YOUR FAMILY AND SPAM

WHAT IS SPAM?

The term 'spam' is generally understood to derive from a Monty Python sketch[1] in which the word 'spam' is repeated continuously, much to the annoyance of those present. The official term is Unsolicited Commercial (or Bulk) Email. Spam has been defined as 'any email that was not requested by its recipient and has clearly been sent out en masse', although nowadays the term is being used increasingly for unsolicited text messages as well.

Spam occurs primarily through email, and to a lesser extent in Usenet newsgroups. It is estimated[2] that spam currently accounts for approximately 34% of email traffic within the EU. Of this approximately a quarter is estimated to contain adult pornographic content.

Spam messages are usually commercial in nature, often containing sales promotions and "get rich quick" schemes. But they can also refer to any message that a user receives from any sender with whom he has no prior relationship.

CHILDNET'S TOP TIPS FOR DEALING WITH SPAM

- Don't give out your personal email address other than to family and friends
- Never open attachments unless you know and trust the sender, they could contain viruses or nasty messages
- Use a separate family email address for subscriptions, competitions or purchases on the Internet.
- Never reply to spam, even to 'unsubscribe' – you could end up getting even more spam
- Create an email address which is hard to guess, but easy for you to remember e.g. mlou21@childnet-int.org
- Use a spam filter which can divert junk mail into a separate folder
- Install a firewall and anti-virus software to prevent any intrusion into your computer

IS SPAM LEGAL?

It is illegal to process personal contact details without the permission of the individual. Therefore spam messages sent to people who have not given consent for their email address to be used for that purpose are illegal. The vast majority of Spam emails originate in the USA and Asia, and the perpetrators are difficult to prosecute. In order to obscure their identity, in many cases they hack into vulnerable computers and the emails appear to be sent from these compromised machines.

It should be remembered that not all spam is inappropriate or illegal. It is perfectly legal to send unsolicited commercial emails to addresses which have been legally acquired and for which the sender has permission to email specific information. For example a user might have joined a mailing list, or given permission for his details to be shared with other companies when making an online purchase.

HOW SPAMMERS GET YOUR EMAIL

Email addresses for spam are collected from a range of sources. Spammers often create email mailing lists by buying or stealing existing lists, scanning newsgroup postings, or searching websites. Email addresses may be obtained through fraudulent promotions or competitions. Spammers may also generate email addresses through the use of software which combines letters and numbers with popular email domains such as hotmail.com in the hope of guessing some live addresses.

1. www.ironworks.com/comedy/python/spam.htm
2. http://europa.eu.int/comm/commissioners/liikanen/media/slides/spam.pdf

WHAT ARE THE DANGERS FOR CHILDREN?

Whilst email can be very empowering for children and young people in communicating with friends and family around the world, there are specific risks to children associated with spam. These risks fall into the three key areas of content, contact and commerce.

Content: spam can contain material which is offensive or even potentially harmful to children or your computer, either in the body of the message or in an attachment. This can include adult pornography, chain letters (which often threaten terrible consequences – even death – to those who don't forward the message) as well as viruses or Trojans. Email is the primary method in which viruses are spread and the email title can be made to look inviting to children (e.g. the I Love You virus).

Contact: although the use of spam for inappropriate adult contact with children is less likely than in chat rooms or interactive areas of the Internet, there is a possibility that an attachment on a spam email could contain a so-called Trojan.

This is a piece of software which effectively takes over the recipient's computer, revealing all data and potentially allowing the spammer to use that computer to send further spam or initiate other forms of inappropriate communication. This means that no matter how careful a child is about keeping his/her personal information secret, that information can become available through opening a spam mail. A firewall can help protect you from this.

Commerce: Spam email is an obvious way for vendors to target potential customers, and children and adults alike can come under considerable pressure to make online purchases in response to spam. Recent US legislation[3] made it illegal to collect personal data from a child under 13 without parental consent, but as yet no parallel legislation exists in the UK.

In addition to the three areas of risk outlined above, dealing with spam can take a considerable amount of time, and this may in itself detract from the potential benefit of the Internet.

HELPING YOU AND YOUR CHILDREN AVOID SPAM

There are a number of ways in which parents can protect their children from the hazards of Spam. These include the following:

Selection of email address and Internet provider:

- Before choosing an Internet service provider it is worth considering what they do to protect their customers from spam. Be aware that free email accounts generally attract more spam.
- Set up a separate email address for the family for online subscriptions or profiles. You can then make sure that the children are not given access to this account and don't receive any spam that it might generate.
- Make sure that children's email addresses do not disclose age, sex, location (a/s/l) or any other identifying information, and that they are not easy to guess.

Protecting contact information:

- Teach your children to treat personal email addresses like bank details, never to be given out unless they are absolutely sure they can trust the recipient to keep those details private.
- Ensure that your child's personal email address is not displayed on websites or profiles.(try doing an Internet search from time to time to check this)
- You can mask your email address by include the words 'nospam' or 'remove to reply' in any email addresses posted on the Internet e.g. ruth@nospam.childnet-int.org. This prevents the automatic processing of addresses collected by 'spiders'. You may need to append a short note explaining that the additional words need removing before using the address.
- Take care to read the privacy and data protection policies when signing up for online services, and do not use services which have no such policies.

3. http://www.ftc.gov/ogc/coppa1.htm

- Make sure you check the 'opt-out' boxes when making online registrations or purchases.

Ignoring Spam:

- Never make a purchase in response to a spam communication. It is because some people do this that spam persists.
- Teach your children to recognize spam and not reply to it, even if there is an 'unsubscribe' mechanism – all this will do is confirm to the spammer that your email address is live.
- Similarly teach your children not to forward chain emails, even if they promise rewards, or threaten them.

Filtering/Tools:

- Use a spam filtering product which can divert spam into a separate folder. Some email services and software offer an inbuilt filter whereby you only receive messages from those in your address book. However, always check the contents of the junk mail folder before deleting it, as genuine email can be erroneously identified as spam.
- Ask your Internet Service Provider about their spam blocking and/or filtering policies and processes.
- To Learn more about software tools to prevent spam take a look at this website which reviews many tools and includes advice on pop-ups which are a new form of spam. **http://spam.getnetwise.org/tools**

Reporting:

- Encourage your children to tell you if they get any suspicious email and prepare them for the fact that this can happen, and most importantly of all that they won't be punished for receiving it.
- Report spam to your ISP using the appropriate 'abuse' address[4].
- If the spam contains or advertises indecent images of children, report it to the Internet Watch Foundation[5].
- Since much spam is generated in the USA you can forward spam to the Federal Trade Commission. Simply forward the messages to **uce@ftc.gov**.

Make sure that you include the header information in the e-mail.

FURTHER INFORMATION

If you wish to complain about spam or text messages that you are receiving from registered companies in the UK or the USA, there are a number of organizations you can contact. They will contact their members to ensure that they are not in breach of their codes of practice. Here below are a few worth considering. The Advertising Standards Authority who can alert the company of their breach in the code of practice. **www.asa.org.uk**

Or in extreme cases you can report an incident to the UK Information Commissioner who have the power to take to company to court. **www.informationcommissioner.gov.uk**

The Direct Marketing Association (US-based) manages a global E-mail Preference Service which allows users to register their email addresses in order to prevent the receipt of unsolicited sales and marketing email messages **www.dmaconsumers.org/offemaillist.html**

Further Information about Spam can be obtained at The Federal Trade Commission website in the USA. The site contains of list of common spam scams, and also provides an email address to forward fraudulent spam **uce@ftc.gov**. The commission keeps a database and investigates spam claims. **www.ftc.gov/bcp/conline/edcams/spam**

---

4. For help in finding the right address for your ISP contact the Internet Services Providers Association: **www.ispa.org.uk**
5. **www.iwf.org.uk**