

## What is Spam?

Spam can be defined as unsolicited communications sent in bulk over an electronic media such as e-mail, mobile (SMS, MMS) and instant messaging services, usually with the objective of marketing products or services.

It is to be noted that there is not a universal definition for spam and the above is based on the Australian and European Union definitions.

In general, spam messages tend to fall into the following categories:

- ✉ Unsolicited commercial advertising;
- ✉ Pornography;
- ✉ Scams or fraud;
- ✉ Propaganda; and
- ✉ Chain letters.

## The Extent Of The Spam Problem

The International Telecommunication Union (ITU) in 2004 estimated that as much as 80% of all e-mail traffic was spam, compared to 35% in 2003, with spammers sending hundreds of millions of messages per day.

The estimated costs of spam to the global economy are approximately US\$25 billion dollars per year.

The problem of spamming is also becoming more and more prevalent in Mauritius with most of the spams originating from overseas.

## Spam Related Issues

Spam raises a number of different kinds of governance issues.

### ◆ *Costs To Consumers*

Spam can be annoying or offensive to consumers and imposes various additional costs, especially on individuals who access the network through pay-per-use or low bandwidth connections, thereby hampering the development of Internet access.

### ◆ *Overheads for Businesses*

Spam imposes significant costs on organizations in the private, public and non-profit sectors, whose employees may spend substantial amounts of work time sorting through email messages to determine which are legitimately related to their work, and in deleting the rest.

### ◆ *Phishing and Fraud*

Spam also provides a cover for other forms of cyber crime, such as identity theft through "phishing" and other forms of online fraud, which cause harm to individual consumers and impose costs on corporations (e.g. in the financial services sector), and government agencies (e.g. that issue licences).

### ◆ *Additional Costs To ISPs*

Spam also imposes significant costs on Internet Service Providers (ISPs) and other network operators, since it requires investment in a range of tools that are needed to counter spam, including anti-spam technologies (e.g. filtering technologies), server and transmission capacity, human resources, and anti-spam information sharing, cooperation, and regulatory structures. This is a particularly important concern in developing countries.

### ◆ *Spreading of viruses and spyware*

Spam provides a cover for spreading viruses, worms, trojans, spyware, etc., which typically are sent as attachments to e-mail messages, which may cause harm to individual consumers and user organizations, as well as to network operators and service providers.

### ◆ *Invasion of Privacy*

By routing their emails through "zombie" computers, the spammers are able to hide the true origin of the spam from consumers and make it more difficult for law enforcement to trace them. Consumers often are not aware that they themselves, have been sending spam.

### ◆ *Invasion of Privacy (Contd)*

As well as causing inconvenience and reducing the utility of the Internet for consumers and users, spam may violate national law – e.g. if it constitutes an invasion of privacy (e.g. spyware) – and may lead to malicious attacks on their personal property (e.g. viruses).

Spammers may use software that allows them to hijack consumers' home computers and route spam through them.

## How do I deal with spam?

Internet users themselves should be aware of the problem so that they can adopt preventive measures.

### Do's:

- ✓ Delete - without opening - all suspicious subject titles and/or e-mail addresses, often from persons or companies you don't recognize or know directly.
- ✓ Be careful when opening attachments. These can contain viruses that activate the moment you open them.
- ✓ Install a spam filter or subscribe to one from your internet service provider.
- ✓ Use multiple e-mail addresses and give out your main e-mail address only to trustworthy persons or organisations.
- ✓ Install a good quality virus scanner and firewall and keep them up to date. A poorly protected computer can be abused via the Internet. In this way you can become the sender of large amounts of spam without even knowing it.
- ✓ If confidential information is being asked in an e-mail that appears to come from your bank or Credit Card Company (for example your bank account number or login code), check by phone if this request is truly coming from them, as these kinds of inquiries are highly uncommon.