

STOPPING
SPAM



CREATING A
STRONGER,
SAFER
INTERNET

STOPPING
SPAM



CREATING A
STRONGER,
SAFER
INTERNET

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

Permission to Reproduce

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from Industry Canada, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that Industry Canada is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced, nor as having been made in affiliation with, or with the endorsement of, Industry Canada.

Opinions and statements in the publication attributed to named authors do not necessarily reflect the policy of Industry Canada or the Government of Canada.

For permission to reproduce the information in this publication for commercial redistribution, please email:
copyright.droitdauteur@pwgsc.gc.ca

Cat. No. lu64-24/2005E-PDF
ISBN 0-662-40232-4
514279B



Cover: 10%
Inside pages: 10%



May 2005

The Honourable David L. Emerson, P.C., M.P.
Minister of Industry
5th Floor, West Tower
235 Queen Street
Ottawa, Ontario K1A 0H5

Dear Minister:

On May 11, 2004, the Government of Canada announced the launch of *An Anti-Spam Action Plan for Canada* and established a government-private sector task force to oversee and coordinate its implementation. We were given one year to do this work. At the end of this period, we were asked to report on the progress made, and to propose any new actions that might be required.

We are pleased to report that we were able to make significant progress toward the goal of stopping spam. This was only possible because of the assistance we received from a large number of people, representing all stakeholder groups, who contributed to our work.

Although we began as a committee of 10 people meeting in a room in Ottawa, we quickly grew to become a network that spanned the country and reached beyond its borders. Much of our work was done online through email. The experience brought home to all of us the potential of the Internet for transforming the ways things get done — and the need to get rid of spam and other threats to Internet use.

Our mandate is finished, but much remains to be done. Our experience has taught us that spam is but one of a number of threats to the safety and security of the Internet as a platform for communications and commerce. We have recommended a series of actions that will help combat spam and spam-related threats in Canada. These actions will position our country as a leader in combatting a growing, worldwide problem. With its long history of leadership in communications, we believe that Canada should aim for nothing less.

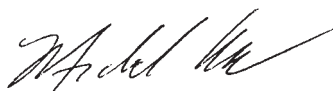
Sincerely,



Lori Assheton-Smith



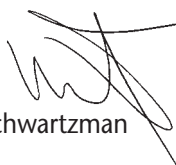
Tom Copeland



Michael Geist



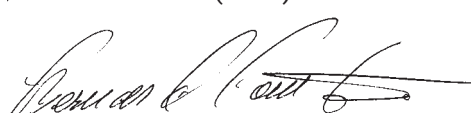
Suzanne Morin



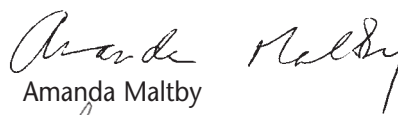
Neil Schwartzman



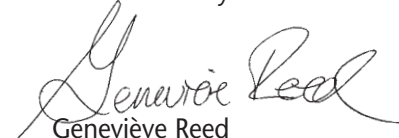
Michael Binder (Chair)



Bernard Courtois



Amanda Maltby



Geneviève Reed



Roger Tassé

CONTENTS

Letter of Transmittal	iii
Executive Summary	1
Recommendations.	3
1. Drawing the Line	7
2. Clarifying the Rules	10
3. Managing Networks to Stop Spam	16
4. Restoring Confidence in Email	20
5. Promoting Public Awareness	24
6. Addressing a Global Problem	27
7. Coordinating Future Action	30
Appendices	
A. Members of the Task Force Working Groups and Secretariat	33
B. Recommended Best Practices for Internet Service Providers and Other Network Operators	37
C. Recommended Best Practices for Email Marketing	43
D. Three Key Tips for Combatting Spam	50
E. Background Reports and Working Documents	53
Glossary	55

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 multi-stakeholder 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.

DRAWING THE LINE

WHAT IS SPAM AND WHY IS IT A PROBLEM?

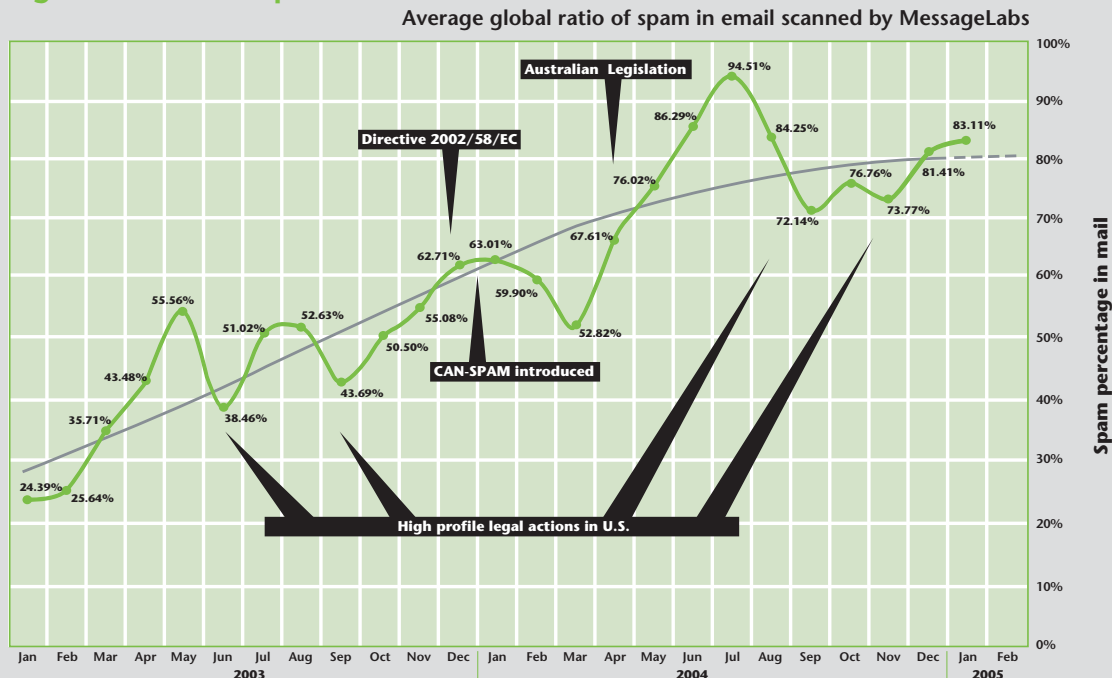
In just a few years, unsolicited commercial email, now generally known as “spam,” has gone from being a minor nuisance to becoming a significant social and economic issue, a drain on the business and personal productivity of Canadians, and a cloak for criminal activity. Spam impedes the efficient use of the Internet for personal and business communications, and threatens the growth and acceptance of legitimate e-commerce.

In 2000, email traffic reports indicated that spam amounted to about 10 percent of the total

volume of electronic mail. As the chart presented in Figure 1 shows:

- by the end of 2002, the amount of spam had climbed to 30 percent;
- by the middle of 2003, the amount of unsolicited commercial email had surpassed that of legitimate communications; and
- by the end of 2004, spam made up 80 percent of global email.

Figure 1: Global Spam Trends 2003–2005



Source: www.messagelabs.com

Reproduced with permission of MessageLabs Ltd., 2005.

The growing volume of spam is now a well-recognized pricing factor for companies that provide facilities for Internet services. This cost is ultimately paid for by organizations and businesses that use electronic communications to conduct their business. It is also paid for by personal users who communicate through the Internet with family, friends and others.

While the overall volume of spam continues to rise, the nature of the spam threat continues to evolve. Improved filtering techniques and other anti-spam safeguards adopted by ISPs and consumers have helped to somewhat reduce the number of spam messages that are reaching the mailboxes of individual Internet users. One public opinion survey, published in Ipsos-Reid's *Canadian Inter@ctive Reid Report* for the fourth quarter of 2004, reported that Canadians believe they are receiving less spam now than a year ago. Nevertheless, as Figure 1 illustrates, the persistent upward trend remains a significant problem for ISPs and users because of the costs of blocking or removing spam from networks.

More significantly, there is disturbing evidence that, even if the volume of traditional spam were to decline, the incidence of new threats posed by mutations of spam would still clearly be on the rise. These broader threats to Internet security include spyware, viruses, phishing and botnets, to name but a few. Recent reports show that these threats have dramatically increased in the year since the Task Force began its work. For example:

- MessageLabs reported seeing 18 million phishing emails in 2004.
- The October 2004 AOL®–National Cyber Security Alliance *Online Safety Study* reported that 80 percent of American users have spyware or adware on their computers, and that 89 percent of those users did not know that these programs were there.

The new mutations of spam undermine consumer confidence in the Internet as a platform for commerce and communications. Because of this, the potential of information and communications technology to buttress productivity, and the ability of e-commerce to attract investment, create jobs and enrich our lives, is constrained not only by torrents of spam, but by the deceptive, fraudulent and malicious activities that sometimes accompany it.

Principles Guiding Canada's Anti-Spam Action Plan

The degree of public concern and the growing costs to our economy have made it clear that government, industry, marketers and consumers must work together in a new partnership to reduce and control spam.

It is also apparent that spam is a multifaceted problem that requires coordinated action on several fronts in order to achieve real and measurable progress. Canadian stakeholders and international partners are all in agreement on the following principles:

- Commercial email sent with the prior and ongoing consent of the recipient is not spam and has a legitimate place in e-commerce.
- Commercial email sent without prior consent — or that is deceptive, fraudulent or malicious — is spam and should be prohibited.
- There is merit in examining the use of current laws and possible new laws to fight spam. However, unless enforcement agencies assign a high priority and allocate sufficient resources to anti-spam actions, laws alone will not stop spam and related threats, even if these laws are accompanied by technical measures, better business practices and changes in consumer behaviour.
- There is a consensus that government should not dictate detailed technical solutions. Instead, government should encourage and assist all partners in using and sharing the best available technical solutions and the best consumer and business practices.

- An effective solution to spam will require not only concerted actions by all partners in Canada, but also greater cooperation at the international level. Although Canada, unfortunately, remains a source of some spam, the great majority of spam emails received by Canadians originate outside Canada. An effective international response to spam will require a coordinated international approach involving governments and other stakeholders.

Mandate, Structure and Working Methods of the Task Force on Spam

On May 11, 2004, the Minister of Industry announced *An Anti-Spam Action Plan for Canada* designed to reduce the volume of unsolicited commercial email, and established a Task Force on Spam to oversee the implementation of the Action Plan. Chaired by Industry Canada, the Task Force brought together experts and key stakeholders representing ISPs, Canadian businesses that use email to conduct legitimate commercial activities and consumers.

The Task Force was given one year to oversee and coordinate the implementation of the Action Plan. After this period, the Task Force was asked to report on the progress made and to propose any new actions that might be required, including legislative initiatives.

Despite its relatively small number of members, the Task Force represented a broad range of organizations with stakes in the future of email communications, from individual users to large companies that develop and supply the software and equipment that fuels Internet growth. In order to organize its work and engage other stakeholders, the Task Force established five working groups, under the following titles, to address specific points contained in the Action Plan:

- Legislation and Enforcement
- Network and Technology Management
- Validating Commercial Email
- Public Education and Awareness
- International Collaboration

Membership in the working groups was open to all interested individuals and organizations. About 60 organizations answered the call. These are listed in Appendix A.

During its mandate, the Task Force was asked to bring key stakeholders together to review the implementation of the Action Plan and identify any other areas that might require further action. This was done through a national Stakeholder Roundtable held December 3, 2004.

The Task Force was also asked to consult all interested stakeholders and individual Canadians who might wish to express their views or make a contribution to its work. To do this, the Task Force issued a notice in the *Canada Gazette* in summer 2004, and established an online forum where individuals could express their views on any of the subject areas under consideration by the Task Force.

General Recommendation

The Task Force's experience has shown the value and necessity of continuing with a multifaceted, multistakeholder approach to combatting spam. Although significant progress has been made in the fight against unsolicited commercial email during the past year, much remains to be done.

In addition, the new and much more serious threats to Internet security that are now emerging — such as spyware and identity theft resulting from phishing and other illegal online activities — heighten the importance of maintaining the multistakeholder momentum developed by the Task Force.

The Task Force has come to the conclusion that, in order to successfully wage the war against spam, it is necessary to establish a focal point that has the responsibility of coordinating the ongoing battle against spam and the illegal activities associated with it.

We therefore recommend the following:

Recommendation 1:

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

CLARIFYING THE RULES

THE CHALLENGE

Traditional markets for physical goods and services operate in the context of laws and regulations designed to promote fair competition and protect consumers. To work effectively, e-commerce markets need similar rules to guide commercial behaviour. As discussed in the previous chapter, spam presents a significant threat to the development of e-commerce by imposing costs, creating inefficiencies, causing harm and undermining the confidence of business and consumers alike.

Some of the threats posed by spam can be dealt with by enforcing existing legislation, raising business and consumer awareness, and promoting public education. However, these measures are unlikely to succeed against the truly bad who are found among spammers — those whose intent is to commit fraud, steal personal identity, violate privacy, gain unauthorized access, or cause harm to computers and network equipment. Clearer laws prohibiting illegitimate behaviour, strong penalties and rigorous enforcement are needed to deal with these kinds of threats, and to underpin Canada's toolkit approach to fighting spam.

A strong domestic framework will become even more crucial as spam increasingly becomes the vehicle for activities such as phishing, and technology such as spyware, viruses and botnets, which pose a serious threat to the Internet as an economic platform by undermining trust. The Internet has become part of our nation's critical infrastructure and we must, as a country, be able to effectively address these threats to its security.

A strong domestic framework is also needed if we are going to play our part in fighting spam worldwide. The vast majority of spam reaching Canadian citizens and businesses originates outside Canada. However, with a clear, solid legislative framework in place, and with effective enforcement capabilities and efforts, Canada would be well positioned to work towards internationally harmonized approaches and cooperative enforcement actions.

One of the first questions facing the Task Force on Spam was how well Canada's current legal and enforcement framework measured up to the challenge of combatting spam.

When *An Anti-Spam Action Plan for Canada* was being developed, many stakeholders expressed the view that improving the enforcement of existing Canadian laws could significantly reduce the flow of spam. Specifically, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the *Competition Act* and the *Criminal Code* of Canada were cited, on the following grounds, as tools that could help address the problem of unsolicited email.

- PIPEDA, designed to protect personal information in the electronic age, prohibits the collection, use or disclosure of personal information, including email addresses, without consent. This law also specifies that personal information can only be used for the purpose for which it was collected, and that consent is required for any further secondary use. Thus, any unsolicited email sent to the email

address of an individual who did not consent to receive that email could be in violation of this federal Act and, possibly, other substantially similar provincial legislation.

- The *Competition Act* contains provisions dealing with deceptive and misleading representations. These have frequently been used to deal with misleading advertising in traditional media. The application of this Act to misleading claims made in email solicitations clearly merited examination.
- The *Criminal Code* of Canada contains specific provisions dealing with unauthorized access to computer systems and networks, mischief to data and more general fraud provisions. Since many email abusers send “Trojan” programs embedded in email messages, which can then be activated by spammers to relay spam, the *Criminal Code* could possibly be used to address these spam-related offences. Its provisions include substantial fines and even imprisonment.

Although these existing acts were identified as having provisions that could potentially be used in the fight against spam, the Task Force noted that their effectiveness remained an open question, since most had not yet been used in spam-related cases.

The first challenge facing the Task Force, therefore, was to determine the adequacy of Canada’s current legal and enforcement framework in the fight against spam. To respond to this challenge, the Task Force decided to work with other government departments and agencies to examine existing laws and enforcement mechanisms to see if there were any gaps that could prevent them from being useful parts of the anti-spam toolkit.

Since this proved to be the case, the second challenge facing the Task Force was to determine what measures would be required to fill these gaps, so that Canada would have an effective legal framework and a coordinated, national enforcement approach for dealing with spam and related activities.

Task Force Actions

Raising Awareness and Catalyzing Action by Enforcement Agencies

The Task Force initially focused on facilitating discussions among private companies and the federal enforcement agencies responsible for legislation that could be used to address spam. These agencies included the Competition Bureau, the Office of the Privacy Commissioner of Canada and the RCMP (Royal Canadian Mounted Police). The intention was to evaluate how effective the individual statutes would be in prosecuting offences related to spam.

First, all federal statutes that could apply to elements of spam were identified. The Task Force decided to focus its efforts on those elements of spam that had the clearest links to provisions in existing statutes. A number of smaller task groups were established to discuss the requirements of different situations involved in pursuing cases under each statute. As of the release of this report, three complaints had been settled under PIPEDA, and one under the *Competition Act* (see Box 1: Recent Spam-Related Cases).

Little progress was made with respect to the *Criminal Code* of Canada, because of a lack of prioritization and jurisdiction, since primary responsibility for prosecution rests with provincial governments and local law enforcement agencies. However, the Task Force worked with these groups to advance the issue. In addition, the Task Force worked with the Department of Justice Canada and the RCMP’s Technological Crime Branch to identify the general evidentiary requirements that would be involved in bringing cases forward under specific provisions of the *Criminal Code*.

Following discussions with the Canadian wireless communications industry, the possibility was raised of applying existing provisions of the *Telecommunications Act* to spam sent to wireless handsets. The passage of Bill C-37 (for the creation of a national do-not-call list) may provide an opportunity to strengthen the Canadian Radio-television and Telecommunications Commission’s (CRTC’s) ability to address wireless

Box 1: Recent Spam-Related Cases

Complaint Findings by the Office of the Privacy Commissioner of Canada

Two members of the Task Force on Spam filed complaints under PIPEDA.

Michael Geist received two email solicitations to purchase season tickets from a community football team. The team's office had obtained Geist's email address from university and law firm websites. He filed a complaint with the Privacy Commissioner after he received the second email, which was sent after Geist requested that he not receive further emails.

The Office of the Privacy Commissioner found that a business email address is personal information and, therefore, protected by PIPEDA. Such information can be collected and used without consent, but only for its intended purposes (i.e. purposes related to Geist's business as professor and lawyer). The Commissioner concluded that the football team could not rely on this exception, since its purposes were entirely unrelated to the intentions of publishing the email address.

Suzanne Morin received email solicitations, from a different company than Geist, at her business email address. Her email address was collected from an online professional association membership directory. She filed a complaint with the Privacy Commissioner. The Office of the Privacy Commissioner again found that a business email address is, for the purposes of PIPEDA, personal information. The Office found that the collection and subsequent use of Morin's email address for commercial email solicitation were done by the marketing company without her consent, in contravention of the Act.

In both cases, the organizations apologized for their actions, removed the email addresses from their email marketing lists and amended their internal practices accordingly.

Resolution of a Case by the Competition Bureau

Performance Marketing Ltd. made false claims about Zyapex and Dyapex Diet Patches, promoting them as safe and natural weight-loss products, giving the impression that without performing any physical exercise or dieting a person could lose weight, reduce their appetite, control their cravings and speed up their metabolism. These claims were made via email. Performance Marketing Ltd. failed to enforce its anti-spam policy, which led to its affiliates using spam to sell the products.

The case was pursued under the Competition Bureau's Project FairWeb, which is aimed at combatting misleading and deceptive advertising on the Internet. According to the resulting Consent Agreement with Performance Marketing issued in December 2004, the company has agreed to ensure that spam will not be used as a vehicle for marketing its products, to post a corrective notice on its website and to provide a full refund to those who purchased the diet patches.

spam — specifically, emailing of SMS (Short Message Service) spam to mobile handsets. Of particular importance would be the CRTC's fining authority. Until Bill C-37 is passed, it may be too early to judge the role that the *Telecommunications Act* could play.

The Problem of Enforcement

The initial stages of the Task Force on Spam's work served to educate both enforcement agencies on the extent and severity of the spam problem; and private companies on the legal requirements, including evidentiary requirements, for the successful pursuit of cases. Parallel with this work, some enforcement agencies have taken direct action against spammers (see Box 1 above). Nevertheless, the overall effectiveness of enforcement efforts to date has been limited.

The enforcement agencies face a number of challenges related to the use of their legislation to address all the various elements of the spam problem. Limited resources and competing priorities are significant factors hindering the two regulatory bodies involved, as well as the RCMP and local law enforcement agencies. A further impediment to effective enforcement is the frequent lack of specialized technical expertise needed to track down, investigate and prosecute spammers. Finally, in many cases, existing enforcement powers have not yet been used, and the legislative tools to attack particular elements of spam are either too uncertain in their application or simply missing.

The Task Force strongly believes in the need to strengthen the enforcement process. This should begin with a clear policy commitment to curbing spamming and spam-like activities by not only responding to complaints but also proactively investigating and prosecuting spammers.

While increasing resources, both in the form of funding and technical expertise, is essential, increased support for enforcement agencies should also take the form of better mechanisms for collecting, coordinating and processing information on spam, including that which is received from user complaints. Chapter 7 of this report discusses these mechanisms. Last, but not least, we must fill the gaps that exist in the legal and regulatory regime governing spam and other threats to the Internet, such as spyware.

Legal Research

As background to its deliberations, the Task Force researched spam legislation in other countries, with a particular focus on the United States, the United Kingdom and Australia, in order to benchmark Canada's current situation in relation to these jurisdictions. Box 2: International Anti-Spam Legislation highlights the legislation in place in a number of key countries.

The Task Force also commissioned a study examining the issue of a private right of action for spam in Canada, including the existing legislative framework, the key elements of building such a right and the views of Canadian companies on the need for such a right.

Identification of Legislative Gaps

After reviewing existing legislation and enforcement activities, taking into account the experience of other countries that have already enacted broad-based anti-spam laws, and reviewing the results of the cases triggered by the Task Force and the resulting lessons learned, a number of gaps in existing Canadian legislation and enforcement became evident.

The existing provisions of the three relevant acts, while applicable to some elements of spamming activity, could not be used with sufficient certainty to effectively address many of the methods and means used by spammers. Nor could they be used against some of the more aggressive and invasive forms of spamming, or to counter the new threats to Internet security that are emerging. Agencies are limited in their enforcement

Box 2: International Anti-Spam Legislation

United States — *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)*

Australia — *Spam Act 2003*

United Kingdom — *Privacy and Electronic Communications Regulations 2003*

France — *Loi pour la confiance dans l'économie numérique 2004*

European Union — *EC Directive 2003/58/EC*

powers by the scopes and purposes of their acts, and, as the laws are currently written, many spamming and spam-related activities fall outside these boundaries.

An additional gap was identified related to deterrence. Where the acts did apply, the question remained "Are the penalties appropriate to deter spamming activities?" The Task Force determined that, while existing mechanisms may be adequate when used against legitimate companies who have spammed in error, it is not clear whether they would deter truly bad actors. Even when significant penalties are available, as through the *Criminal Code*, the practicality of applying them in spam-related cases is limited.

A Framework for Spam Legislation and Enforcement

After fully assessing the adequacy of existing legislation and enforcement capabilities in light of the threats posed by spam and spam-related activities, the Task Force came to the following conclusions:

- While existing laws address specific aspects of spam, they are not, separately or together, sufficient to achieve the overall goal of deterring spammers in Canada.
- A stand-alone, technology-neutral law that clearly addresses spam, spam-related offences and emerging threats (e.g. botnets, spyware and keylogging) is required. Amendments to existing laws may also be required.

Nature of Offences and Remedies/Penalties

- Failure to abide by an opt-in regime for sending unsolicited commercial email should be made an offence in a stand-alone, technology-neutral spam statute.
- 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 should be made an offence. This should be the case whether the objective is to mislead recipients or to evade technological filters.
- Constructing false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit the other offences listed) should be made an offence.
- The harvesting of email addresses without consent, and the supply, use or acquisition of such lists should be made an offence.
- Dictionary attacks should be made offences.
- 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 outlined above.
- 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.

Administration and Enforcement

- The Minister of Industry should be responsible for administering new legislation on spam, and a centre of responsibility should be established for policy oversight and coordination, public education and awareness, and support to enforcement agencies.

- Enforcement of new legislative provisions addressing spam should be undertaken by existing agencies.
- New and existing spam provisions must be accompanied by increases in dedicated resources and support for the agencies that will enforce them.
- Given that spam is a borderless problem, there is a need for provisions allowing for cooperative international enforcement and investigation. Any current provisions should be examined and amended as required to allow for seamless action on spam.

Regulatory Arrangements

Although the main focus of discussions among working group members was the prohibition of spamming and spam-related activities, there was some discussion at the Stakeholder Roundtable meeting in December 2004, as well as among Task Force members, about broader regulatory arrangements. Some argued for a “co-regulatory” approach, based on the Australian model, that would outline responsibilities, primarily for ISPs, in areas such as protecting networks against spam. Others maintained that the Canadian practice of voluntary cooperation and industry peer pressure would prove to be a faster and more effective way of fighting spam than the co-regulatory approach. While there was much debate on this topic, there was general agreement that government should play no role in dictating specific technical solutions, and that the legislative ground rules (including those outlined above) should be technology-neutral.

Although industry efforts to address the problem of spam were already under way, the experience of the Task Force has demonstrated the value of government–industry dialogue in catalyzing private sector action. The Task Force, therefore, considers continued government–industry dialogue in this area essential. The Task Force has also noted that broader questions about Internet regulation should be addressed through the Telecommunications Policy Review announced by the Government of Canada in the federal Budget 2005.

Recommendations

It is clear to the Task Force, from our analysis of the Canadian situation and the experiences of other countries, that Canada will not be able to combat spam effectively within Canada unless its multistakeholder toolkit approach includes a clearer, more comprehensive, and actively enforced set of domestic laws that protect Internet users and facilitate the development of e-commerce.

We therefore recommend the following:

Recommendation 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.

Recommendation 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 construction 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;**
- **constructing 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.**

Recommendation 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.**

Recommendation 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.**

Recommendation 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.

Recommendation 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.



MANAGING NETWORKS TO STOP SPAM

THE CHALLENGE

Any measure aimed at successfully protecting the security of Internet communications from threats such as spam, viruses and spyware must involve more than government actions. There is consensus among stakeholders on a number of steps that can be taken by ISPs and other network operators (e.g. large enterprise users, universities, government departments) to build trust in Internet communications.

Some of these initiatives relate to the development and application of technology. Others relate to the implementation of best practices within the industry, including Acceptable Use Policies that prohibit spamming. All of these industry initiatives are based on a common goal: ensuring that email remains a viable tool for legitimate business and personal communications.

By its design and architecture, the Internet is an open network of networks that allows the free flow of information. The redesign and implementation of technical standards to enhance security and curtail abuse will be ongoing over many years.

There are, however, a number of known practices that permit spam and other forms of network abuse to happen. These include leaving servers open to relay and forward messages, thereby allowing computer systems to be hijacked as proxy email servers for abusers. Some steps have been taken by several organizations to warn businesses and network managers

about the importance of securing systems and networks, but adoption of these practices remains uneven.

While the problem of spam, like the Internet itself, is global in scope, network-management actions taken in Canada can contribute to the solution. Those who own and manage networks and facilities must address and adopt management practices that will effectively reduce and control spam and related threats.

Canadian industry stakeholders have the ability to agree on basic operating practices for network facilities that will reduce spam, and can show leadership by requiring the adoption of these practices on networks and facilities based in Canada.

Task Force Actions

The Task Force on Spam represents the first-ever collaborative, concerted effort involving a broad range of organizations, including most of the country's largest and smallest broadband and dial-up ISPs, other network operators, large enterprise users, software developers, anti-spam advocates and government. The agreement by these stakeholders to work together to develop and implement industry-wide spam solutions is an important step forward. However, it is only the beginning of a long-term commitment to taking the actions necessary to stop spam.



Box 3: Recommended Best Practices for Internet Service Providers and Other Network Operators

- All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible.
- ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive email over port 25 should be restricted to hosts and the provider's network. Use of port 25 by end-users should be permitted only on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.
- ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.
- ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.
- ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.
- ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.
- ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.
- ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).
- Non-delivery notices (NDNs) should only be sent for legitimate emails.
- ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.
- ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFC) 1918 — "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.
- ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822; and reference domains and IP addresses should have up-to-date, accurate registration information.

Recommended Best Practices for Internet Service Providers and Other Network Operators

The Task Force has developed a set of recommended technical best practices intended to help reduce spam in Canada. Box 3 above presents the highlights of that document. The adoption of these practices will also address spam-related security issues, since spam is often the vehicle for more harmful activities. The practices represent a continuation of efforts and progress that have been under way for some time in Canada and internationally. The Task Force has advanced this work to establish the first truly national consensus on recommended technical measures for combatting spam. Through these best practices, Canada has a model to share internationally in the global fight against spam. However, it will be important to continually update these best practices to reflect the continuing evolution of spam trends and techniques.

The full text of the best practices recommended by the Task Force is presented in Appendix B.

Measuring Implementation and Impact

A substantial number of Canadian ISPs, including many of the major players and other network operators, have started to implement some or all of the recommended technical practices, particularly by blocking port 25 and upgrading their filtering techniques.

The experiences of other countries have shown that ISPs themselves, particularly market leaders, can do much to spread the adoption of anti-spam technical and business best practices throughout the industry. The leadership already shown by some Canadian ISPs in implementing the recommended best practices has been instrumental in encouraging other ISPs to do likewise.

While this is an encouraging beginning, it will clearly be necessary to systematically monitor the implementation of the recommended best practices, in order to assess their impact and identify any new problems that may need to be addressed through amendments or additions to the best-practices provisions. If this is not done, it will be difficult for industry, government policy-makers and other stakeholders to determine the level to which industry has adopted the recommended best practices, or to measure their effectiveness in the fight against spam.

In the spirit of industry self-regulation, the Task Force encourages the major players in the ISP and network-operator communities to continue to show leadership in implementing the recommended best practices, and to encourage others to follow their example.

The Task Force also calls on the major players and relevant industry associations to play an active role, together with the coordination body described in Chapter 7, in helping develop an effective system for measuring and publicly reporting on the impact of the recommended best practices.

Canadian Spam Database (“Spam Freezer”)

The Task Force on Spam evaluated the idea of establishing, under a public-private sector partnership, a Canadian spam database, or “Spam Freezer,” similar in design to the “Spam Fridge” maintained and monitored by the U.S. Federal Trade Commission (FTC).

The objective of a Canadian database would be to provide a repository to which email users could send copies of spam received in their computer mailboxes. Spam messages sent to the database would be inventoried and kept for a prescribed period of time by a Canadian organization with central coordinating responsibility in the fight against spam.

The database would provide an opportunity for law enforcement agencies from Canada and possibly other countries, ISPs, other network operators and various levels of government to access data that could be used for statistical analysis and to gather evidence for anti-spam enforcement activities.

Internet Email Spam Over Wireless Devices

Unlike the Internet, which developed as an open, public network, mobile technologies were originally deployed on closed, private networks.

Convergence of technologies and increased interaction between the Internet and mobile technologies, however, mean that some of the problems that originally affected the Internet are beginning to affect mobile networks. This can happen when people use wireless devices to retrieve email, including spam, from their ISPs. It can also happen when people begin to receive new forms of spam originated on wireless networks and transmitted through mobile-phone text messaging (i.e. SMS), multimedia messaging and instant messaging services. These kinds of messaging services have become successful applications of mobile technology. They provide a host of possibilities for developing innovative services, but also give spammers new opportunities.

“Mobile” or “wireless” spam is potentially more problematic than spam sent to desktop computers, since wireless spam follows the customer and since, in some cases, customers pay a fee per message received. Wireless spam is a major annoyance to wireless subscribers, and can potentially be much more intrusive than spam sent to a personal computer.

The Task Force consulted with the Canadian wireless industry to discuss this issue and explore what might be done to prevent spam from becoming a major problem on wireless networks. Through these discussions, the Task Force learned that spam originating on wireless networks is perceived as a serious threat by wireless-network operators. The wireless industry is implementing

4

RESTORING CONFIDENCE IN EMAIL

THE CHALLENGE

Before the establishment of the Task Force on Spam, most Canadian initiatives aimed at controlling the growing volume of unsolicited commercial email focused on a combination of filtering technologies and the use of “black lists” of servers and domains that have been identified as sources of spam. As these spam-control services have become more and more sophisticated, so have the tactics used by spammers to bypass them.

The diverse types of spam-filtering and blocking tools used by ISPs and other network operators — and the resulting cyclical battles between spammers and spam blockers — produced some unwanted results. Legitimate commercial email communications, as well as legitimate noncommercial and personal email communications, are now often blocked by filters, sometimes without the knowledge of either the senders or the intended recipients. These filtering techniques and practices, though well intended, have inadvertently contributed to undermining consumer confidence in the reliability of email.

For this reason, a number of commercial organizations are now considering moving their email services to closed networks, which would undermine the Internet as a platform for commerce. While the motivation for considering this solution is understandable, a migration of commercial activity away from the public Internet and toward closed networks could have undesirable consequences.

Less drastic alternatives to closed networks are beginning to emerge in the form of techniques that shift the focus away from blocking unwanted communications toward facilitating the movement of legitimate commercial email. Although these techniques impose costs on the senders of commercial email and on the owners and managers of network facilities, it is possible that these costs may be offset by the following benefits that could result for different stakeholders:

- for commercial email senders, the value of improved deliverability;
- for service providers, reduced costs in managing email service and customer preferences;
- for email users, more effective tools to manage their email.

Certification is one of the techniques emerging for improving deliverability. At minimum, a certification regime should require verifiable identification of both the sender and the nature of the communication. To be fully effective, it should also include performance-measurement tools and appropriate sanctions for certificate holders that do not abide by the rules.

In addition to certification tools, techniques are becoming available to facilitate the movement of legitimate email by authenticating sending and receiving sites. However, these techniques do not necessarily protect recipients against false, misleading or fraudulent emails sent from authentic sites.

Box 4: Recommended Best Practices for Email Marketing

- Marketing email should only be sent to recipients who have provided their consent to receive such information.
- In all marketing email, recipients must be provided with an obvious, clear and efficient email or web-based means to opt out of receiving all further business and/or marketing email messages from the organization.
- The internal process used to obtain consent should be clear and transparent. Organizations should keep records of the type of consent obtained from recipients so that email lists can be scrubbed prior to campaign broadcasts.
- Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.
- Every email should provide a link to the sender's privacy policy. The privacy policy should explain the intended use and disclosure of any personal information that might be gathered through "clickstream" means or other website monitoring techniques.
- Marketers, list brokers and list owners should take reasonable steps to ensure that the addresses on their email lists were obtained with the proper consent.
- Marketers should use a high degree of discretion and sensitivity in sending email marketing to persons under the age of majority, in order to address the age, knowledge, sophistication and maturity of this audience.
- When the content of an email is adult in nature the sender must — prior to sending the communication — verify that the recipient is of age to legally receive and view such content.
- All email containing sexually explicit content should include the prefacing tag "SEXUALLY EXPLICIT" in the subject line.
- Organizations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.
- Organizations may disclose the email addresses of existing customers to third-party affiliates or within a family of companies if:
 - they have consent to do so;
 - they are using the addresses for purposes consistent with their collection (i.e. marketing related to the original purchase or to provide services related to that purchase);
 - it is transparent to the recipient why they are receiving email communications; and
 - there is an easy-to-use way to opt out of receiving further email communications.

False positives are a problem, not only because they undermine the effectiveness of email as a marketing tool for businesses, but also because they cause difficulties for end-users, who are increasingly relying on the deliverability of the email they send and receive from associate sources, be they professional (e.g. business colleagues), commercial (e.g. as a result of marketing and online purchases the user has requested) or personal (e.g. private correspondence).

Marketing firms and others are increasingly using outsourced deliverability firms to better their returns on investments, or hiring full-time personnel to deal with these issues.

The publishing by ISPs of clear policies and procedures for inbound email, as well as their providing points of contact, would also serve to improve the deliverability of legitimate email.

Several of the largest receiving sites — AOL®, MSN® Hotmail and Yahoo!® — have all published policies and procedures outlining the requirements for legitimate emailers who want to be white-listed. How much this status circumvents inbound-spam filtering naturally varies between sites.

Email Certification

Several technical methods are currently used to fight spam. However, some of these methods may not always be able to distinguish between legitimate email and spam. For example, some spam filters block bulk mailings of legitimate emails simply because they look similar in nature to spam. Others analyze the content of email messages in order to decide whether or not to filter them, using keywords that can appear in legitimate email as well as in spam. To complicate matters further, spammers often design their emails to look like legitimate email, and also use other techniques to trick filters.

As mentioned in the "Challenge" section of this chapter, email certification is emerging as a method that could be used to help spam filters allow legitimate email through to its intended recipients. It could also allow verifiable determination between legitimate and phishing emails.

Working in cooperation with the ICT Standards Advisory Council of Canada, the Task Force on Spam explored the principles, business models and techniques that characterize the different certification methods currently available in the Canadian marketplace, in order to develop a reference paper that captures the results of this analysis and examines options for implementing an email certification regime in Canada.

Recommendations

Commercial emailers have the most to lose and the most to gain in the battle to stop spam. Of the various stakeholder groups involved in the fight against spam, commercial emailers also face the greatest challenges in organizing themselves to take concerted action against spammers and to play their part in implementing the toolkit approach.

A number of distinctly different kinds of organizations make up the commercial-emailers stakeholders group, including:

- companies that commission bulk commercial email in order to market their products and services;
- companies that engage in email marketing;
- companies that design and manage marketing campaigns;
- commercial-email service providers; and
- companies that supply lists of email addresses.

In some cases, the companies that provide these different kinds of products and services are vertically integrated across different segments of the commercial-email supply chain. In other cases, they are independent of each other and operate on the basis of contractual arrangements.

The majority of companies that make up the diverse population of the email stakeholder group operate according to existing laws and in conformity with generally accepted business practices. As the PIPEDA cases demonstrated, these companies are usually quick to make amends if they are found to be engaging in activities or practices that contravene these standards.

Unfortunately, each segment of the email supply chain contains spammers — companies and individuals that deliberately contravene the laws that currently prohibit sending unsolicited commercial email, or that use email as a cover for activities that are intended to deceive, cause harm to computers and network facilities, steal personal information and commit fraud.

To stop spam, it is necessary to stop spammers. If this is not done, there is a risk that Canadians will lose confidence in the Internet — not just as a vehicle for marketing and promoting products and services, but also as a method of effective communication. A general loss of confidence in email would, in turn, severely inhibit the emergence of an e-economy in Canada, and would undermine the interests of the many businesses, organizations, institutions and governments involved in the professional email supply chain.

We therefore recommend the following:

Recommendation 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.

Recommendation 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.

Recommendation 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.

5

PROMOTING PUBLIC AWARENESS

THE CHALLENGE

While there is much that lawmakers, enforcement agencies, ISPs and other network operators, and commercial emailers can do to fight spam, there is general agreement that all Internet end-users, whether they are employees, students or consumers, have an important role to play in the ongoing battle against spam.

It is also clear that, in order to help Internet users play their part, more needs to be done to inform them about what they can do to limit the amount of unwanted commercial email they receive, to protect themselves and others against viruses, to avoid falling prey to fraud and to prevent their computers from being turned into “botnets” used without the user’s knowledge to send spam.

There is a considerable amount of readily available information on the steps users can take to limit the amount of spam they receive and avoid falling victim to the kinds of deceptive, fraudulent or other criminal practices associated with spam. However, public opinion surveys have demonstrated that more effort is needed to communicate this information, particularly as it pertains to emerging threats that can compromise machines, harm consumers and undermine Internet security.

Some of the simplest messages — such as “do not open unsolicited emails,” “do not buy from spammers” and “do not provide personal information if you are not certain who you are dealing with” — have either not yet reached all users or not been understood. For example,

the Ipsos-Reid *Ipsos Trend Report Canada* for May–June 2004 reported that more than one third of online Canadians open their spam emails, and that the main reason they give for doing so is curiosity.

A recent study by Option consommateurs also indicated that certain groups might benefit from increased education and awareness efforts tailored to their specific needs. These groups included people under 30 — who reported receiving more spam than other groups — and the elderly.

Given the low rates of positive consumer response needed to make spamming operations commercially viable, awareness of the relationship between the incidence of spam and consumer behaviour needs to be more strongly emphasized as part of the toolkit approach.

Because of their direct relationship with Internet users, ISPs and legitimate sellers of goods and services are in good positions to deliver a public education and awareness campaign in partnership with consumer groups and governments. The challenge facing the Task Force on Spam, therefore, was to facilitate the development of an appropriate social marketing and communications campaign aimed at users; and to implement it in conjunction with consumer groups, other government departments and agencies, and interested international partners.

Task Force Actions

The Task Force reviewed existing public opinion research related to consumers' views on spam, and looked at current education and awareness campaigns, both in Canada and in other countries. Many of these initiatives had enjoyed limited exposure, but in certain cases, key messages had lacked consistency. Following the review of research and initiatives, the Task Force developed a general communications strategy to identify the objectives, key audiences and necessary tools of a potential broad-based public education campaign on spam.

The "Stop Spam Here / Arrêtez le pourriel ici" Campaign

The first phase of the campaign strategy was the development of a bilingual Internet-based user-education campaign. Critical to this initiative was the development of consistent key messages and a common look, and the broad dissemination, by a wide range of partners, of three key tips to help users protect themselves and fight spam.

Working with communications and marketing experts, the Task Force on Spam developed an icon that could be hosted on partners' websites and would contain a link to user tips available at <http://stopspamhere.ca> and <http://arretezlepourrielici.ca>. Information on becoming a partner is also available at these two websites.

The Task Force enlisted both government and non-government partners to host the icon on their websites.

There has been a strong response to the "Stop Spam Here / Arrêtez le pourriel ici" campaign from organizations in the private and public sectors, as well as from the general public. Between November 25, 2004, the date the site went live, and April 2005, there were more than 500 000 unique visits to the site, and some 200 organizations joined the campaign.

Recommendations

The "Stop Spam Here / Arrêtez le pourriel ici" campaign has started a process of educating Canadian Internet users about what they can do to reduce the amount of spam they receive in their inboxes and avoid falling victim to the kinds of deceptive, malicious, fraudulent and otherwise illegal activities associated with certain kinds of spam.

However, much more needs to be done to enable Canadians to play their part in fighting spam, beginning with enhancing the "Stop Spam Here" and "Arrêtez le pourriel ici" websites, and extending the information they provide to other communications media.

General messages that apply to all consumers, of the kind in the "Three Key Tips" presented below, provide a solid foundation for raising awareness and educating the public. However, the Task Force believes that in order to make further progress it is also necessary to develop awareness and education campaigns that are targeted to the specific needs and interests of different groups in the Canadian population.



Stop Spam Here: Three Key Tips

1. Protect your computer

Spam is a growing source of computer viruses. It is critical that you protect your computer from virus-carrying messages. Install and regularly update antivirus and anti-spam software. If you don't have the extra protection of a firewall, get it.

2. Protect your email address

Reserve one email for your trusted personal and business contacts. Create a separate, expendable email address for other online uses.

3. Protect yourself

Don't try, don't buy and don't reply to spam. Just delete it. It's a great way to prevent receiving more spam in the future.

The Task Force feels that it is particularly important to engage small and medium-sized enterprises in the fight against spam, since they stand to be among the major beneficiaries of a spam-free e-commerce environment.

We therefore recommend the following:

Recommendation 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 the websites, and through the use of other appropriate methods and media.

Recommendation 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 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).

Recommendation 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.

ADDRESSING A GLOBAL PROBLEM

6

THE CHALLENGE

It has been estimated that only a small proportion of the spam received by Canadians originates in Canada. This reflects the fact that, because of the open nature of the Internet, spam can potentially be sent from anywhere, to anywhere. Stopping spam therefore requires the harmonization of anti-spam policies, and cooperation among different countries in enforcing anti-spam laws.

Canada has been active for a number of years already in international forums where Internet issues are discussed. Recently, much of this discussion has focussed on the different legislative, regulatory and enforcement actions taken by some countries to deal with spam, and the need to ensure that these approaches are compatible with the global Internet environment.

As a result of this work, progress is being made in coordinating anti-spam policies between countries, and in cooperating internationally to enforce anti-spam laws and regulations. In some cases, this has been done by piggybacking anti-spam enforcement action onto existing cooperative agreements, such as the one between Canada's Competition Bureau and the U.S. Federal Trade Commission. However, these existing arrangements have been used only to a limited extent, and new arrangements should be developed to deal specifically with anti-spam enforcement.

Much remains to be done to promote effective international coordination and collaboration in the worldwide fight against spam. While it is important to coordinate legislation, regulation and enforcement, it is now clear that a broader approach is needed at the international level. Many countries now recognize that a multistakeholder toolkit approach, of the kind Canada has consistently advocated, is proving to be the most effective approach in fighting spam and dealing with other online problems.

For this reason, the Task Force on Spam supports the development and adoption of best practices for email marketers and network management in an internationally coordinated manner. We also encourage Canadian ISPs, email marketers, business email users and Canadian consumer representatives to become active in international efforts to combat spam through initiatives such as the development of globally compatible email authentication and certification regimes.

Task Force Actions

The Task Force on Spam promoted the strong, coordinated presence by the Government of Canada and all Canadian stakeholders in developing and implementing bilateral and multilateral approaches to fighting spam. To this end, members of the Task Force were active in a number of important international forums.

Multilateral Cooperation

1) Organisation for Economic Co-operation and Development Task Force on Spam

Canada is an active participant in the Organisation for Economic Co-operation and Development Task Force on Spam, which has developed an anti-spam toolkit along lines similar to Canada's multifaceted approach.

Individual countries have volunteered to lead or participate in developing elements of the toolkit. Canada has volunteered to undertake a comparative analysis of the anti-spam legislative frameworks that are in place internationally, and has also offered contributions to a number of other items, such as public education and awareness, anti-spam technologies and industry-led measures resulting from Canada's Task Force on Spam's work, including its recommended best practices for ISPs and other network operators.

2) London Action Plan

In October 2004, representatives of the public and private sectors from 15 countries, including Canada, met in London, England, to discuss ways of improving international cooperation in enforcing anti-spam laws and regulations. Since different countries have different anti-spam legislative frameworks, the meeting brought together a broad range of enforcement agencies that may not usually work together, including agencies responsible for data- and privacy-protection, consumer protection, competition and communications regulation.

The result of this meeting was the London Action Plan on International Spam Enforcement Cooperation, which aims to develop ways and means of improving international cooperation in dealing with spam and spam-related problems.

The London Action Plan on International Spam Enforcement Cooperation does not replace international agreements that already exist between enforcement agencies. Rather, its main purpose is to enhance communication among the diverse agencies involved in the fight against spam. The Task Force indicated its support for the London Action Plan on International Spam Enforcement Cooperation, and, through Industry Canada, participated in its implementation. The Office of the Privacy Commissioner of Canada is also participating.

3) Other Multilateral Cooperation

The Task Force was involved in the anti-spam activities of the Asia-Pacific Economic Cooperation forum, the International Telecommunication Union and the World Summit on the Information Society, including in the work of the United Nations Working Group on Internet Governance.

The Task Force also supported the anti-spam activities of the United Nations Conference on Trade and Development, the Internet Engineering Task Force, and the International Consumer Protection and Enforcement Network.

The Task Force would also like to acknowledge the important work done by the private sector through bodies such as the Anti-Spam Technical Alliance, the Messaging Anti-Abuse Working Group and various industry associations.

Bilateral Initiatives

Canada is actively promoting international cooperation in the implementation of anti-spam policies and strategies through bilateral policy agreements with key partners, including Australia, the United Kingdom, the United States, Taiwan and the European Commission. Agreements have already been signed with Australia and the United Kingdom, and the Task Force anticipates that agreements will be signed later in 2005 with the United States, Taiwan and the European Commission.

Recommendations

Canada has a long history of international leadership in communications policies and strategies. In recent years, our comprehensive e-commerce policy framework, our competitive broadband marketplace, and our service-transformation and government-online initiatives have drawn international attention.

The Task Force believes Canada has an opportunity to lead in the next phase of the global fight against spam. Although a number of other countries have already enacted anti-spam legislation, and were the first to promote cooperative enforcement mechanisms, Canada has seen demonstrated results in industry best practices and its public awareness campaign, which are solid first steps demonstrating the value of adopting a multifaceted, multistakeholder approach that complements strong laws and vigorous enforcement with other tools.

As well as an opportunity, the Task Force believes Canada has an obligation to exercise international leadership in combatting spam. One major contribution the country can make is to reduce the amount of spamming in Canada.

In analyzing the experiences of other countries and the efforts currently under way to construct cooperative enforcement mechanisms, the Task Force has come to the following conclusions.

- There is much to be learned from the experience of other countries about what works — and what does not work — in the fight against spam and related threats to the Internet. As well as reinforcing the importance of adopting a multistakeholder toolkit approach, these experiences demonstrate the importance of founding the fight against spam on laws that prohibit sending commercial email without the prior consent of the intended recipients, and that provide significant penalties for engaging in spamming activities.

- The actions that we take within Canada to reduce the amount of spam will only have a limited effect on the amount of spam arriving in Canadians' email inboxes, unless these actions are complemented and reinforced by strong, effective international cooperative actions against spammers.
- Canada has an opportunity to lead in the growing international fight against spam, particularly by helping developing countries adopt a multistakeholder toolkit approach to fighting spam and adapt it to their own needs and capabilities.

We therefore recommend the following:

Recommendation 18:

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

Recommendation 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.

Recommendation 20:

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

COORDINATING FUTURE ACTION

THE CHALLENGE

Success in implementing Canada's multistakeholder, multifaceted strategy for combatting spam and related threats to Internet security requires a highly synchronized, coordinated approach to spam prevention and enforcement. In enforcement, in particular, the work of the Task Force on Spam has revealed the need for more effective communications, cooperation and collaboration, as there are many law enforcement and regulatory bodies, each with partial responsibility for fighting spam.

The toolkit approach was adopted because of the complex nature of the spam problem. This complexity will not change after the Task Force completes its mandate. Going forward, the government and other stakeholders will face the same set of challenges that led to the establishment of the Task Force. Examples of these challenges include the following:

- There will be continuing issues surrounding the enforcement of anti-spam laws, including coordination between different agencies and different jurisdictions, the need for adequate technical expertise to conduct investigations and the availability of dedicated resources to successfully prosecute perpetrators.
- ISPs and other network operators will have a continued need to share information on best practices and effective strategies to counter emerging threats, as well as to develop sound metrics to measure the scope of the spam problem in Canada and the effectiveness of anti-spam measures.

- Canada's Internet users will have an ongoing need for reliable, accurate information on how to protect themselves from spam and the deceptive, malicious and fraudulent practices associated with spam. They will also continue to need a focal point where complaints can be made through a simple process.
- There will be a continuing and increasing need to coordinate participation by Canadian stakeholders in the international fight against spam.

Task Force Actions

Taking into account its own experience and the experiences of other countries, the Task Force on Spam came to the conclusion that, in order to respond successfully to spam-related challenges, the Government of Canada must establish or designate a focal point or centre to lead the fight against spam and related threats. This centre should be responsible for two main functions: policy oversight and coordination, and support to enforcement agencies.

To be an effective focal point for ongoing policy development and coordination, the Task Force believes the centre should have the mandate and resources to:

- develop policy approaches to deal with the issue of spam and related threats — including through monitoring and analyzing issues, and maintaining ongoing consultations with key stakeholders;

We therefore recommend the following:

Recommendation 21:

In order to carry forward the multi-faceted, 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.

Recommendation 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.

Network and Technology Management

Co-chairs

Tom Copeland, President, Canadian Association of Internet Providers
Lori Assheton-Smith, Senior Vice-President and General Counsel, Canadian Cable
Telecommunications Association

Member Organizations

Allstream
AOL Canada
Bell Canada
BorderWare Technologies Inc.
Canadian Coalition Against Unsolicited Commercial Email
Canadian Internet Registration Authority
Canadian Wireless Telecommunications Association
CANARIE Inc.
Chief Information Office, Industry Canada
CipherTrust
Cogeco Cable Inc.
Delta Cable Communications
E-Gate Communications Inc.
easyDNS Technologies Inc.
Group Telecom
Interlink Connectivity
Internet Light and Power
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
LinuxMagic
MessageLabs Americas
Microsoft Canada
Nortel Networks
PhoneBusters
Rogers Communications Inc.
SecuritySage Inc.
Shaw Communications Inc.
Spamhaus
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
TELUS Communications Inc.
University of British Columbia
University of Manitoba
Videotron Telecom Ltd.
Vircom Inc.

Validating Commercial Email

Co-chairs

Neil Schwartzman, Chair, Canadian Coalition Against Unsolicited Commercial Email
Amanda Maltby, Senior Vice President, Ipsos-Reid Public Affairs, Representing the Canadian Marketing Association

Member Organizations

24/7 Canada Inc.
AOL Canada
Bell Canada
Canadian Cable Telecommunications Association
Canadian Marketing Association
Cornerstone Group of Companies
Daemon Defense Systems
Digital Cement
Doubleclick
eBay Inc.
ICT Standards Advisory Council of Canada (ISACC)
Information Technology Association of Canada
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
MS Planners
Office of Consumer Affairs, Industry Canada
Partners Inc.
Rogers Communications Inc.
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
Technology Surveys International

Public Education and Awareness

Co-chairs

Suzanne Morin, Assistant General Counsel, Regulatory Law and Policy, Bell Canada
Geneviève Reed, Head of Research and Representation, Option consommateurs

Member Organizations

Bell Canada
Canadian Association of Internet Providers
Canadian Coalition Against Unsolicited Commercial Email
Canadian Internet Policy and Public Interest Clinic
Chief Information Office, Industry Canada
Competition Bureau
Consumers Council of Canada
Information Technology Association of Canada
Media Awareness Network
Office of Consumer Affairs, Industry Canada
Office of the Privacy Commissioner of Canada
Openface Internet Inc.
Public Interest Advocacy Centre
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
The Canadian Chamber of Commerce
Union des consommateurs

International Collaboration

Co-chairs

Bernard Courtois, President, Information Technology Association of Canada
Michael Geist, Canadian Research Chair in Internet and E-Commerce Law, University of Ottawa

Member Organizations

Bell Canada
Competition Bureau
Department of Communications, Information Technology and the Arts, Australia
Department of Trade and Industry, United Kingdom
European Commission
LinuxMagic
Microsoft Canada
Organisation for Economic Co-operation and Development
Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
The Canadian Chamber of Commerce

Task Force Secretariat

Spectrum, Information Technologies and Telecommunications Sector, Industry Canada

Richard Simpson, Director General, Electronic Commerce Branch
Shari Scott, Director, Electronic Commerce Branch
David Charter, Electronic Commerce Branch
G rard Desroches, Electronic Commerce Branch
Peter Ferguson, Electronic Commerce Branch
Lisa Foley, Electronic Commerce Branch
Angie Forte, Electronic Commerce Branch
Jennifer Kealey, Electronic Commerce Branch
Serge Presseau, Electronic Commerce Branch
Howard Chatterton, Spectrum Engineering Branch
David Gibson, Spectrum Engineering Branch

Don MacLean, MacLean Consulting, Report Author
John Levine, Glossary Author and Technical Editor

APPENDIX B

RECOMMENDED BEST PRACTICES FOR INTERNET SERVICE PROVIDERS AND OTHER NETWORK OPERATORS



Background

In August 2004, the Working Group on Technology and Network Management started developing a number of technical best practices that would contribute to the reduction of email spam. The Working Group's mandate represents a continuation of the efforts and progress that have been under way for some time, in Canada and internationally, including the work of the Anti-Spam Technical Alliance (ASTA) and the Messaging Anti-Abuse Working Group (MAAWG), and the efforts of various industry associations. A number of different ISPs, other network operators, technical groups and forums have been working collaboratively for many months to share best practices for reducing spam.

The Working Group on Technology and Network Management did not try to redo work that had already been done. Rather, it sought to bring the various industry groups together to share the results of work already under way, and to encourage the broad adoption of best practices among ISPs, other network operators and large enterprise users.

The Working Group emphasizes that the widespread adoption of these best practices will not, in and of themselves, constitute a comprehensive solution to spam. They are, however, part of a broader, multi-prong strategy for addressing the problem of spam.

Intent

The Working Group's recommendations for best industry practices to combat spam are voluntary. The actual time frames for their implementation may vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges. In some cases, alternative solutions may achieve the same objectives outlined in the recommendations. The selection of solutions is at the discretion of the provider/operator.

The Working Group supports all efforts to combat spam. Flexibility in the implementation of the recommended best practices is the key to achieving their broad and meaningful adoption by service providers of all sizes. Because of the technical nature of these recommendations, and the rapid pace of technological change, the Working Group is strongly of the view that these recommended best practices should not be codified as mandatory requirements.

Recommended Best Practices and Rationales

Following are the recommended anti-spam best practices for Canadian Internet service providers and other network operators, as well as a rationale for each recommendation.

1. All Canadian registrants and hosts of domain names should publish Sender Policy Framework (SPF) information in their respective domain name server zone files as soon as possible.

The purpose of email-sender authentication is to reduce domain-name spoofing in email, thereby reducing the incidence of spamming and phishing attempts.

Methods of sender authentication are continuing to be evaluated by the Internet Engineering Task Force (IETF). At this point in time, the SPF classic (SPFv1) proposal is the most technically mature and widely deployed sender-authentication scheme.

This recommendation does not preclude the use of other methods to authenticate email messages (e.g. sender ID, domain keys, SPF, identified Internet mail, etc.). Standards will continue to develop within the industry.

2. ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive mail over port 25 should be restricted to hosts on the provider's network. Use of port 25 by end-users should be permitted on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.

Most ISPs and other network operators agree that there is no practical reason for dial-up / dynamic IP-address ranges to have email servers at the customer end.

There are a variety of ways to avoid this. Through their own network management, ISPs and other network operators can block the use of port 25 on an egress basis.

It has been the experience of members of the Working Group that blocking port 25 affects very few users, and that these users can usually be accommodated in other ways.

The benefits of blocking port 25 are frequently dramatic — some ISPs have seen a 95-percent drop in virus emissions, a 98-percent drop in abuse reports, a reduction in internal viruses / compromised machines used to send spam and attendant cost savings in abuse-related network management.

3. ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.

Many viruses and worms are carried by file attachments. Blocking email containing problematic attachments would have little impact on users. The most common file extensions carrying a payload are: .pif, .scr, .exe and .vbs.

Many ISPs and other network operators should filter attachments based on their properties (i.e. infections) versus extension names. This is a matter of resource availability. Since some business or technical users may have legitimate reasons for sending .exe or .vbs files, filtering for content may be more efficient than filtering for extension names.

4. ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.

Monitoring and possibly rate-limiting the amount of email that can be sent from a particular user would be useful in discouraging spammers from using provider networks as their launching points. It would also provide an early indication of the possible infection of user machines.

Some providers currently do a limited amount of rate-limiting. Techniques will vary depending on the email server in use.

5. ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.

Using viruses, worms and malicious software, hackers and spammers have intentionally deposited millions of “back-door” open relays and proxies on the personal computers of unsuspecting users. The spammer community uses this network of compromised devices to generate billions of unsolicited email messages. In addition, hackers have used this network of devices to mount distributed denial of service (DDoS) attacks on websites, register fraudulent accounts and lay the groundwork for future anonymous hacking activities.

There are a number of methods that can be used to address compromised devices, from suspending client accounts to isolation or quarantine from the network.

6. ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators’ incident reports.

The Working Group on Technology and Network Management is developing a list of ISPs and other operator contacts. It would be beneficial for operators to have common response expectations when reporting incidents of significant network abuse to other network operators. Escalation processes within companies would remain a proprietary process, but initial intercompany communications need a common “estimated time to recovery.”

7. ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.

This is to ensure that subscribers are well aware of their ISPs’, other network operators’, and/or enterprise email providers’ security policies and procedures. It will be particularly important to relay information related to recommendations #2, #3 and #5.

Another Task Force working group, the Working Group on Public Education and Awareness, has developed a multistakeholder public information and awareness campaign to educate, most specifically, Canadian end-users about what they can do to limit the amount of unwanted commercial email they receive.

8. ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).

Email validation would ensure that only authenticated clients are allowed to send email via the server. For example, SMTP authentication is an enhancement to SMTP servers to enable them to verify the identity of email clients. The protocol works by requesting the user name and password of the email sender and validating this against preregistered clients. This procedure can be used to reduce spam messages, since these messages are unlikely to be from registered users in the SMTP authorization list.

9. Non-delivery notices (NDNs) should only be sent for legitimate emails.

Message transfer agent (MTA) administrators and spam-filter manufacturers have now generally accepted this practice. When a message is sent to a nonexistent user account, the MTA responds stating that the user does not exist. This can cause problems when a spammer spoofs a large number of addresses from a domain. Each nonexistent address generates a non-delivery response from the mail server. The MTA software should be configured not to send non-delivery messages for spoofed addresses.

Blanket cessation of NDNs may, however, create some problems for users who, for example, have mistyped an email address and are assuming that the message reached its destination.

10. ISPs and other network operators should ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.

Identifying the points of contact for ISPs and network operators is crucial for managing the abuse of email communication systems. All email messages include information such as DNS host names, IP addresses and other records relating to the source, transmission and destination of the message. The ISPs or other network operators responsible for sources of the email messages should be easily and accurately identifiable. All fully qualified domain names (e.g. hostname.domainname.ca), domain names and IP addresses should be registered and maintained with information allowing such identification.

Network operators should also ensure that domain name records; forward and reverse DNS records; and WHOIS, shared WHOIS Project (i.e. SWIP) or referral WHOIS (i.e. RWHOIS) records are responsibly maintained with correct, complete and current information. For example, American Registry for Internet Numbers WHOIS records should include an OrgAbuseHandle including contact information for those responsible for managing abuse originating in that network. ISPs and network operators are responsible for maintaining registration information, DNS records and other identifying information in accordance with the relevant Request for Comments (RFCs) such as RFC 2142 — Mailbox Names for Common Services, Roles and Functions.

11. ISPs and other network operators should ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries. All local area network (LAN) operators should be compliant with Request for Comments (RFCs) 1918 — “Address Allocation for Private Internets.” In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.

Forged email-header information is common in spam and email malware. Ensuring that all publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS, WHOIS and SWIP registration records is very important for being able to identify the sources of email and other online communication methods. Identification of the source provides the information required to contact the responsible ISPs or other network operators, so that they can take appropriate actions to address spam or other concerns involving protocol. IP addresses registered to another organization should not be used within private networks, as their use can significantly complicate efforts to identify the ISPs and network operators responsible for an email message. DNS host names may also be used by recipients to determine access policy, but should be chosen carefully in order to avoid recipients choosing overly broad filtering policies that have the potential to block valid email. Please see Recommendation #10 regarding recommendations for maintaining correct, complete and current information.

To assist with identification of email sources, it is also suggested that email servers should have DNS host names that clearly differentiate these servers from consumer or business desktop addresses. Host names should exist and match in both forward (resolution of host name to IP address) and reverse (resolution of IP address to host name) DNS entries. ISP customers who are permitted by policy to operate email or other servers will benefit from this by having the ability to operate customized forward and reverse DNS within their domains, thus distinguishing hosts from residential or policy-prohibited hosts. This lets email recipients establish systems that differentiate between legitimate email servers and hosts that may be sources of spam.

Residential, dynamic or policy-restricted IP addresses should also have a clear and consistent forward and reverse DNS naming convention. For example, access-control policies enacted by email recipients which differentiate between trusted and untrusted email sources are easier to establish for naming conventions that include the domain owner; service class; static or dynamic assignment; and other identifiers, such as an IP-pool identification. This can prevent ISP customers who are permitted to run email servers from being blocked due to their being indistinguishable from illegitimate email sources. Naming conventions with a “most-significant-to-the-right” scheme simplify filters and reduce the likelihood of access-control policies affecting legitimate email sources. For example, such a naming convention for the residential, dynamic IP address “1.2.3.4” at ISP Example.ca would be “4-3-2-1.dyn.res.example.ca.” A sample naming convention for the small business, static IP address “1.2.3.4” at ISP Example.ca would be “4-3-2-1.static.bus.example.ca.” A sample naming convention for an email server used by Smallbizcustomer.ca would be “mail.smallbizcustomer.ca.”

12. ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822, and reference domains and IP addresses should have up-to-date, accurate registration information.

Accurate email-header information is important for ISPs and other network operators to be able to identify sources of spam and email malware within an ISP's network. Please see Recommendation #10 regarding recommendations for maintaining correct, complete and current information.

While internal networks will often use private IP addresses (as per RFC 1918 — Address Allocation for Private Internets) that are not externally routable or identifiable, email providers should ensure that the sources of email messages are accurately identifiable for policy- and law-enforcement purposes.

Conclusion

Spam is a multifaceted, global problem that requires coordinated action on several fronts in order to achieve real and measurable progress. Implementing these recommendations can help reduce many of the worst types of spam, forgery and spoofing that occur in email. These measures will not stop spam entirely, but will significantly enhance the Internet community's ability to trace the sources of spam and hold senders accountable for their actions. The recommendations are also expected to provide the foundation on which future solutions can be built.

APPENDIX C

RECOMMENDED BEST PRACTICES FOR EMAIL MARKETING



Background

As part of the federal government's Task Force on Spam, the Working Group on Validating Commercial Email has developed a set of best practices for email marketing. These best practices will help Canadian organizations adopt spam-free marketing techniques and will make it clear that spam plays no legitimate role in Canadian marketing.

Most responsible organizations already follow industry codes or have adopted best practices. In Canada, organizations are guided by the Canadian Marketing Association's *Code of Ethics and Standards of Practice*, which includes guidelines for email marketing and the online collection of data for marketing purposes. Members of Canadian Survey Research Council organizations that conduct online surveys are also developing a uniform code of practice.

This document brings together a set of best practices drawing upon existing codes in order to provide all with a basis to using email for commercial or marketing purposes.

Increasingly, Internet service providers (ISPs) and email service providers (ESPs) are looking for ways to stop spam by using filtering, black and white lists. As a result, they are inadvertently blocking legitimate email messages before they reach their intended recipients. Organizations are encouraged to adopt the best practices cited here as a way to ensure that their own legitimate email messages reach their intended recipients.

These best practices are not legally binding, but are intended to complement existing Canadian laws that govern spam, privacy, email marketing and marketing to children. For example, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into full force throughout Canada in January 2004, establishes the obligations of those who collect, use and disclose personal electronic-mail addresses. Other relevant federal acts include the *Competition Act*, the *Telecommunications Act* and the *Criminal Code* of Canada. Organizations should make themselves aware of these laws and govern their activities accordingly.

The best practices, along with explanatory notes and illustrative examples, are outlined in the following sections.

Recommended Best Practices

1. Marketing email should only be sent to recipients who have provided their consent to receive such information.

This best practice directly relates to the sending of unsolicited commercial email for the purposes of soliciting goods and/or services. If organizations have not obtained the express consent of recipients prior to sending these types of email messages, then they are sending spam.

If the organization has an existing business relationship (see glossary) with the intended recipient, it is sufficient to rely on implied consent. Under existing Canadian law, where an individual has entered a contest, made a donation, or registered online for a product, newsletter, etc.; has provided their email address as part of the transaction; and has been provided with the opportunity to opt out of receiving further marketing email messages, and has not done so, the organization has the implied consent to

email the individual. When using this form of consent, the marketer should explain to the intended recipient why they are receiving the email. In the follow-up communications, the organization must provide the individual with an opportunity to opt out of receiving further marketing emails (see Best Practice #2).

Organizations should not send email marketing messages to recipients who have indicated they do not wish to receive email messages from the organization. While an organization may send email messages during an existing business relationship, they must honour an individual's request to be removed from email marketing lists at any time. This can be accomplished by providing an opt-out opportunity in every message sent (see Best Practice #2).

There is an exception for sending email messages outside of an existing business relationship, or to a customer whose file has become inactive. If the organization has service, warranty or product-upgrade information, or if there are health and safety issues related to a product purchase, the organization may send email messages to its customers. Organizations should use discretion in doing so, however, as customers may view this email as spam if the organization uses it as an opportunity to up-sell or cross-sell products.

2. In all marketing email, recipients must be provided with an obvious, clear and efficient email or web-based means to opt out of receiving any further business and/or marketing email messages from the organization.

In all email messages to current customers, organizations must include an opportunity for the recipient to opt out. This opportunity should not be buried in the email message and must, at minimum, be website- and/or email-enabled. The language used should be as simple as: "If you no longer wish to receive marketing offers from this organization, please **click here** or email **info@ABCcompany.com.**"

The process for opting out should be simple and straightforward, and organizations should confirm by email that the opt-out request has been or will be followed through without requiring further action by the consumer.

In Canada, the industry best practice for telephone or mail do-not-contact files is to honour opt-out requests for a three-year period. After that time, organizations may re-contact individuals with marketing offers. However, because of the sensitivities associated with email communications, and the problems caused by spam, organizations should honour an email opt-out request as final and remove that individual from their marketing lists until such time as the individual opts to receive email messages again.

3. The internal process used to obtain consent should be clear and transparent. Organizations should keep records of the type of consent obtained from recipients so that email lists can be scrubbed prior to campaign broadcasts.

Organizations should ensure that they have the means to honour opt-out requests on a timely basis and to scrub their lists accordingly.

In addition, an internal process should be in place that records proof of consent, including the date, time, originating Internet protocol (IP) address and location (including URL), where the address collection occurred and whether consent was obtained via another medium (e.g. business card, contest form, telephone, verbal communication or credit card [e.g. through a paying subscription to a list]). Organizations should be able to provide this information to a recipient upon request.

4. Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.

The identification of the sender and source of the email should be clearly and obviously specified and, whenever possible, placed above the fold (that part of the email that is visible without scrolling).

Example #1: Direct from organization to subscriber

```
Date: Tue, 5 Oct 2004 07:32:02 -0400
From: Bell Canada - Electronic bill <bill.presentment@bell.ca>
To: JOE CONSUMER<joe@consumer.ca>
Subject: Your Bell e-bill is ready / Votre facture électronique est prête
```

Example #2: Third-party email service provider to subscriber on behalf of an organization

```
From: "peteMOSS PUBLICATIONS <bounces@peteMOSS.com>"
<v2user-13990-IXoyuP..CahrNet_0bkttg@mailier.whitehat.com>
Subject: spamNEWS 07/21/04
To: <joe@consumer.ca>
Date: Sat, 24 Jul 2004 18:50:17 -0700
```

Even in cases where the content is accurately related to the subject line, organizations are cautioned against using subject lines that refer to “free offers” or “winning prizes.” This is, in part, due to the fact that some spam filters use keywords such as these to signal that the message is spam.

Email messages should include the sender’s main postal address. Canadian organizations are strongly encouraged to become familiar with the provisions in Canadian laws that address this issue, and with the related laws of other jurisdictions, such as Australia, the United States and the European Union.

5. Every email should provide a link to the sender’s privacy policy. The privacy policy should explain the intended use and disclosure of any personal information that might be gathered through “clickstream” means or other website monitoring techniques.

Organizations are obliged under PIPEDA to adopt a significant degree of transparency in disclosing their personal-information gathering and handling practices. A privacy policy might include the type of information collected and/or used; whether information is disclosed to third parties; the use of “cookies” or other passive means of data collection; and security, accountability and enforcement procedures.

Organizations must make the information on their online information-gathering processes readily available in one comprehensive privacy policy on their websites. The privacy policy should also include an active link to an opt-out mechanism.

6. Marketers, list brokers and list owners should take reasonable steps to ensure that the addresses on their email lists were obtained with the proper consent.

Organizations, list brokers and list owners should share responsibility for sending email to recipients who have not given appropriate consent to receive these messages. Where an organization, list broker or list owner knew or should have known that the proper consent was not obtained, they could be accountable. Some examples of reasonable steps that an organization can take to ensure clean lists include:

- reviewing the privacy policy of the broker/owner of the list;
- reviewing the opt-in procedures used to obtain the email addresses;
- having the broker or owner sign a contract warranting that they have complied with the requirements of PIPEDA (see the sample at the end of this appendix).

7. Marketers should use a high degree of discretion and sensitivity in sending email marketing to persons under the age of majority, in order to address the age, knowledge, sophistication and maturity of this audience.

Organizations should refer to both the Canadian Marketing Association’s Special Considerations in Marketing to Children and Teenagers, from its *Code of Ethics and Standards of Practice* (www.the-cma.org/consumer/ethics.cfm), and existing Canadian laws (see www.justice.gc.ca) for guidance on this issue.

The ways in which those under the age of majority perceive and react to email marketing communications are influenced by their age and experience, and the context in which the message is framed. For example, email marketing communications that are acceptable for teenagers will not necessarily be acceptable for younger children. There is no way to guarantee the age of any person who signs up to an email subscriber list. Organizations should, therefore, use discretion and sensitivity when marketing to those under the age of majority, and should seek to engage parental permission in such communications.

8. (a) When the content of an email is adult in nature the sender must — prior to sending the communication — verify that the recipient is of age to legally receive and view such content.

Adult content includes material of a sexually explicit nature and material related to gaming and gambling, tobacco, alcohol, firearms and other weapons.

(b) All email containing sexually explicit content should include the prefacing tag “SEXUALLY EXPLICIT” in the subject line.

For example, the subscriber may be required to provide a telephone number so the organization can verify that the recipient is of the age of majority. It is important to note that contracts with minors are not enforceable.

9. Organizations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.

Any complaints from individuals regarding the use of their email address should be dealt with courteously and within a reasonable time frame.

10. Organizations may disclose the email addresses of existing customers to third-party affiliates or within a family of companies if:

- (i) they have consent to do so;
- (ii) they are using the addresses for purposes consistent with their collection (i.e. for marketing related to the original purchase or to provide services related to that purchase);
- (iii) it is transparent to the recipient why they are receiving email communications; and
- (iv) there is an easy-to-use way to opt out of receiving further email communications.

Organizations may only disclose customers’ email addresses to an affiliated third party or within a family of companies for cross-marketing purposes if they offer these customers an easy-to-use opt-out opportunity before disclosing the email address.

It must be transparent to customers why they are receiving additional, related marketing offers (e.g. under a company brand). The organization should not assume that customers understand a corporate relationship or structure.

For further guidance, organizations are advised to follow the best practices established by the Canadian Marketing Association in its *Code of Ethics and Standards of Practice* under Section E4.1.3 of the *E-mail Marketing Communications* compliance guide. The section states that “an individual’s email address may not be disclosed to any third party (e.g. list rental company) without the express consent (more commonly known as opt-in or positive consent) of the individual. If you want to disclose email addresses to marketing partners or list brokers, you must obtain positive consent. Similarly, you need to ensure appropriate permission for the use of any email addresses your company may have acquired from others.”

The CMA defines a “third party” as follows:

“Third party” refers to an organization corporately distinct from that with which the customer originally did business (list rental company), including an organization corporately related to the original organizations (or charity) or part of the same group, where the relationship would not be apparent to the customer. Third parties do not include data processors operating on behalf of the organization with whom the individual has established a business relationship.

Technical Tips for Electronic Marketers

1. Sending parties should implement the following standard technical specifications:

- All servers (e.g. inbound, outbound, websites) must have reverse Domain Name System pointer (rDNS PTR) entries in DNS records, the forward and reverse DNS lookups for the host must match, and the sending machines should HELO/EHLO with this name.
- Sender Policy Framework (SPF) (e.g. <http://spf.pobox.com>) and domain-key (e.g. <http://antispam.yahoo.com/domainkeys>) records should be published by the senders and third-party sites associated with a mailing (e.g. websites, ESPs, etc.) and kept current at all times. Adoption of technologies that are similar in nature should be considered as they develop and become standardized.
- IP addresses that are distinct from other site servers should be assigned to outbound mail servers.
- WHOIS database records for all sender domains must be kept accurate and complete.
- Role accounts (e.g. postmaster@ and abuse@) must be functional and actively monitored for all sender domains, including websites, referenced in email content.

2. Senders must attend to bounce messages as follows:

- They must promptly remove “hard” (5xx — No such user / Mailbox unavailable, etc.) bounced addresses from all lists under their control when the total number of refusals surpasses three or more in fourteen days. If a 5xx bounce indicates spam blocking, the address may be reactivated if the spam block is removed.
- They must remove “soft” (4xx — Transient failures) bounced addresses when the total number of refusals surpasses five in consecutive campaigns from a single list, or five in aggregate from several lists within ten days.

Bounce-handling policies are explained in depth at the following sites:

- <http://help.yahoo.com/help/us/mail/defer>
- www.isipp.com/standards.php
- <http://postmaster.info.aol.com/guidelines/bestprac.html>

3. Web bugs (hidden HTML elements) and return receipts are inaccurate ways to determine open rate statistics for campaigns. Senders are strongly encouraged to cease using them and adopt alternative performance metrics.

Web bugs or web beacons have become extremely inaccurate as measurements for the effectiveness of email campaigns, and their use is discouraged.

Web beacons are no longer reliably accurate for several reasons, which mainly involve technical changes in popular client email software (e.g. as part of its antivirus security measures, Outlook will no longer download such items by default or show them in the preview pane). There is also increased use of client-side antivirus software, which, by default, disallows web-beacon downloading.

Relying on 1x1 pixel, white-on-white graphic elements as a way to measure open rates is also discouraged. The use of user click-throughs of encoded, embedded URLs and other forms of measuring subscriber actions (e.g. returns on investments, purchase actions) is advised.

If senders are going to use web beacons, the privacy implications raised in studies such as the one published by the Network Advertising Initiative (www.networkadvertising.org/Web_Beacons_11-1-04.pdf) should be seriously considered, and the conditions set out therein should be implemented.

Currently, one of the best measurements to look at when assessing the success of an email program is subscriber retention — that is, how many people continue to subscribe after each email. Clearly, the goal is to have no unsubscribers, which would indicate that the organization is providing content that is timely, relevant and valued. In turn, these benefits build loyalty and trust among customers — a good thing for any organization.

Sample Letter of Compliance with the Personal Information Protection and Electronic Documents Act

List Name: _____

As a leader in list brokerage services, **ABCcompany** takes pride in its commitment to protecting consumer privacy and ensuring compliance with applicable legislation, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA). We are, therefore, taking this opportunity to update the information we have about the list referenced above.

A Review of PIPEDA and Consumer Privacy

PIPEDA addresses consumer records only (those going to a home address). Among other things, the legislation states that consumers on a list must have provided their consent (opt-in) for the collection of their personal information and its disclosure to outside parties for marketing and/or communications purposes. Additionally, it mandates that name-removal options (opt-out) available to consumers be put into effect prior to consumers' names being released for marketing purposes.

What We Need

Increasingly, mailers are asking for specific information about the privacy messaging being used by list owners. Accordingly, we need to have the following information on record to ensure that orders are processed expediently.

Please provide a sample copy of the consent form or name-removal option currently in use. We will keep a copy on file for future reference for potential and repeat uses of this list.

Please check one of the boxes below, then sign, date and return this document to the attention of **ABCcompany** at fax number (XXX) XXX-XXXX. Please contact our XXXXXXXXX department at (XXX) XXX-XXXX or info@ABCcompany.com with any questions.

[] I warrant and represent that this list IS COMPLIANT with PIPEDA. My organization has obtained consent from all consumers on this list to collect their personal information and disclose it to outside parties for marketing and/or communication purposes, and has ensured that name-removal options are available to consumers prior to these consumers' names being released for marketing purposes. My organization shall comply with all legislation, provincial and federal, pertaining to the protection of personal information that may come into force from this date forward, as it applies to personal information collected, used or disclosed by my organization.

[] I warrant and represent that this list IS NOT COMPLIANT with PIPEDA. My organization has not obtained consent from all consumers on this list to collect their personal information and disclose it to outside parties for marketing and/or communication purposes, and/or has not ensured that name-removal options are available to consumers prior to these consumers' names being released for marketing purposes.



APPENDIX D

THREE KEY TIPS FOR COMBATTING SPAM

Spam refers to unsolicited email, mostly commercial, advertising a product or service that is mass mailed to thousands of email addresses at a time, filling people's inboxes. Spam does not refer to legitimate commercial email for which consumers have given their consent. Spam is often a source of scams, viruses and offensive content.

Spam is a major problem that takes up valuable time and increases costs for consumers, business and governments. Each of us must do our part to protect ourselves and others from spam. **Canada's Task Force on Spam** has developed these three tips to help you protect yourself and fight spam.



Stop Spam Here: Three Key Tips

1. Protect your computer

Spam is a growing source of computer viruses. It is critical that you protect your computer from virus-carrying messages. Install and regularly update antivirus and anti-spam software. If you don't have the extra protection of a firewall, get it.

2. Protect your email address

Reserve one email for your trusted personal and business contacts. Create a separate, expendable email address for other online uses.

3. Protect yourself

Don't try, don't buy and don't reply to spam. Just delete it. It's a great way to prevent receiving more spam in the future.

1. Protect your computer

Shield your computer with anti-spam and antivirus programs, and other security software.

Anti-spam software can automatically scan your email for spam before it gets to your inbox, sending it to a junk email box instead. This prevents you or a family member from inadvertently opening spam messages, and helps you manage your email more effectively.

To protect against virus-laden spam emails and attachments, install security patches and antivirus programs on your operating system and update them regularly.

A firewall provides added protection from hackers by protecting your privacy and personal information.

Never go online with any computer before it has had anti-spam, antivirus and firewall protection installed.

Always question the source.

Never open attachments unless you are expecting them from someone you trust. Spammers can hijack the personal and corporate email accounts of others — a process known as "spoofing" — to send viruses that can corrupt your computer. If you are in doubt about an attachment, verify with the sender before opening it.



Don't let your computer become a spam zombie.

Without the system protection listed here, your computer could be infected with viruses that are programmed to create gateways (known technically as *proxies*) that relay spam to other email recipients. In severe cases, your Internet service provider (ISP) may have to shut down your account. An infected computer can cost hundreds — or even thousands — of dollars to repair.

When completing a session on the Internet, it is a good idea to disconnect from the Internet and shut down your system. Spammers are increasingly seeking out and exploiting unprotected home computers with high-speed Internet connections to use as “spam zombies.”

2. Protect your email address

Manage your online risks.

Use separate email addresses for different online activities: create one email address and share it *only* with trusted personal and business contacts. Create expendable email addresses for other online activities. If these email addresses become clogged with spam, discard them.

Select an email address consisting of a combination of letters and numbers. By choosing a more complex email address, you are making it more difficult for spammers to randomly discover and fill your email account using software that randomly combines people's first and last names.

Stay under cover.

Posting your email address anywhere on the Internet will attract spam. Share your email addresses *only* with people you know and trust.

Spammers collect email addresses using programs such as spiders, crawlers and bots that search the Internet for email addresses to add to their lists.

If you are swamped with spam, change your email address.

3. Protect yourself

Just delete it.

Don't try, don't buy and don't reply. Never visit websites or buy anything advertised in a spam message. Spam is almost always a scam. *Just delete it.*

Don't respond.

Never open, reply to or click on the “remove” or “unsubscribe” link in a spam message. These actions can confirm your email address, causing you to receive more spam.

Don't let spammers hook you like a "phish." Protect your personal information.

Spammers can reel in your valuable personal information through a practice known as "phishing." This occurs when an email shows up appearing to come from a reliable source with which you do business, like a bank or online business. Often the message suggests that there is an urgent need for you to provide personal information, such as your log-in name, passwords or even credit card numbers, often combined with the faked threat that your account will be blocked if you do not comply. In these cases, the website link provided is to a copycat, but counterfeited site. Be aware that companies will NEVER contact customers in this manner. If you have doubts, don't trust the information supplied in the email, call the company to confirm if the request is legitimate. Also, never reply to these messages or connect through the link provided in a spam that you suspect is "phishing." If you are interested in a website, access it directly through a web browser.



APPENDIX E

BACKGROUND REPORTS AND WORKING PAPERS



The following documents provide background and supplementary material on the work of the Task Force on Spam and on the conclusions of the working groups. These documents are available at www.e-com.ic.gc.ca.

General

- An Anti-Spam Action Plan for Canada — *Canada Gazette* Notice Summary of Submissions
- Task Force on Spam: Roundtable Meeting with Key Stakeholders
- Task Force on Spam Online Public Consultation Forum Summary of Contributions

Working Group Documents

- Anti-Spam Technology Overview
- Canadian Spam Database Concept Document
- Companion Document to *Recommended Best Practices for Internet Service Providers and Other Network Operators*
- Working Group on Legislation and Enforcement Conclusions

Background Papers

- A Statutory Private Right of Action Against Spammers in Canada
- Assessment of Email Certification
- Overview of Wireless Spam Issues in Canada
- Proposal for the Canadian Anti-Spam Action Centre
- International Spam Measures Compared

GLOSSARY

Address harvesting

The collection of lists of email addresses by automated means from websites or other online sources.

Black list

A list of IP addresses, domains or email addresses from which email is not accepted. The most common form of black list is a Domain Name System black list (DNSBL), a list of IP addresses distributed via the Internet's DNS. Popular DNSBLs include the Spamhaus Black List (SBL), the Composite Black List (CBL) and the original DNSBL, called the Mail Abuse Prevention System (MAPS) Reverse Black List (RBL). Contrast this with "white list."

Botnet

A collection of "zombies" used to send spam or for another purpose. A single botnet often contains hundreds or thousands of computers.

Bounces

The process of rejecting the attempted delivery of an email message. Sometimes a stylized "bounce report" email message reports that a previous message couldn't be delivered.

A bounce may be a "soft bounce," in which case the sending computer can retry the delivery later, or a "hard bounce," in which case the delivery is a failure.

A soft bounce may occur because the recipient's mailbox is full, the server is overloaded or there are other temporary problems. A hard bounce most often occurs because the recipient address is invalid or the recipient host, by policy, rejects mail from that sender.

Clickstream

The series of mouse clicks and related actions that a user makes while visiting a website. For an e-commerce website, a clickstream might include browsing the catalog, putting items into a virtual shopping cart, providing payment and shipping information, and then entering the order.

Cookie

A small data file created by a web server and stored on a user's computer. Cookies are a way for websites to identify users, keep track of users' preferences and recognize users who are revisiting the website. By keeping user histories, cookies let websites tailor pages and create custom experiences for individuals. Depending on how the web server is programmed, cookies may also contain personal information, such as site passwords and account numbers.

First-party cookies are ones created by the website you are visiting. Third-party cookies are created by a website other than the one you are currently visiting, most often a third-party advertiser on that site. Third-party cookies let advertisers determine whether an individual user is visiting multiple websites that display the advertiser's ads, and are often considered a privacy risk.

Modern web browsers offer options to refuse all cookies, to refuse third-party cookies and/or to accept or refuse cookies from specified websites.

Cross-sell

To encourage a customer to buy a product or service related to one already purchased. Contrast this with “up-sell.”

Denial of service attack

Often abbreviated as DoS or DOS. An attempt to keep a server or network from performing its intended function, by flooding it with unwanted traffic. For example, an attacker could send tens of thousands of email messages to a mail server to overload it and keep it from processing desired mail. Many different DOS attacks and targets are possible, including attacks on mail servers, web servers, DNS servers and network routers. Spam sent in large volume can act as a DOS attack on mail servers.

Dictionary attack

An email-address guessing technique. The attacker tries to deliver email to a large number of made-up addresses, using either words out of a dictionary or letter combinations such as **aaaa@example.ca**, **aaab@example.ca** or **zzzz@example.ca**.

DNS

Domain Name System, the system that lets users locate computers on the Internet by domain name. DNS servers maintain a database of domain names (i.e. host names) and their corresponding IP addresses. For example, if the name **www.mycompany.ca** were presented to a DNS server, the IP address 204.0.8.51 might be returned. The DNS includes several different kinds of data, such as A records for IP addresses and mail exchanges (MXs) for mail servers.

The DNS is distributed among many different servers, with most servers delegating responsibility for names to other servers. In the example above, the Internet Assigned Numbers Authority (IANA), which is responsible for the entire DNS, would delegate all of **.ca** to the Canadian Internet Registration Authority (CIRA), which, in turn, would delegate all of **.mycompany.ca** to the registrant for that name, which, in turn, would operate the DNS servers that have information for **www.mycompany.ca**.

Domain

A name used on the Internet. Domains consist of multiple sections separated by dots, such as **ic.gc.ca** or **www.mycompany.com**.

Domain keys

A technology proposal by Yahoo!® that puts a cryptographic signature on messages, which recipients can verify. This provides a way to verify both that the message was sent from the domain of its email sender and that the message was not altered during transit.

EHLO/HELO identity

The name by which a sending computer identifies itself to a receiving computer at the beginning of each SMTP transaction. The command the sending computer uses to identify itself by this name to the receiving computer is called the “EHLO” or “HELO” command.

Email address

The name by which the sender or recipient of an email is identified. Each address is of the **mailbox@dom.ain** form, where **dom.ain** is a domain name that can be looked up in the DNS, and **mailbox** is an arbitrary identifier used by the domain’s management to identify a mail user.

ESP or email service provider

A company that provides email services to other businesses. ESP services include collecting and maintaining lists of email addresses, sending bulk email to the addresses on the lists, removing addresses that bounce, and dealing with complaints and abuse reports related to the mailings.

Existing business relationship

An existing business relationship exists where:

- 1) the recipient has purchased a product or service from an organization within the past 18 months; and
- 2) the recipient has not unsubscribed or opted out from commercial or promotional email messages, or otherwise terminated the relationship.

An affiliate or third party may not rely on another organization's prior business relationship in order to send commercial or promotional email messages.

Filters

Software used to separate wanted from unwanted email, based on the mail's characteristics.

Filters might check for specific text strings, approximate text patterns, similarity to other messages or other criteria.

Harvesting

Shorthand for "address harvesting."

Header

In Internet email, the initial part of a message, consisting of a series of lines that describe the message. Each header-line starts with a label such as From: or Subject: to identify its meaning. The header is followed by a blank line, and then the body of the message.

HTML

Hypertext markup language, the coding scheme used to format web pages and formatted email messages. HTML uses textual tags, such as <h2>A Topic</h2> to indicate a second-level header, or important text to indicate bold-faced text.

Identity theft

The use of stolen personal information to impersonate someone, generally for financial fraud purposes. An identity theft may involve impersonating a victim to gain access to existing bank accounts or take out bank loans, or for other fraudulent purposes.

IM or instant messaging

Text messages delivered immediately from the sender's computer to recipients. Popular IM systems include AOL® Instant Messenger™, Yahoo!® Messenger and MSN® Messenger.

Implied consent

The Canadian Standards Association Model Code says that "Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual." This covers situations where intended use or disclosure is obvious from the context, and the organization can assume, with little or no risk, that the individual, by providing personal information, is aware of and consents to its intended use or disclosure. (Source: Office of the Privacy Commissioner of Canada fact sheet.)

IP address

Internet protocol address, the number that identifies a computer or other device attached to the Internet. An IP address is usually written as four decimal numbers separated by dots, as in 168.0.1.10.

Malware

A general term for hostile software such as viruses, worms and Trojan Horses.

Marketing email

Email primarily advertising the availability of goods or services. Contrast this with "transactional email."

Opt-in

Also called “express” or “positive consent.” Under this form of consent, commonly referred to as “express consent,” the organization presents an opportunity for the individual to express positive agreement to a stated purpose. Unless the individual takes action to “opt in” to the purpose — in other words, says “yes” to it — the organization does not assume consent. (Source: Office of the Privacy Commissioner of Canada fact sheet.)

Opt-out

Also called “negative consent.” The organization presents the individual with an opportunity to express non-agreement to an identified purpose. Unless the individual takes action to “opt out” of the purpose — that is, say “no” to it — the organization assumes consent and proceeds with the purpose. The individual should be clearly informed that the failure to “opt out” means that the individual is consenting to the proposed use or disclosure of information. (Source: Office of the Privacy Commissioner of Canada fact sheet.)

Phishing

Impersonation of a trusted person or organization in order to steal a person’s personal information, generally for the purpose of “identity theft.” For example, an email message may appear to be from a well-known bank asking recipients to visit a website to confirm their account details, but the website is actually controlled by a hostile party.

Port 25 blocking

Traditionally, every computer on the Internet has had the technical ability to send mail to any other computer. In practice, most ISP customers send their outgoing mail to their ISP’s mail server to be forwarded along to its ultimate recipient. In recent years, the large majority of mail sent directly, rather than via the ISP, has become spam and viruses. Many ISPs now block their customers from sending mail directly, and require it be sent via ISP mail servers, where the ISP can do virus filtering and take other anti-abuse measures. Since transmission control protocol (TCP) assigns each type of service a port number, and email is sent via port 25, this is called “port 25 blocking.”

Blocking port 25 for consumer dial-up and broadband customers is widely considered a best practice.

Port 587 or SUBMIT

An alternative facility many mail systems provide for users to send outgoing mail to the ISP’s mail server. It requires its sending users to authenticate themselves before sending, making SUBMIT much more auditable than port 25 mail. SUBMIT is also sometimes called port 587, after the TCP port number it uses.

rDNS or reverse DNS

Reverse Domain Name System, a service that looks up IP addresses to find domain names. It performs the opposite function of the usual DNS lookup. Reverse DNS is often used to log incoming traffic by domain name for statistical and auditing purposes. It is widely considered a best practice for all mail client and server computers to have accurate rDNS.

Role account

Email accounts that must be in place and maintained by all domains with Internet connectivity, as specified in the Internet Engineering Task Force’s Request for Comments (RFCs) document series. Such accounts include **postmaster@sampledomain.ca**, **abuse@sampledomain.ca** and **hostmaster@sampledomain.ca**.

Sender ID

An authentication scheme, similar to SPF, sponsored by Microsoft. See “SPF.”

Server

A computer that provides one or more services to other computers, such as email, DNS or World Wide Web pages.

Web bug

Also called a web beacon, pixel tag, clear GIF (graphics interchange format) or invisible GIF. A way for an HTML email message's sender to determine if and when the message was opened and read.

West African, 419 or Nigerian scam

An advance-fee fraud in which the perpetrator claims to be an official, typically in West Africa, who wants the victim's help to steal large amounts of money from a government account. Also known as 419 fraud, after the section number of Nigerian law that forbids it.

Before this scam moved to Africa, it was best known as the Spanish Prisoner, in which form it dates from the 1600s.

White list

A list of email addresses or IP addresses from which a mail server is configured to accept incoming mail. White lists can be useful as one part of an email filtering system. Compare this with "black list."

WHOIS

An Internet service used to ask registrars for a domain or network's registration information. It has not been universally implemented.

Worm

"Malware" that spreads directly by copying itself onto other computers through security holes in the other computers' software. The earliest worm used a security flaw in Sun Microsystems' Solaris systems and in VAX systems, but current worms all use flaws in Microsoft Windows. Contrast this with "virus."

Zombie

A computer infected by "malware" so that the computer can be remotely controlled by the creator, distributor or controller of the malware. The majority of spam is currently sent through zombies.

