Helping you piece IT together

Everything You Wanted to Know About SPAM (but were too afraid to ask)

Disclaimer:
BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

Table of Contents

1. Introduction

Email has become an indispensable business tool allowing us to communicate quickly and effectively with work colleagues, customers and business partners, be they in the same office or in an office on the other side of the world. Documents and information can be transferred quickly and easily at the click of a button resulting in email becoming embedded in our daily business and personal lives as a mission critical communication tool.

However, just as legitimate business communications can be distributed using e-mail, so too can non-business related material such as computer viruses, copyrighted material, SPAM or content of an illegal, immoral or racist nature. All these items can expose your business to risks that need to be managed to minimise their impact on your company's bottom line.

In particular, Unsolicited Email, more commonly known as SPAM, can impact on your bottom line. SPAM emails have moved from being a slight annoyance to a major threat as they clog up expensive Internet and network connections with unnecessary traffic and expose recipients to unwanted and indeed unsavoury content.

Each SPAM message has to be processed by your network and your mail server. Recent surveys indicate that SPAM emails can account for up to 50% of all email traffic. In effect this means that 50% of your email traffic is SPAM email. There is also the productivity issue as employees sort and deal with the deluge of unwanted email in their inboxes and the invariably lost legitimate email accidentally deleted when dealing with SPAM.

The purpose of this paper is to provide the reader with an overview of SPAM, where it comes from and even why the name for a meat based product became the term for unwanted email.

2. What is SPAM?

Some people argue that there is a very narrow line between SPAM and legitimate marketing emails. This distinction between legitimate marketing emails and SPAM is, SPAM emails are Unsolicited Emails or bulk emails used to promote material that is very often not wanted or applicable to the recipient. In other words there has been no relationship of any form between the sender and the receiver of the email. In the main the content of SPAM emails can also be immoral, illegal and offensive.

3. Why do people send SPAM?

Quite simply, to make money! Email allows the spammer to send emails to thousands, indeed hundreds of thousands of people worldwide with the click of a button. The spammer is often paid on a commission basis by the person or company selling the products in the SPAM email. So it only takes a small percentage of the email recipients to sign up to the advertised product or website for the spammer to make his/her money.

With more and more people coming online to the Internet everyday, the bigger the potential market is for the spammer.

As the spammer only makes money on items sold, there is a lucrative market amongst spammers for lists of email addresses that are active, i.e. are real. Having a list of real email addresses increases the likelihood of the spammer getting someone to buy the product they are touting.

SPAM is also now being used to spread other unwanted software such as viruses, spyware, keyloggers and Trojan horse applications.

4. How did my email address get on spammer's list?

Your email address can get on spammers' mailing lists by several routes;

- The most common is posting a reply to a newsgroup on an Internet website.
- Spammers also use automated programs that crawl through websites and newsgroups harvesting anything that looks like a valid email address.
- Another common method is by people subscribing to email lists without realising that those email lists are used and/or sold to spammers.
- Filling in forms on websites that do not have proper privacy policies in place or who do not respect peoples privacy.
- Many spammers also have automated programs that guess the email address of the recipient and will automatically send emails to many different combinations and permutations of email addresses in a particular email domain.
- Finally there is a lucrative market where spammers exchange and sell their list of email addresses to each other. So not only does the spammer make money from sending you emails but also from selling your email address onto other spammers.

5. Can't I simply unsubscribe to the email to stop receiving SPAM?

Never reply to a spam email, even to unsubscribe, as this simply confirms that your email address is an active address and more spam will subsequently be sent.

6. How do I reduce the amount of SPAM I am receiving?

To following steps can help reduce the amount of SPAM you receive;

- Never reply to a spam email, even to unsubscribe, as this simply confirms that your email address is an active address and more spam will subsequently be sent.
- Never open a spam email. These emails often have hidden scripts or programs in them that acknowledge back to the spammer that your address is active and real.
- Never post your real email address on an online web site or bulletin board. People who send SPAM scour these sites to collect legitimate email addresses. If you do have to include your email address, try using the format "youraddress at somewhere.com" rather than using the normal format of "youraddress@somewhere.com."
- When filling in any form on the Internet read very carefully the conditions upon which your personal information, such as your email address, will be used. Ensure that you read carefully the website's privacy policy and make sure to check or uncheck the boxes that allow emails to be sent to you.

- Use a filtering solution to prevent spam from reaching your mail server. This will reduce the amount of spam that the users get and also reduce the overhead on your network and email system

7. Isn't it illegal to send SPAM?

The Irish minister for communications recently introduced new legislation to help deal with SPAM. Under this legislation individuals must opt-in, or agree to receive, marketing emails from companies, while marketing emails to businesses must be as a result of a pre-existing relationship. This in effect means that people receive emails only from companies that they want to receive emails from. Any organisation breaking this new law can be fined up to €3,000.00 per unsolicited email message sent.

While this is a positive step towards eliminating SPAM, there is still a long way to go. The above legislation only applies to emails originating from companies within the Republic of Ireland, i.e. someone in Ireland has to send you the SPAM email. As the large majority of SPAM is sent from addresses in the United States and Asia, the impact this legislation will have on SPAM from those sources will be negligible

8. How big is the SPAM problem?

The SPAM problem is quite large and is growing larger each day. Recent surveys by the Gartner Group indicate that SPAM emails can account for up to 50% of emails, which in effect means that 50% of your email traffic could be SPAM.

9. Does SPAM pose any risk to my business?

SPAM emails are becoming a major threat to businesses as they clog up expensive Internet and network connections with unnecessary traffic and expose recipients to unwanted and indeed unsavoury content. Each SPAM message has to be processed by your network and your mail server which adds to the costs and overheads to the running of your network.

The content in SPAM emails is often of unsavoury content and can expose your business to litigation by employees for sexual harassment or criminal proceedings if the SPAM emails contain illegal content, such as child pornography.

There is also the productivity issue as employees sort and deal with the deluge of unwanted email in their inboxes and the invariably lost legitimate email accidentally deleted when dealing with SPAM.

Recently, it has been discovered that SPAM emails are also being used to transport computer viruses and spyware (software that secretly collects personal information and sends it back to a third party), which pose a threat to the stability and security of your business.

10. Can't the SPAMMERS' computers be blocked from connecting to the Internet?

The people who send SPAM emails are constantly adopting to ensure they can remain in business. Many use ISPs and servers in countries where there is very weak or no legislation against sending SPAM.

They also exploit unprotected email servers to send SPAM on behalf of the spammer.

Recent computer viruses install software on the infected PC to enable the PC, without the owner knowing, to be used to send SPAM. According to an article in USA Today, the going price to rent a network of 20,000 PCs infected with this type of virus is $2,000 to $3,000.

11. How much does SPAM cost my business?

SPAM impacts the bottom line for your business in a number of ways.

Firstly the cost to your business of downloading storing and backing up SPAM has to be taken into account. A Gartner Survey estimates that 50% of all email traffic is SPAM. This means that 50% of the money your business spends on bandwidth for email, storage for email and processing of email is being spent so that you can receive SPAM.

There is also the loss of productivity to take into account. On a per employee basis, if the employee is on an average salary of €27,500 per year and they receive up to 30 emails a day, with each SPAM email taking 2 seconds to be dealt with, this translates into an annual cost per employee of €57. For a company with 100 employees the annual cost due to SPAM in lost productivity alone would be €5,700.

12. Why is SPAM called SPAM?

Spam is a tinned meat product, so what is the connection with the electronic version of SPAM?

Legend has it that the term SPAM comes from a comedy sketch in the British TV comedy series, Monty Python's Flying Circus. The sketch shows a waitress in a restaurant listing the various menu dishes containing spam to a customer, while in the background a group of Vikings begin incessantly chanting the words "spam, spam, spam .. " until the waitress can no longer be heard.

In the early days of the Internet, SPAM became the reference for people who excessively posted items into message boards and newsgroups. The term subsequently became used for unsolicited emails and bulk emails.

13. Contact Us

Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : **+353-(0)1- 4404065**
Website : **http://www.bhconsulting.ie**
Email : **info@bhconsulting.ie**