

Measures to Control Spam and other related threats to the online marketplace

2007

According to the Canadian Internet use Survey for 2005, the vast majority of people use the internet for e-mailing and web browsing. Businesses, in turn, use email for a significant proportion of their core business and communications activities. As such, spam is viewed as a considerable burden not only to consumers, but to the business community. It is not only an irritant, but also causes lost time at work and lost productivity and clogs up network systems. Further, spam often carries more harmful problems, such as viruses, phishing attempts and spyware, which security breaches that entail significant losses to businesses.

What is spam?

Not all unwanted email is spam. While individual consumers may dislike some forms of email, legitimate commercial email, even where unsolicited, allows senders to ask to be removed from the distribution list ("opt out"). It is email where it is not possible for a recipient to communicate with the sender in order to stop the flow of spam – indeed, communicating often increases the problem – that is frequently the most damaging and must be addressed.

Spam may be best defined as unsolicited electronic communication that could not be reasonably assumed to be wanted or expected by the recipient. Spam thus has a personal component, based on the individual's preferences. More importantly, however, the most egregious spam is that which is deceptive or false in content, or is sent for malicious purposes, such as virus distribution. It is this spam which causes security problems for firms, clogs networks reducing the ability of service providers to meet the needs of businesses and consumers. As defined by the Global Business Dialogue for Electronic Commerce, spam is unsolicited electronic communications that included any of the following characteristics:

Absence of consent to receive either via opt-out or opt-in principles

1. Harvesting of personal information
2. False information or claims
3. Intent to defraud
4. Erroneous reply address information

Scope of the Problem in Canada

According to Brightmail, a leading internet security firm, in March 2004, spam accounted for 63% of Internet email. Canada is heavily implicated in spamming, rated within the top ten countries from which spam originates. According to software firm Sophos, Canada is responsible for 6.8% of worldwide spam, second only to the United States (56.74%). Spamhaus, an organisation dedicated to identifying spammers and fighting spam, places Canada as seventh on its list of top ten spamming countries.

Fighting spam necessitates a coordinated approach that includes enforcing legislation as well as educating users.

Recommendations

That the federal government:

1. Work with stakeholders to develop a multifaceted national strategy to address and stop spam and other related online threats as was outlined in the 2005 Canada Task Force Final Report entitled *Stopping Spam: Creating a Stronger, Safer Internet*

2. Implement the recommendations of the Stopping Spam Report that deal specifically with:
 - a) making the internet more secure and addressing the broad range of potential internet harms (ie. spyware, phishing, trojan horse).
 - b) Encourage the adoption and promotion of “best practices” for internet service providers and other network users.
 - c) Pursue bi-lateral international agreements on anti-spam policies and strategies.
3. Work with the provinces and territories to prevent duplication of legislation or approaches.
4. Place a priority on consumer education and awareness and dedicate the appropriate resources to pursue such initiatives.