



## Information Sheet on Spamming

### 1. What is Spam?

“Spam” can be defined as all unsolicited electronic mail sent out in bulk to individuals/organisations that have not consented to receive it. Spam comes under a number of classifications:

- Unsolicited Commercial Email (UCE) which usually advertises a product or service.
- Unsolicited Bulk Email (UBE) which is used for things like lobbying.
- Chain letters and pyramid schemes.
- Emails relating to other fraudulent schemes such as phishing.
- Messages sent to a recipient who had agreed to receive mail but has subsequently opted-out.
- Any email without an “Opt-out” facility.
- Where an Opt-out facility is provided but it is deliberately misleading or difficult to activate.
- Any email that does not have a valid address in the Reply To line.

### 2. How can I tell whether or not an Email Message that I receive is Spam?

The clues are often in the ‘Email Subject Line’. Watch out for words like ‘free’, promises of money, investment opportunities, love or friendship. More creative spammers will make out they know you e.g. ‘Hi there’, or make out you have been specially selected in some way.

Beware of messages that come from businesses or addresses you do not recognise. Many of these addresses are bogus and are used for a specific campaign and then discarded. Look out for messages where the sender is

not clearly identified. Be cautious of opening any attachments to emails, particularly from messages you are suspicious of.

### 3. What does Opt-in and Opt-out mean?

Giving your permission to an organisation to be contacted via Email is called ‘opt-in’. ‘Opt-out’ is the opposite of opt-in and is the term used for removing your email address from a list. An Opt-out link should be attached to emails you receive from the lists you have joined so that you can leave at any time. The terms opt-in and opt-out are also referred to as ‘Subscribe’ and ‘Unsubscribe’.

### 4. How did I get on a Spammers List?

“Spammers” (people that distribute spam) often buy “Email Lists” from people who have harvested addresses from “Web Sites” or “Newsgroups”. Before you submit your own email address to a website, check the site’s privacy policy.

Look out for “Websites” offering prizes in return for you filling in surveys or forms or providing personal information. It may simply be a technique used in an effort to secure your email address for use by “Online Marketers”. If you are not careful, you could receive large quantities of spam in your email inbox.

### 5. How do I get off a Spammers List?

Firstly, do not reply to [spam](#), as it shows that your email address is active and therefore a target for further [spam](#). Unfortunately, once your email address is on a spammers list, it is often impossible to remove it.

### 6. How can I protect myself from spam?

You can reduce the amount of spam you receive by:



## Information Sheet on Spamming

### a. *Protecting your email address when online*

Spammers use automated tools to collect (or 'harvest') email addresses from the Internet. Your email address may appear on web pages and be collected by spammers.

When online, it is best to avoid giving out your email address where possible. If you must provide an address, look for options, for example a tick box, that indicate no further offers or information will be sent to you. Make sure you read the terms and conditions of anything you are subscribing to and the organisation's privacy policy and consent arrangements before disclosing your personal information online.

If you want people to be able to contact you from your website, but do not want to be inundated with spam, you have several options:

- Use a non-personal address, such as: info@example.com or my-business-address@example.com.
- Use a web-based form that site visitors can use to contact you. The form can be set up to send you an email when submitted, and you can reply to the person who filled in the form as if they had sent you an email directly. This defeats the automated mailing systems used by spammers.
- Write your email address in a way that makes it harder to 'harvest', for example, omit the '@' symbol: rather than your-name@example.com, try: your-name at example dot com.
- If you publish your email address, consider adding an accompanying statement such as 'No spam please', so it is clear you do not consent to receiving unsolicited commercial emails.

### b. *Using filters*

A filter is a piece of software that sorts incoming email messages and

rejects (or 'bounces') those it thinks are spam.

Filtering is very useful, but it's not perfect. Sometimes filters will fail to identify spam; other times they can mistakenly block a genuine non-spam message.

Because of these factors, many people choose to 'tag' their spam and direct it into a 'spam folder', rather than automatically deleting it. This allows you to periodically scan for genuine messages that your filter has mistakenly identified as spam.

If you use web-based email, such as Hotmail or Yahoo, your email provider will probably offer an anti-spam setting. Filter software can also be purchased from computer shops and from your Internet Service Provider (ISP)

### c. *Not becoming an 'accidental spammer'*

If you do not have effective security measures in place, spammers can infect your computer with a virus and use it to send spam to other people without your knowledge. To avoid becoming an accidental spammer, you need to adopt these good security practices:

- Use anti-virus software, and ensure it is updated regularly.
- Use personal firewall software.
- Download and install the latest security patches for your computer system.
- Attachments to email messages can be dangerous. Only open them if you know what they contain and who has sent them to you. Otherwise, it's safest to delete them immediately. If you do need to open an attachment, run it through up-to-date anti-virus software first.