



Australian Government

Australian Communications Authority

Protecting your business from spam

#spam

What is spam?

Spam is the common term for electronic ‘junk mail’—unwanted messages sent to a person’s email account or mobile phone. Spam messages vary: some simply promote a product or service, or invite the user to visit a website where they can make purchases; others attempt to trick the person into divulging their bank account or credit card details.

In Australia, spam is defined as ‘unsolicited commercial electronic messages’—it can range from a single message from a legitimate business, to the high-volume or ‘bulk’ messages sent out by professional spammers.

This guide gives an overview of a new Australian law relating to spam—the *Spam Act 2003*—and offers advice on reducing the amount of spam you receive, and suggestions on what to do when you receive it.

Detailed information about how your business can ensure it does not send spam is on the Australian Communications Authority (ACA) website—www.aca.gov.au and click on ‘spam – Information for business’.

Why is spam a problem?

The billions of unwanted spam messages flooding the Internet cause significant inconvenience to individuals and businesses. Spam disrupts email delivery, clogs up computer systems, reduces productivity, wastes employees’ time, causes irritation through sheer volume, erodes users’ confidence in email and ultimately raises the cost of Internet access fees. Many spam messages also contain offensive or fraudulent material, and spam is sometimes used to spread computer viruses.

What do Australia's anti-spam laws do?

On 10 April 2004, the Australian Government's new anti-spam legislation came into effect. Under the *Spam Act 2003* it is illegal to send, or cause to be sent, 'unsolicited commercial electronic messages' with an Australian link. 'Australian link' means the message originated or was commissioned in Australia, or originated overseas but was sent to an address accessed in Australia.

The use of address-harvesting software and harvested address lists to send spam is also prohibited under the Spam Act.

The legislation covers electronic messages—emails, mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (iM)—of a commercial nature. However, it does not cover faxes or voice-to-voice telemarketing.

How can I tell if it's spam?

To comply with Australia's spam laws, a commercial electronic message must meet the following conditions. Any message sent to you that doesn't meet these conditions is breaching the Spam Act:

- **Consent**—it must be sent with your consent. You may give *express* consent, or consent may be *inferred* from your conduct and 'existing business or other relationships'.
- **Identity**—it must contain accurate information about the person or organisation that authorised the sending of the message.
- **Unsubscribe**—it must contain a functional 'unsubscribe' facility to allow you to opt out from receiving messages from that source in the future.

Exemptions

Certain types of electronic messages from particular sources are exempted from the legislation. These include certain messages from:

- government bodies;
- registered political parties;
- charities;
- religious organisations; and
- educational institutions (sent to attending and former students and their households).

To be exempted, the message must relate to goods or services supplied by the sender of the message. However, government bodies that are incorporated as companies are not exempted from the Spam Act.

Purely factual messages with no commercial content are also exempted, but the sender must still include accurate identifying information. See the ACA website—www.aca.gov.au and click on ‘spam – Frequently asked questions’—for more information about exemptions and purely factual messages.

How can I protect my business from spam?

There are several tricks you can use to reduce the amount of spam your business receives: these include protecting your email addresses from spammers, using filters and taking security precautions to ensure you don’t accidentally spam others.

Protect your business email addresses

Spammers use automated tools to collect (or ‘harvest’) email addresses from the Internet. Email addresses for your business may appear on web pages and be collected by spammers when staff members list their work email address on a website, register a domain name or post a message to a mailing list.

Spammers may also send out bulk emails to random possible addresses in the hope of hooking a genuine recipient—a tactic known as ‘dictionary attacks’. Harvesting and dictionary attacks are prohibited under the *Spam Act 2003*.

If you must provide your work-related address when using the Internet, look for options, for example a tick box, that indicate no further offers or information will be sent to you.

If you want people to be able to contact you from your business website, but don’t 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.
- Consider using different email addresses for different business purposes. This is especially important when signing up with companies on the Internet using a web form.
- 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 business email address, consider adding a statement such as ‘No commercial messages please’, or ‘No spam’, so it is clear you do not consent to receiving unsolicited commercial emails. However, this may mean that some businesses wishing to email you for legitimate purposes under the Spam Act’s ‘inferred consent’ provision may not be able to do so.

Use filters

Filtering is an important element in your business' spam reduction strategy. A filter is a piece of software that sorts incoming email messages and 'quarantines' or 'tags' those it thinks are spam.

Many Internet service providers (ISPs) undertake spam filtering or offer it at extra cost. When choosing your ISP, discuss their spam filtering options and make that a factor in your decision.

Filtering is very useful, but it's not perfect. Sometimes filters may fail to identify spam—a 'false negative'—or mistakenly block a genuine, non-spam message—a 'false positive'. Many filters can be tuned for vigilance—a more aggressive setting blocks more spam, but may cause more false positives.

To reduce the risk of false positives, many businesses use filters that 'tag' their spam and direct it into a 'spam folder', rather than automatically deleting it. This means you can periodically scan for genuine messages that your filter has mistakenly identified as spam.

If your businesses use web-based email, such as Hotmail or Yahoo, your email provider probably offers an anti-spam setting. Filtering software is available from computer shops, or check the Internet Industry Association security website—www.security.iiia.net.au—for links to organisations that sell the software.

If your business has its own email server, the ACA recommends that you consider installing an email filter at the server level, to screen all incoming messages before they are delivered to employees.

Don't become an 'accidental spammer'

If you don't have effective security measures in place, spammers can infect your computer with a 'Trojan horse' and use your computer to send spam to other people without your knowledge. To avoid becoming an accidental spammer, learn about and 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. In recent versions of Windows operating systems, this can be controlled with the 'automatic updates' feature in your Windows control panel.
- 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.
- Use long and random passwords.

You can learn more about security by browsing in a computer bookshop or by typing 'good security practices' into your favourite search engine. Anti-virus and personal firewall software is available from your ISP, computer shops and through organisations listed on the ACA website—www.aca.gov.au and click on 'spam'.

Secure your server

Most spammers operate by taking advantage of legitimate businesses that do not have fully secure servers. Spammers send their bulk junk messages through the servers of these businesses.

If your business has its own web or email server, there are important measures you should take to ensure that your server is secure. Leaving your server open to abuse by spammers is risky—your system may crash or be damaged, important messages will be lost, time and money will be wasted fixing the problem, your business reputation will be tarnished, millions of spam messages may be sent out purporting to be from your business and you may be blacklisted by anti-spam sites.

The ACA website has detailed information on steps you can take to secure your server—www.aca.gov.au and click on ‘spam – Information for Business: secure your server’.

What can I do if I receive spam?

If you think your business has been sent spam, you have several options:

Do not respond if the source seems dubious

If you receive spam from a source that looks dubious, it is safest to simply delete the message without opening it. Do not reply, and do not click on any links or buttons, including those that promise to remove you from a mailing list.

In general, it is unwise to open any spam email: if it is sent by a professional spammer, this may just confirm your existence to the spammer and result in yet more spam. Do not purchase products or services that are advertised using spam—many are fraudulent, and purchasing spam-advertised products only encourages more spam.

Contact the sender directly to make a complaint

If you have already opened the message and it advertises a legitimate Australian business, you may wish to contact that business directly by telephone or in writing, to make a complaint and request that they do not send you any more messages. Most legitimate businesses are keen to maintain a good reputation and satisfied customers.

Make a spam complaint or report to the ACA

The ACA's immediate focus is on spam of Australian origin. Bearing in mind the warning (above) about the risks of opening spam emails, if you have already opened the message, and it has come from an Australian business and you have been unable to resolve the matter with that business, you can make a complaint to the ACA. This can be done using our online complaint form (see below for website details).

The ACA also collects reports about spam that originates overseas. These international spam reports will help the ACA to analyse patterns of spamming activity affecting Australia; they will also enable the ACA to share evidence of global spam with relevant international authorities, and to coordinate effective international efforts to reduce spam.

More information about how to report spam or make a complaint is available on the ACA website—www.aca.gov.au and click on 'spam – Reporting, Complaints and Enquiries'.

Beware of email scams and fraud

Many spam messages are used to propagate illegal scams. To learn more about email scams, visit the government's scamwatch website at www.scamwatch.gov.au.

The ACA website has information about some common email scams, how to avoid being taken in by them and where you can report email fraud—www.aca.gov.au and click on 'spam – Consumer Information: beware of email scams and fraud'.

What are government and industry doing about spam?

The Australian Government is pursuing a five-way strategy for tackling spam. Under this five-way strategy, the ACA is committed to the following anti-spam measures:

- directly enforcing the Spam Act;
- promoting education and awareness among consumers and business;
- industry liaison;
- technological solutions and monitoring; and
- international cooperation.

To complement the *Spam Act 2003*, the ISP and e-marketing industries are developing **codes of practice** to reduce the amount of spam entering and propagating across the Internet, and to assist Australian businesses and ISPs to follow best practice in reducing spam.

Unfortunately, much of the spam that affects Australians comes from overseas. Efforts to combat spam on a national level are necessary, but significant long-term gains will only come about through cooperative arrangements with other countries and relevant international bodies. The Australian Government is at the forefront of establishing and strengthening these international arrangements.

More information

A list of useful links, frequently asked questions, official guides for business, contact details for other relevant organisations and a link to the Spam Act are on the ACA website—www.aca.gov.au and click on ‘spam’.

www.aca.gov.au

*The Australian Communications Authority is
a government regulator of telecommunications
and radiocommunications*