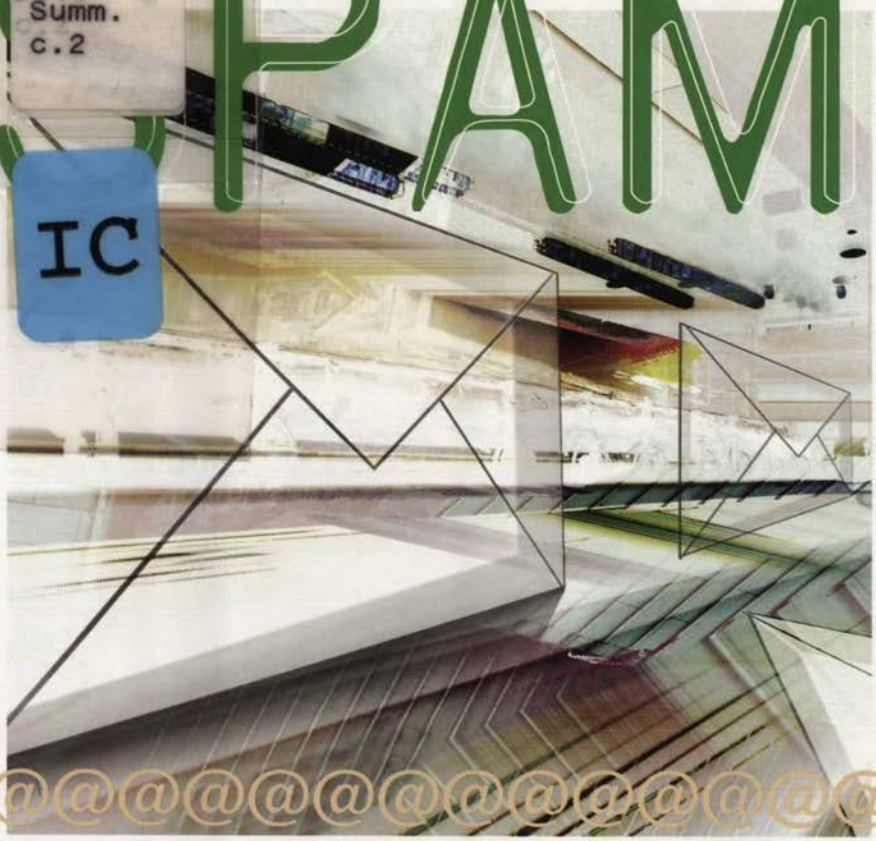
TOPPING SPAM



CREATING A STRONGER, SAFER INTERNET

Task Force on Spam
Executive Summary and Recommendations
May 2005

Canada

This publication is available upon request in multiple formats.
Contact the Information Distribution Centre at the numbers listed below.

For additional copies of this publication, please contact:

Information Distribution Centre
Communications and Marketing Branch
Industry Canada
Room 268D, West Tower
235 Queen Street
Ottawa ON K1A 0H5

Tel.: (613) 947-7466
Fax: (613) 954-6436
Email: **publications@ic.gc.ca**

This publication is also available electronically on the World Wide Web at the following address: **www.e-com.ic.gc.ca**

Cat. No. Iu64-24/2005-1
ISBN 0-662-69021-4
51480B

Cover: 10%
Inside pages: 10%

EXECUTIVE SUMMARY

WHAT IS SPAM AND WHY IS IT A PROBLEM?

The May 2004 Anti-Spam Action Plan for Canada defined spam as "unsolicited commercial email." By this definition, the firm MessageLabs estimated that spam accounted for as much as 80 percent of global email traffic at the end of 2004 — up from about 10 percent in 2000.

Spam is more than a growing nuisance. It is a public policy issue that challenges governments, Internet service providers (ISPs), other network operators, commercial emailers and consumers to work together in new ways — with each stakeholder group fully playing its part — to solve a problem that threatens the interests of all.

At the macro level, spam is a direct threat to the viability of the Internet as an effective means of communication. Because of this, spam is also a direct threat to increasing economic prosperity, to more efficient public services and to the emergence of an e-economy that includes all Canadians.

At the micro level, spam annoys and offends Internet users. It also provides a vehicle for activities that are clearly illegal — or should be. These include:

- malicious actions that cause harm to computers, networks or data, or use personal property for unauthorized purposes (e.g. viruses, worms, Trojan Horses, denial of service attacks, zombie networks);
- deceptive and fraudulent business practices, including online versions of traditional mail-based frauds (e.g. the "Nigerian bank account" or "419" scam, and "spoofed" websites masquerading as legitimate businesses);
- phishing emails designed for identity theft or to steal money; and
- invasions of privacy (e.g. email-address harvesting, spyware).

Who Does Spam Hurt?

Because of the above threats, spam undermines consumer confidence in e-commerce and electronic transactions between citizens and their governments. In addition, it imposes significant costs throughout the economy.

These costs fall on a wide range of actors, including:

- ISPs and other network operators (e.g. large enterprise users, universities, government departments), who must invest in the technical, financial and human resources needed to deploy anti-spam technologies, at the expense of investments in new or improved services, and who must allocate resources to respond to customer complaints;
- legitimate commercial emailers and other users of email services whose messages get filtered out by anti-spam technologies before they reach their intended recipients; and
- private and public sector organizations, whose employees waste time dealing with spam sent to their business email addresses.

Ultimately, all of these costs fall directly or indirectly on consumers and Internet end-users, who must cover the costs of fighting spam not only by purchasing Internet security software, but also by foregoing other kinds of service improvements and paying higher prices for online products.

What Do We Need to Do to Fight Spam?

To fight spam, Canada needs to pursue a multifaceted strategy that involves all stakeholders. The Government of Canada's May 2004 Anti-Spam Action Plan was a good beginning. It identified the main tools that are needed to stop spam. These are:

- vigorous enforcement of current laws that prohibit spamming activities, as well as new legislation as required to fill any gaps identified in existing laws;
- stronger penalties and enforcement mechanisms to deter spammers more effectively;
- industry standards and recommended practices to guide ISPs, other network operators and commercial email marketers in the legitimate conduct of business;
- public education and awareness; and
- international cooperation to fight spam.

During the past year, the Task Force on Spam led the development of a unique, made-in-Canada approach to combatting spam, with the assistance of hundreds of people representing different stakeholder groups. This report details the actions the Task Force has taken, and the work that remains to be done. Through the process, the Task Force learned a number of lessons that are important for the ongoing fight against spam, not only in Canada, but also around the world.

The Need for a Multifaceted, Multistakeholder Approach

The most important lesson has been that a multifaceted, multistakeholder approach to fighting spam works — and is the only approach likely to be fully effective in the long term.

Some countries have chosen to fight spam by relying mainly on legislation and regulations to do the job. The Task Force's experience has confirmed that clear laws, strong penalties and vigorous enforcement are needed to fight spam successfully. Our work has also shown that there are gaps in current Canadian law that must be filled, and weaknesses in its enforcement system that must be addressed. Nevertheless, while good legal tools are needed to fight spam, they are not enough to guarantee victory.

Sound business practices, consumer awareness, public education and international cooperation are equally important instruments of the anti-spam toolkit. To maximize results, these tools must be developed and used in a coordinated fashion within a sound legal framework backed by effective enforcement.

The Need for Communication and Cooperation Among Stakeholders

The second major lesson that the Task Force has learned is the importance of getting the different stakeholder groups that are involved in the fight against spam talking and working together.

When the Task Force began its work, we quickly discovered that the structure of the stakeholder community was like a collection of silos within silos, which presented the challenge of bridging the gaps that normally exist between government, the private sector and public-interest advocates because of differences in interests and perspectives.

The experience of working together on practical tasks to fight spam proved to be a very effective way of breaking down these kinds of barriers. As well as improving communications, the multistakeholder approach adopted by the Task Force produced very significant results in terms of precedent-setting anti-spam enforcement actions, world-leading industry best practices, and high-impact public awareness and education campaigns.

The key to achieving practical results in the ongoing fight against spam will be in continuing to coordinate the actions of all stakeholders through good communications.

The Need for a Comprehensive Strategy to Fight Threats to the Internet

The third major lesson the Task Force has learned is that the fight against spam is only part of a much larger battle now beginning against emerging and potentially much more serious threats to the Internet as a platform for communications and commerce.

When Canada began developing *An Anti-Spam Action Plan* two or three years ago, spam was seen mainly as a time-wasting annoyance for consumers and businesses. This was still the general view of spam when the Task Force began its work.

During the past year, the Task Force has come to appreciate that spam is much more than a mere nuisance. Spam is increasingly associated with activities that are intended to mislead and deceive, to violate privacy, to make unauthorized use of consumer or business equipment, to cause harm to computers or networks, to commit fraud or to steal personal information.

During this same period, spam and these other kinds of threats have begun to spread from Internet email to instant messaging and wireless communication services.

In preparing our report, we have therefore tried to look beyond the familiar problem of unsolicited commercial email, and to take a comprehensive, strategic view of the challenges and opportunities facing Canada from spam and other threats to the Internet.

Recommendations

To combat spam, we recommend the following actions:

Leadership and partnership

1. The federal government, in partnership with other stakeholders, should continue to pursue a multifaceted strategy for stopping spam.

Legislation, regulation and enforcement

2. The federal government should establish in law a clear set of rules to prohibit spam and other emerging threats to the safety and security of the Internet (e.g. botnets, spyware, keylogging) by enacting new legislation and amending existing legislation as required.

3. To this end, the following email activities and practices should be made offences in spam-specific legislation (these provisions may also be reflected, in whole or in part, in existing legislation):

   - the failure to abide by an opt-in regime for sending unsolicited commercial email;
   - the use of false or misleading headers or subject lines (i.e. false transmission information) designed to disguise the origins, purpose or contents of an email, whether the objective is to mislead recipients or to evade technological filters;
   - the construction of false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit other offences listed);
   - the harvesting of email addresses without consent, as well as the supply, use or acquisition of such lists; and
   - dictionary attacks.

4. For these new offences, the following penalties and remedies should be applicable:

   - The new offences created should be civil- and strict-liability offences, with criminal liability open for more egregious or repeated offences. There should be meaningful statutory penalties for all offences listed in Recommendation #3.
   - There should be an appropriate private right of action available to persons, both individuals and corporations. There should be meaningful statutory damages available to persons who bring civil action.

- The businesses whose products or services are being promoted by way of spam should also be held responsible for the spamming. Responsibility should also rest with other third-party beneficiaries of spam.

5. Regarding the enforcement and administration of new legislation:
   - the administration of a new stand-alone law should be undertaken by the Minister of Industry, with support from a separate body responsible for policy oversight and coordination, public education and awareness, and support to enforcement agencies; and
   - enforcement of legislative provisions addressing spam should be undertaken by existing agencies.
6. The federal government should place priority on anti-spam enforcement by providing stronger support and dedicated resources to agencies to administer and enforce new and existing anti-spam legislation.
7. The federal government, in coordination with the provinces and territories, should conclude and implement cooperative enforcement agreements with other countries. These efforts should include examining and amending existing legislative provisions as required to allow for seamless international cooperative investigation and enforcement action.

Best practices for Internet service providers and other network operators

8. ISPs and other network operators should implement the best practices recommended by the Task Force on Spam.
9. ISPs and other network operators, in cooperation with the coordination body established by the Minister of Industry (pursuant to Recommendation 5) should, on an ongoing basis, measure the scope of the spam problem in Canada and assess the impact of the recommended practices. They should continue to identify issues that may require further study, with a view to developing additional recommendations.
10. To assist in the ongoing monitoring of spam trends and the continued development of anti-spam measures and techniques, the federal government should lead in establishing a Canadian spam database (i.e. the "Spam Freezer").
11. ISPs and other network operators should adopt and enforce Acceptable Use Policies (AUPs) that clearly prohibit spamming activities on their networks.

Best practices for email marketing

12. Commercial email marketers should implement the best business practices recommended by the Task Force on Spam and should, in cooperation with the coordination body established by the Minister of Industry, monitor the effectiveness of these practices on an ongoing basis.

13. Canadian industry, in coordination with international standards-development organizations, should continue to investigate various certification methodologies and their associated costs to determine which, if any, would provide the most suitable certification regime for Canada.

14. To help determine the extent of the problem of non-deliverability of legitimate email in Canada, the coordination body established by the Minister of Industry should, with the help of appropriate stakeholders, formally study this issue on an ongoing basis.

User awareness and education

15. As part of its ongoing effort to increase user awareness and education, the federal government, in cooperation with interested stakeholders, should continue to promote the "Stop Spam Here / Arrêtez le pourriel ici" user-tips campaign by encouraging others to link to these websites, and through the use of other appropriate methods and media.

16. The federal government, in cooperation with interested stakeholders, should continue to maintain and enhance the "Stop Spam Here / Arrêtez le pourriel ici" websites in order to increase their value as education tools and sources of appropriate links to other anti-spam resources, and so as to ensure that they remain up to date and relevant (e.g. by including information on industry best practices and future anti-spam legislation and complaints procedures).

17. The federal government, in cooperation with interested stakeholders, should develop appropriate and consistent anti-spam education and awareness campaigns tailored to the needs of different target audiences.

International cooperation

18. The federal government should continue to pursue bilateral agreements on anti-spam policies and strategies with foreign governments.

19. The federal government, in consultation, collaboration and partnership with other stakeholders as appropriate, should actively promote and assist the coordinated international implementation of anti-spam policies, laws, regulations and enforcement measures; industry standards and practices; and public education and awareness activities.

20. Canada should make its expertise in developing multistakeholder toolkit approaches to combatting spam available to help developing countries.

Establishment of a coordinating body

21. In order to carry forward the multifaceted, multistakeholder approach that has been developed by the Task Force on Spam, and to provide a focal point for facilitating the implementation of its recommendations, the federal government should establish a centre, reporting to the Minister of Industry, responsible for policy oversight and coordination, public education and awareness, and providing support to enforcement agencies.

22. The federal government, through this coordinating body, should monitor the impact of the implementation of the Task Force's recommendations; evaluate the results; provide regular public reports; and, in consultation with stakeholders, take whatever additional measures are necessary to combat spam.