Australian Government
National Office for the Information Economy
Australian Communications Authority

Spam Act 2003:
An overview for business

This overview has been designed for:

- **small businesses** that wish to gain an understanding of the Spam Act; and
- **senior managers** within firms that send electronic messages.

NOIE has also developed a more comprehensive guide to the Spam Act. Copies of *Spam Act 2003: A practical guide for business* are available at **www.noie.gov.au/publications/index.htm**

SPAM ACT 2003:
AN OVERVIEW FOR BUSINESS

This overview of the Spam Act 2003 (the Spam Act) may be used by anyone who needs a snapshot of the Act, but is particularly intended for people who need an outline of its main elements, such as business executives and owners of small businesses. The guide has been developed in consultation with key industry stakeholders to provide a clear explanation of the Act's requirements.

WHAT IS SPAM?

The Spam Act refers to spam as "unsolicited commercial electronic messaging".

"Electronic messaging" covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone.

To be covered by the Spam Act, the message must be commercial in nature — for instance offering a commercial transaction, or directing the recipient to a location where a commercial transaction can take place.

There are a large number of commercial electronic messages that can be sent legitimately. They are only considered to be spam if they are sent without the prior consent of the recipient — as unsolicited messages.

A single message may be spam. The message does not need to be sent in bulk, or received in bulk.

In addition to prohibiting spam, the Spam Act lays out rules for sending legitimate commercial electronic messages.

Spam Act 2003: An overview for small business February 2004
National Office for the Information Economy 1 74082 048 7 Print
National Office for the Information Economy 1 74082 049 5 Online

Disclaimer

Please note:

This guide has been prepared by NOIE to provide information to business in relation to the sending of commercial electronic messages.

While every effort has been made to ensure that the document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This guide should not be relied upon as legal advice. Users are encouraged to seek independent advice relevant to their own particular circumstances.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

THE SPAM ACT - WHAT DOES IT SAY?

SPAM PROHIBITED

The Spam Act says that *unsolicited commercial electronic messages* must not be sent.

Messages should only be sent to an address when it is known that the person responsible for that address has consented to receive it.

RULES FOR SENDING COMMERCIAL ELECTRONIC MESSAGES

Commercial electronic messages must contain:

- Accurate information about the sender of the message; and
- A functional way for the message's recipients to indicate that they do not wish to receive such messages in the future – that they wish to unsubscribe.

ADDRESS HARVESTING SOFTWARE, HARVESTED ADDRESS LISTS

Business must not use electronic address harvesting software or lists which have been generated using such software, for the purpose of sending unsolicited commercial electronic messages.

MESSAGES COVERED BY THE ACT

The Spam Act covers commercial electronic messages that are sent using applications such as:

- email;
- short message service (SMS);
- multimedia message service (MMS); and
- instant messaging (iM).

MESSAGES NOT COVERED BY THE ACT

The following examples are not covered by the Spam Act:

- Non-electronic messages (such as ordinary mail, paper flyers etc);
- Voice-to- voice telemarketing;
- The majority of "pop up" windows that appear on the internet (they are usually an intrinsic part of a webpage that has been accessed, rather than a message sent to the recipient address); and
- Messages without any commercial content that do not contain links or directions to a commercial website or location.

THE ACT COVERS MESSAGES WITH AN AUSTRALIAN LINK

The provisions of the Spam Act cover commercial electronic messages:

- originating in Australia that are sent to any destination; and
- originating overseas that are sent to an address accessed in Australia.

FINANCIAL PENALTIES

The maximum penalties under the Spam Act are substantial.

A business that is found to be in breach of the Spam Act may be subject to a Court imposed penalty of up to $220,000 for a single day's contraventions. If a business is found to have breached the Act and breaches it again, they may be subject to a penalty of up to $1.1 million.

The Spam Act specifies a number of options that are available to enforce the legislation, depending on the circumstances. The range of possible activities includes formal warnings, infringement notices (similar to a speeding ticket), and court actions.

OTHER CONSIDERATIONS...

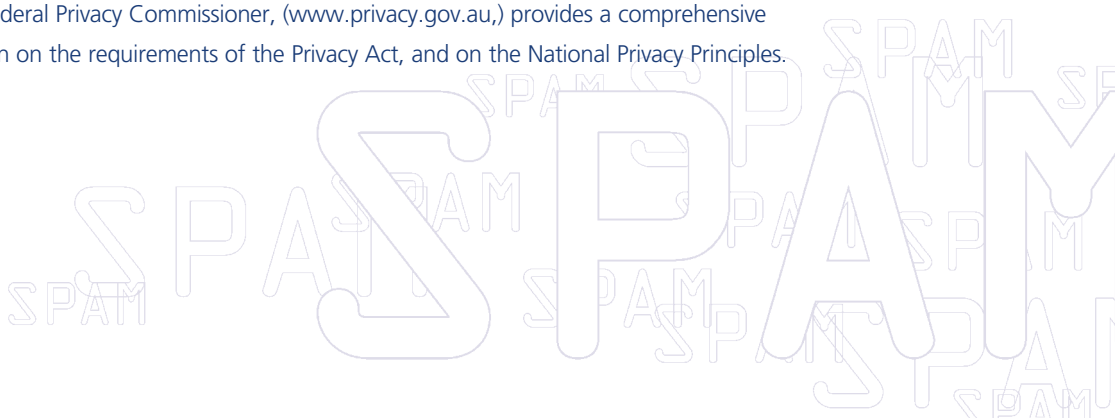
Check your ISP's policies

It should be noted that many businesses may have existing agreements with their Internet Service Providers (ISPs) on "Acceptable Use Policies" (AUPs) which specify a higher level of consent than is provided for in the spam legislation. For example, such agreements may require express consent or require the use of double opt-in methodologies for confirming consent. This helps to protect business reputations and to avoid problems with groups that block perceived spammers on the Internet. The Spam Act does not overrule cases where a higher standard is required in an AUP. Businesses should pay close attention to their AUPs to avoid difficulties with their ISP.

The Privacy Act 1998 and the National Privacy Principles (NPPs)

In addition to the requirements of the Spam Act, you should always be in compliance with the provisions of the National Privacy Principles.

The Office of the Federal Privacy Commissioner, (www.privacy.gov.au,) provides a comprehensive range of information on the requirements of the Privacy Act, and on the National Privacy Principles.



WHAT SHOULD I DO?

3 steps to follow

When reviewing your business practices and the content of your commercial messages to ensure you comply with the Spam Act, you should consider the following three steps.

STEP 1 - CONSENT

Your commercial messages must only be sent when you have **consent**.

This may be **express consent** from the person you wish to contact – a direct indication that it is okay to send the message, or messages of that nature.

It is also possible to **infer consent** based on a business or other relationship with the person and their conduct.

STEP 2 - IDENTIFY

Your commercial messages must always contain clear and accurate **identification** of who is responsible for sending the message and how they can be contacted.

It is important for people to know who is contacting them and how they can get in touch in return. This will generally be the organisation that authorises the sending of the message, rather than the name of the person who actually hits the "send" button.

Identification details that are provided must be reasonably likely to be accurate for a period of 30 days after the message is sent. This would be a consideration if the business was about to change address.

STEP 3 - UNSUBSCRIBE

Your commercial messages should contain an **unsubscribe facility**, allowing people to indicate that commercial messages should not be sent to them in future. This could be as simple as a line in your message saying "If you wish to opt out from future messages, send a reply with the subject UNSUBSCRIBE".

After a person indicates that they wish to unsubscribe, you have five working days to honour their request.

Similar to the identification of the message's sender (step 2, above) the unsubscribe facility must be reasonably likely to remain accurate and functional for a 30 day period. It need not be an automated process, but should be reliable.

MORE INFORMATION

We've listed the three steps your business should follow to satisfy the requirements of the Spam Act. Additional Information in relation to the Spam Act and preventative measures is available from the ACA and NOIE websites located at the following addresses: www.aca.gov.au and www.noie.gov.au.

MORE DETAILED "PRACTICAL GUIDE FOR BUSINESS"

A more comprehensive guide to the requirements of the Spam Act, is available from the NOIE website. *Spam Act 2003: A practical guide for business* is available with other resources from **www.noie.gov.au/publications/index.htm**

The practical guide provides more detail on what is involved in:

- having consent for your commercial electronic messages;
- accurate sender identification; and
- a functional unsubscribe in your messages.

OTHER SOURCES OF INFORMATION

Many industry organisations also offer advice about the Spam Act 2003 and about spam in general. This information can be found from the following website addresses:

- Spam Act 2003: A practical guide for business available with other resources from **www.noie.gov.au/publications/index.htm**;
- E-business Guide – An Australian guide to doing business online **www.e-businessguide.gov.au**;
- Small Business Enterprise Association of Australia and New Zealand **www.seaanz.asn.au**;
- Australian Direct Marketing Association (ADMA) **www.adma.com.au/asp/index.asp**;
- Coalition against Unsolicited Bulk Email (CAUBE) **www.caube.org.au**;
- Internet Industry Association (IIA) **www.iia.net.au**;
- Internet Society of Australia (ISOC) **www.isoc-au.org.au**;
- Public Relations Institute of Australia (PRIA) **www.pria.com.au/home.php**;
- Small Enterprise Telecommunications Centre (SETEL) **www.setel.com.au**; and
- Presidian Legal Publications **www.presidian.com.au**.