the Czech Republic has run several interviews in the media on issues such as spam and phishing, as well as releasing sample complaint letters for consumers and providing information on spam issues.

Finland

11. Finland held a National Data Security Day to enhance awareness on computer security basics targeting especially the home users, the small and home offices, children and students, with broad media coverage from daily newspapers to TV and internet. Advertisement, information, and also security guide have been sent out through the media.

France

12. CNIL, the Commission Nationale de l’Informatique et des Libertés – the organisation which ran a three-month campaign of “Spam Box”, provides easy-to-understand information on spam and Internet security on their website. It also has a “Vos Traces (Your Traces)” section where one can learn how personal information may be traced and used for abuser’s advantage. This section explains in details and demonstrates the process. It is a useful tool for raising awareness on security.

Germany

13. The Federal Ministry of Economics and Labour published one issue of its magazine ef@cts, which exclusively deals with Spam and gives information to SME’s, Direct Marketers and end users. The magazine is published online in German and English together with other useful information about Spam on the Ministry’s homepage: http://www.bmwa.bund.de/Navigation/Technologie-und-Energie/Informationsgesellschaft/spam.html. A survey of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) describes successful anti-spam strategies: www.bsi.bund.de/literat/studien/antispam/. Both the Center for Protection Against Unfair Competition and the Consumer Organisations provide comprehensive material on how to protect yourself against spam. Eco (Association of the German Internet Industry) is running the “Anti-Spam-Task-Force”. On its Website http://www.eco.de (see: “Initiative: Anti-Spam”) it provides information for end users and a Whitepaper
for ISP’s on how to deal with spam and some rules for Direct Marketers for responsible online-marketing.  
http://www.eco.de/servlet/PB/show/1466257/Whitepaper_Kurzfassung_eng_100.pdf

Greece


Ireland

15. The Office of Data Protection Commissioner provides guidance material on data protection to inform individuals on spam and how to make a complaint at www.dataprivacy.ie/images/Spamguide.pdf.

Italy

16. The Centro Europeo Consumatori, on their website www.euroconsumatori.org/16842v16921d17289.html, has provided information to consumers on spam and what they can do to fight against spam.

Japan

17. Japan has a high rate of access to the Internet using mobile communications and, as a result, mobile spam has surpassed e-mail spam by 9:1 (Survey by Japan Computer Communications Association, 2003 fiscal year). In November 2003, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (now Ministry of Internal Affairs and Communications) and six mobile operators formed a Working Group against spam in order to promote self-regulation in the sector. Spam sent to mobile telephones is more difficult to disguise than e-mail spam so such self-regulation has worked relatively well for spam sent from mobile telephones to mobile telephones. However, it is much easier to send anonymous spam from PCs to mobile telephones so the mobile operators need to adopt appropriate technical solutions to deal with such spam.

18. The Ministry of Economy, Trade, and Industry (METI) has distributed educational materials such as video and brochures for high school and college students on spam.

Korea

19. The Korean Ministry of Information and Communication (MIC) and the Korea Information Security Agency (KISA), along with 8 major e-mail service providers, have published a Guide to Best Practices for Blocking Spam targeting internet and e-mail service providers and network operators.

20. KISA has also dedicated a designated month each year for anti-spam campaign. Also on its website, KISA has provided online spam alert software, e-mail address iconizing software (NeverSpam), and easy e-mail complaint software (SpamCop) at no charge for internet users. For ISPs and SMEs, KISA provides free online open relay test services followed by security advice and guidance.

21. ISPs and ESPs have adopted many different technologies and best practices of their own. Some accept subscribers only when they have been verified through their social security numbers, thereby discouraging any subscribers to disguise their identity. Some filter out spam e-mails into a spam e-mail box and allow users to verify whether the e-mail is spam. Some ISPs allow you to create a list of contacts and then differentiate mail sent from the contacts from other mails. All ISPs provide detailed information on spam and internet security, and provide complaint centres for users.
Mexico

22. The International Consumer Protection and Enforcement Network (ICPEN) and Procuraduría Federal del Consumidor (Office of the Federal Attorney for Consumer Protection, Profeco) launched the Fraud Awareness Month Campaign (FAMC) in February 2005. The campaign aimed to provide consumers with the necessary knowledge and skills to recognise, report, and stamp out scams and spam. Profeco published a website with a brief introduction of the efforts carried out by ICPEN for combating deceptive, abusive, and misleading commercial practices on the Internet, examples of scams and recommendations on how to prevent them, and the OECD guidelines for protecting consumers from fraudulent and deceptive commercial practices across borders. Around 98,000 visited the site during the campaign month.

23. During the last months, Profeco has taken several steps in order to increase consumers awareness related to the spam phenomenon. The activities have been developed in the international as well as in the domestic arena:

**Domestic actions**

- Profeco has taken concrete measures in trying to raise awareness among Mexican consumers on how to react to spam. Recently, this institution published a new section within it’s institutional website related to Spam. Please visit: [http://www.profeco.gob.mx/html/ecomercio/spam/spam.htm](http://www.profeco.gob.mx/html/ecomercio/spam/spam.htm). The section is intended to inform consumers what is spam, the risks and problems caused by spam, as well as to communicate Mexican cyber consumers what type of actions Profeco is carrying out in order to deter spam (international as well as domestic ones).

- Profeco will publish an article explaining the spam phenomenon and its consequences in its monthly Consumer Magazine. This Office has foreseen that the article will be presented at the magazine of October 2005. Please take note that the Magazine has 80,000 copies by month.

- Likewise, Profeco participated in two important Seminars in Mexico City: i) "The Spam and its impact” co-sponsored by the Federal Telecommunications Commission (Cofetel, by its initials in Spanish language) and the University “La Salle”, held on March, 2005, and ii) "Spam and Solution perspectives” organized by the Communications Commission of the House of Representatives of the Mexican Congress, held on June, 2005. During the Seminars the academic sector, private sector and the governmental sector discussed the spam phenomenon.

**International activities**

- In February 2005, the Procuraduría Federal del Consumidor (Office of the Federal Attorney for Consumer Protection, Profeco) of Mexico participated in the international Fraud Awareness Month Campaign (FAMC) launched by the International Consumer Protection and Enforcement Network (ICPEN). The campaign aimed to provide consumers with the necessary knowledge and skills to recognize, report and stamp out scams and spam. Profeco published a website with a brief introduction of the efforts carried out by ICPEN for combating deceptive, abusive and misleading commercial practices on the Internet, examples of scams and recommendations on how to prevent them, and the OECD guidelines for protecting consumers from fraudulent and deceptive commercial practices across borders.
The material developed can be visited at:
http://www.profeco.gob.mx/html/ecomercio/spam/a_int_spam.htm

Private sector activities

- Members associated to the Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A.C. (Mexican Association on the Internet’ Advertisement and Commercial Industry) are due to abide the AMIPCI’s Ethic Code published in October 2000. Article 24 of the above mentioned code establishes that “…. In an effort to guarantee the appropriate use of the electronic mail for advertising purposes, AMIPCI will establish as a minimum standard the possibility that the user will make the decision if he would like or not to continue receiving this sort of e-mails”.

- The Mexican private sector is also concerned about the spam problem. Microsoft Mexico is doing efforts to raise awareness and educate clients about the spam problem. Microsoft Mexico does not yet have a formal program in place. However, they are taking every opportunity available to inform government officials, consumers, etc. about this matter. They participate in press interviews, in workshops and seminars and are including spam-related articles in their bi-monthly newsletter “ALCANCE”, distributed to 1,500 key officers from government, private sector and academia, throughout Latin America.

- T1msn Mexico (a main commercial web site) has a continuous campaign on their network of internet sites and services to raise the level of awareness among their users on how to better use the tools they make available to them to combat Spam. This includes content and articles on how to detect Spam and other malicious mail and information, and how to set Hotmail’s spam filters to identify and block it before it reaches a user’s inbox. Parallel to these online efforts, they take advantage of any opportunity available in seminars and workshops to give information about spam and how to combat it. They also have a content channel dedicated to safe computing available at: www.t1msn.com.mx/seguridad/ in addition to continuously publishing articles about spam, i.e. : www.t1msn.com.mx/tecnologia/seguridad/peligro/ It is important to highlight that it is an ongoing program and there is continuously monitoring of the levels of spam circulating through Hotmail servers with the help of MSN.

Netherlands

24. Consumentenbond (the largest consumer organisation in the Netherlands) has sent out a brochure on spam “Spam, what to do against unsolicited e-mail” from the national government with its monthly journal to all members of the organisation. It also plans on distributing more brochures on the issue. It has also used many different media (pen, chewing gum, games, etc.) to provide consumers with a basic understanding of the rules and on consumers’ rights under these rules, practical information on acceptable marketing practices under the opt-in regime, how to avoid spam, and products and services available to avoid spam.

New Zealand

25. A non-profit internet group, InternetNZ, created an Anti-Spam Task Force, and included the Direct Marketing Association as a member. It encourages all ISPs to refer its customers to its website http://www.internetnz.net.nz to discuss anti-spam activities.
26. The Ministry of Education has also set up a website [http://www.netsafe.org.nz](http://www.netsafe.org.nz) with information on Internet safety for children, schools, parents, adults, businesses, counsellors, and community groups. The website also includes Net Safe Kit for schools.

Norway

27. The Norwegian Post and Telecommunication Authority implemented “the Action Plan on Spam” for consumers and SMEs on April 26th, 2005. Website [www.nettvett.no](http://www.nettvett.no) will be opened by the Ministry of Transport and Communications on April 26th, the National IT Security Day.

28. SAFT in Norway is very active in its role of educating children the Internet safety and spam. It broadcasts advertisement and works with schools and parents to proactively educate children on Internet. It focuses on reducing ‘risk’ behaviour of children on the Internet and to teach them to be responsible Internet users.

Spain

29. The Spanish Association of Internet Users (AUI) has launched a campaign against UCE which includes education and working with companies to promote ethical practices relating to commercial e-mail. The AUI stated that it intended to campaign for spam to be treated the same as the massive distribution of commercial faxes. Its website [http://www.aui.es](http://www.aui.es) (in Spanish only) includes material on issues ranging from a description of the problem and a range of measures both legislative and technical for dealing with it.

Sweden

30. The Swedish National Post and Telecom Agency provides a website [www.pts.se/internetsakerhet](http://www.pts.se/internetsakerhet) targeting home users (for hemmet) and workplace (for arbetsplatsen). The home users can find information under the following menu: about the Internet, Connection, Surfing, E-mail, Download, Divide files, Chat, Network games, Implement bank matters and e-commerce, Fifteen good tips, Learn interactively, Common questions, Common terms and Links. The workplace users can find information under the following menu: Prepare policy, Rules for infrastructure, Connect to the Internet, Configure systems, Create safety copies, Connect at a distance, Connect business partners, Protecting against harmful codes, Managing IT incidents, E-identification and transactions, Buy security services, Good tips for the workplace and Links.

31. The site has been evaluated by Web Service Award ([http://www.webserviceaward.com/en/index.asp](http://www.webserviceaward.com/en/index.asp)), the largest website survey in Sweden. It has been provided that the web service index for the website is 66, higher than 57, the average of all sites participating in the survey.

32. The Swedish Consumer Agency/Consumer Ombudsman provides information to consumers at [www.konsumentverket.se](http://www.konsumentverket.se). In 2004, seven to eight million visited the website and twenty thousand filed complaints against unsolicited e-mail marketing.

Switzerland

33. The State Secretariat for Economic Affairs (SECO) distributes “Attention Trap” brochures to consumers to provide an alert against fraud activities at: [http://www.seco.admin.ch/imperia/md/content/spezialthemen/wettbewerb/seco_prospekt_internet_d_a51.pdf](http://www.seco.admin.ch/imperia/md/content/spezialthemen/wettbewerb/seco_prospekt_internet_d_a51.pdf) (German).
34. OFCOM Switzerland, the telecommunication regulator, implemented the SPAM-SPAMMING-SPAMMER programme on March 29th, 2005. The programme informs consumers through fact sheets at http://www.bakom.ch/en/service/tc/spam/index.html.

United Kingdom

35. The UK government launched an IT Safe programme, a virus alert service, in February 2005. The service allows home users and small businesses to sign up and receive virus alerts by either text or e-mail. The service is funded by the Home Office and uses information provided by the National Infrastructure Security Co-ordination Centre (NISCC) – the government’s centre for electronic defence.

United States

36. The Federal Trade Commission (FTC) website www.ftc.gov provides a wide and in-depth range of information on spam and other Internet security matters. During the last decade, the FTC has conducted high-profile education and awareness-raising campaigns on such topics as recognizing scams on the Internet, shopping securely online, avoiding hackers and viruses, and dealing with spam, spyware, phishing and ID theft, and peer-to-peer file-sharing. Now the FTC is taking a broader look at its education materials and tactics related to cybersecurity, online privacy, and Internet fraud, and updating its messages and outreach strategies to better educate computer users about these important issues.

37. In the fall of 2005, the FTC will unveil a new website at OnGuardOnline.gov with general information about online safety, as well as modules with specific information on such topics as phishing, spyware, zombie drones, and P2P file-sharing. The FTC will add to the site as new topics arise. Each module will include the most current information, as well as interactive features, such as videos and quizzes. The FTC is coordinating with public and private sector partners to include additional content appropriate for the site.

38. The Federal Trade Commission (FTC) website www.ftc.gov provides a wide and in-depth range of information on spam and other Internet security matters.

39. The US has many non-profit organisations working on spam issues. The Anti-Spam Technology Alliance (ASTA) is one example that has developed and published recommended best practices that promote network management practices against spam. CAUCE (Coalition Against Unsolicited Commercial Email) is another organisation that works to fight against spam and also cooperates with CAUCE from other regions such as EU, APEC, Canada, and Australia. SpamCon Foundation provides banners, buttons, and texts that link back to SpamCon website to be promoted on users’ sites and emails.

40. Sponsored by Star ATM and Debit Network, National Consumers League (NCL) has launched a stand-alone website, www.phishinginfo.org, as a central resource on phishing. It explains how phishing works, how to protect against phishing, and what to do if people become victims. The website also provides downloadable materials such as tips, brochures, and ready-to-use news articles. To raise awareness and drive people to the site, NCL created television, radio, and print public service announcements. The campaign was launched with a press release, a two-hour radio media tour in which experts from NCL and Star participated, and announcements in NCL’s newsletters.
## ANNEX II. SPAM MATRIX

<table>
<thead>
<tr>
<th>Government</th>
<th>NGOs</th>
<th>Private Sectors (ISPs, ESPs, Direct Marketers, companies)</th>
<th>2. ISP Security Measures and protection provided</th>
<th>3. Code of Practice among Direct Marketers?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td></td>
<td>Australian Direct Marketing Association (<a href="http://www.adma.com.au">www.adma.com.au</a>)</td>
<td>Optus (spam filter)</td>
<td>Yes (Code of Practice; ADMA)</td>
</tr>
<tr>
<td></td>
<td>- Australian Communications Authority</td>
<td>- Internet Industry Association (<a href="http://www.ia.net.au/nospam">www.ia.net.au/nospam</a>)</td>
<td>- Optus (spam filter)</td>
<td>- AOL (spam filter, parental control)</td>
</tr>
<tr>
<td></td>
<td>(<a href="http://internet.aca.gov.au">http://internet.aca.gov.au</a>)</td>
<td>- CAUBE (<a href="http://www.caube.org.au">www.caube.org.au</a>)</td>
<td>- Optus (spam filter)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Dept. of Communications, Information Technology and the Arts (<a href="http://www.dcita.gov.au/ie/spam_home">www.dcita.gov.au/ie/spam_home</a>)</td>
<td>- NetAlert for parents (<a href="http://www.netalert.net.au">www.netalert.net.au</a>)</td>
<td>- Optus (spam filter)</td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td></td>
<td>- ISPA (Internet Service Providers Austria) (<a href="http://www.ispa.at">www.ispa.at</a>)</td>
<td>(Direct Marketing Verband Österreich)</td>
<td>(Self-regulation Code; Belgian Direct Marketing Association)</td>
</tr>
<tr>
<td></td>
<td>- Austrian Data Protection Commission (<a href="http://www.dsk.gv.at">www.dsk.gv.at</a>)</td>
<td>- Österreichisches Institut für angewandte Telekommunikation (OIT; Austrian Institute for Applied Telecommunications) (<a href="http://www.oit.at">www.oit.at</a>)</td>
<td>(Direct Marketing Verband Österreich)</td>
<td>(Self-regulation Code; Belgian Direct Marketing Association)</td>
</tr>
<tr>
<td>Belgium</td>
<td></td>
<td>- ISOC Belgium (<a href="http://www.isoc.be">www.isoc.be</a>)</td>
<td>Yes</td>
<td>(Self-regulation Code; Belgian Direct Marketing Association)</td>
</tr>
<tr>
<td></td>
<td>- Spam Pagina (<a href="http://www.spam.pagina.be">www.spam.pagina.be</a>)</td>
<td>- ISOC Belgium (<a href="http://www.isoc.be">www.isoc.be</a>)</td>
<td>Yes</td>
<td>(Self-regulation Code; Belgian Direct Marketing Association)</td>
</tr>
<tr>
<td>Canada</td>
<td></td>
<td>- CAUCE Canada (<a href="http://www.cauce.ca">www.cauce.ca</a>)</td>
<td>Canadian Marketing Association (<a href="http://www.the-cma.org">www.the-cma.org</a>)</td>
<td>Bell Sympatico (3 months trial)</td>
</tr>
<tr>
<td></td>
<td>- Industry Canada (<a href="http://www.ic.gc.ca">www.ic.gc.ca</a>)</td>
<td>- CAUCE Canada (<a href="http://www.cauce.ca">www.cauce.ca</a>)</td>
<td>- Bell Sympatico (3 months trial)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Spam Task Force (<a href="http://www.stopspamhere.ca">www.stopspamhere.ca</a>)</td>
<td>- Canadian Marketing Association (<a href="http://www.the-cma.org">www.the-cma.org</a>)</td>
<td>- Bell Sympatico (3 months trial)</td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>- Consumer Defense Association (<a href="http://www.consumers.cz">www.consumers.cz</a>)</td>
<td>- Bell Sympatico (3 months trial)</td>
<td>(Code of Practice; ADMA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Anti Spam (<a href="http://www.antispm.cz/iso-8859-2/info/1/index.htm">http://www.antispm.cz/iso-8859-2/info/1/index.htm</a>)</td>
<td>- Shaw (Shaw Secure)</td>
<td>(Code of Practice; ADMA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Safer Internet (<a href="http://www.saferinternet.cz">www.saferinternet.cz</a>)</td>
<td>- Telus (Spam Control)</td>
<td>(Code of Practice; ADMA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rogers (McAfee Privacy for Rogers Yahoo! High speed only)</td>
<td>(Code of Practice; ADMA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Cogeco (security for Standard and Pro users only)</td>
<td>(Code of Practice; ADMA)</td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td>NGOs</td>
<td>Private Sectors (ISPs, ESPs, Direct Marketers, companies)</td>
<td>2. ISP Security Measures and protection provided</td>
<td>3. Code of Practice among Direct Marketers?</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>----------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td><strong>Denmark</strong></td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
</tr>
<tr>
<td><strong>Finland</strong></td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
</tr>
<tr>
<td><strong>France</strong></td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
</tr>
<tr>
<td><strong>Germany</strong></td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
<td>![image]</td>
</tr>
</tbody>
</table>
### 1. Active group in spam awareness

<table>
<thead>
<tr>
<th>Government</th>
<th>NGOs</th>
<th>Private Sectors (ISPs, ESPs, Direct Marketers, companies)</th>
<th>2. ISP Security Measures and protection provided</th>
<th>3. Code of Practice among Direct Marketers?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greece</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iceland</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Data Protection Commissioner (<a href="http://www.dataprivacy.ie">www.dataprivacy.ie</a>)</td>
<td>- SAFT Ireland (<a href="http://www.saft.ie">www.saft.ie</a>)</td>
<td>- Irish Internet Association (<a href="http://www.ilia.ie">www.ilia.ie</a>)</td>
<td>- eircom net (email protector service on trial) - Blacknight Internet Solutions Ltd (spam filter, virus filter) - HEA.net Ltd (local copy of MAPS RBL+ real-time blacklist) - Protocol Internet-Hosting Ireland (&quot;spamburn&quot; anti-spam product)</td>
<td>Yes (Code of Practice; Irish Direct Marketing Association Ltd)</td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td></td>
<td></td>
<td></td>
<td>(AIDIM)</td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td></td>
<td></td>
<td>Yes (Code of Ethics; Japan Direct Marketing Association)</td>
</tr>
<tr>
<td>Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ministry of Information and Communications (<a href="http://www.mic.go.kr">www.mic.go.kr</a>) - Korea Internet Security Centre (<a href="http://www.kicerti.or.kr">www.kicerti.or.kr</a>) - Korea Spam Response Centre (<a href="http://www.spamcop.or.kr">www.spamcop.or.kr</a>) - Information Communications Ethics Committee (<a href="http://www.ieec.or.kr">www.ieec.or.kr</a>)</td>
<td>- e-Clean Korea (<a href="http://www.e-clean.or.kr">www.e-clean.or.kr</a>) - Internet119 (<a href="http://www.internet119.or.kr">www.internet119.or.kr</a>) - CAUCE Korea (<a href="http://www.cauce.or.kr">www.cauce.or.kr</a>)</td>
<td>- Ahn Lab (<a href="http://www.ahnlab.com">www.ahnlab.com</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luxembourg</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td></td>
<td></td>
<td></td>
<td>(NLIP Association of Netherlands Internet Providers)</td>
</tr>
<tr>
<td>Country</td>
<td>Active Group in Spam Awareness</td>
<td>ISP Security Measures and Protection Provided</td>
<td>Code of Practice among Direct Marketers?</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td>- SAFT Norway (<a href="http://www.saftonline.no">www.saftonline.no</a>)</td>
<td></td>
<td>(NORDMA)</td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>- CNDP (<a href="http://www.cndp.pt">www.cndp.pt</a>)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovak Republic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>- Association of Internet Users (<a href="http://www.aui.es">www.aui.es</a>)</td>
<td></td>
<td>(Federacion de Comercio Electronmico y Marketing Directo)</td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td>- SAFT Sweden (<a href="http://www.saftonline.se">www.saftonline.se</a>)</td>
<td></td>
<td>(SWEDMA)</td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td></td>
<td></td>
<td>(Schweizer Direktmarketing Verband)</td>
<td></td>
</tr>
<tr>
<td>Turkey</td>
<td>- Turkish Anti-Spam Organisation (<a href="http://www.spam.org.tr">www.spam.org.tr</a>)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 1. Active group in spam awareness

<table>
<thead>
<tr>
<th>Government</th>
<th>NGOs</th>
<th>Private Sectors (ISPs, ESPs, Direct Marketers, companies)</th>
<th>2. ISP Security Measures and protection provided</th>
<th>3. Code of Practice among Direct Marketers?</th>
</tr>
</thead>
</table>
| **United Kingdom** | - Department of Trade and Industry  
- Information Commissioner  
- Office of Fair Trading |  
- Interactive Advertising Bureau ([www.iabuk.net](http://www.iabuk.net)) | - AOL UK (McAfee, anti-virus, parental)  
- Freeserver (Wanadoo UK; free McAfee, 1 month trial for firewall and virus)  
- Tiscali (anti-spam, anti-virus)  
- UKFast (anti-spam and virus for hosting only) | Yes (Code of Practice; DMA) |
| **United States** | - Federal Trade Commissions ([www.ftc.gov/spam](http://www.ftc.gov/spam))  
- GetNetWise ([www.getnetwise.org](http://www.getnetwise.org))  
- Spam Abuse ([http://spam.abuse.net](http://spam.abuse.net))  
- Spamsbad ([www.spamsbad.com](http://www.spamsbad.com))  
- Network Abuse Clearinghouse ([www.abuse.net](http://www.abuse.net))  
- Email Abuse ([www.emailabuse.org](http://www.emailabuse.org))  
- Internet Privacy for Dummies ([www.internetprivacyfordummies.com](http://www.internetprivacyfordummies.com))  
- Spywareguide ([www.spywareguide.com](http://www.spywareguide.com)) | Yes (Privacy Promise Member Compliance Guide, Ethical Business Practice, Privacy Policy Generators; DMA) |
| **Worldwide** |  
- OECD Work on Spam ([http://www.oecd.org/about/0,2337,en_2649_22555297_1_1_1_1_37441_00.html](http://www.oecd.org/about/0,2337,en_2649_22555297_1_1_1_1_37441_00.html))  
- ITU SPU ([www.itu.int/osg/spu/policy/](http://www.itu.int/osg/spu/policy/))  
- W3C Internet Security ([www.w3.org/security/](http://www.w3.org/security/))  
- BestPrac.Org ([www.bestprac.org](http://www.bestprac.org))  
- ICC The World Business Organisation ([www.iccwbo.org](http://www.iccwbo.org))  
- Business and Industry Advisory Committee to the OECD (BIAC) ([www.biac.org](http://www.biac.org))  
- Federation of European Direct Marketing Associations (FEDMA) | - Global Business Dialogue (GBDe)  
NOTES

1. The definitions have been provided by Canada.

2. A survey conducted by The Pew Internet & American Life Project in March 2004 reports that 9% of e-mailers said they had responded to an e-mail that they later discovered were fraudulent, 3% had provided personal information in response to an unsolicited e-mail, and 5% of users – representing some six million people – had ordered a product or service in response to unsolicited e-mail.

3. The marginal cost for spammers to send an e-mail is so small, a return rate of only 0.025% or less is sufficient enough for a spammer to make a return on investment.

4. The Korea Information Security Association surveyed the general public’s awareness of internet security in 2003 and discovered that 71.1% of those who had experience in spreading viruses did it for fun and/or out of curiosity. Teens accounted for the largest percentage (13%) of the population who had tried to spread viruses.

5. Online at: http://www.saftonline.org

6. E-mail Service Providers.

7. iCAUCE, CAUCE Australia, CAUCE Canada, EuroCAUCE, CAUCE India, CAUCE Korea, CAUCE USA

8. The icon leads to Stop Spam Here web site where it provides three key tips on protecting your computer, protecting your email address, and protecting yourself. Its web site is at: http://www.stopspamhere.ca.


10. NeverSpam is software for “munging” e-mail address, i.e. iconizing or creating a graphic file of an e-mail address in order to deter any spamware from harvesting the address.

11. www.krcert.or.kr/secureyourserver


14. www.nap.edu/netsafekids/

15. www.nap.edu/netsafekids/


17. Some examples: example@example.com may be “munged” and appear like this: ‘example@NOSPAMexample.com’ or ‘example [at] example [dot] com’.