Australian Government
Australian Communications Authority

Fighting spam in Australia

A consumer guide

Fighting spam

- Use filtering software
- Install anti-virus software
- Use a personal firewall
- Download security patches
- Choose long and random passwords
- Protect your email address
- Protect your mobile phone number
- Read terms and conditions carefully
- Beware of email scams and fraud
- Don’t open suspicious attachments
- Don’t unsubscribe if the source seems dubious
- Report the spam to the ACA

Australia’s spam laws:

☑ consent

CONSENT

email from @address.com identify

IDENTIFY

unsubscribe unsubscribe

UNSUBSCRIBE

www.spam.aca.gov.au

What is spam?

Spam is the common term for electronic 'junk mail'—unwanted messages sent to your email account or mobile phone. Under Australian law, spam is defined as 'unsolicited commercial electronic messaging'.

Some spam promotes a product or invites you to visit a website, other spam tries to trick you into investing in fraudulent schemes, or revealing your bank account or credit card details. Email spam often carries viruses.

Australian spam law—the *Spam Act 2003*—covers email, mobile phone messages (SMS, MMS) and instant messaging. It does not cover faxes, voice telemarketing or Internet pop-ups.

How can I tell if it's spam?

Any commercial message sent to you that doesn't meet the following conditions is breaking Australia's spam laws:

- **Consent**—it must be sent with your consent. You may give **express** consent, or your consent may be **inferred** from your existing 'business or other relationships', or certain other restricted conditions.
- **Identify**—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. Your request must be honoured within five working days.

How can I protect myself from spam?

Tricks to reduce incoming spam include protecting your email address and mobile phone number, using filtering software and boosting your Internet security to ensure that spammers can't send spam via your computer.

Check the terms and conditions of anything you sign up to, and be wary of fine print. Are you consenting to receive commercial messages?

Protect your email address when online

Spammers automatically collect (or 'harvest') email addresses from the Internet. Your email address can be harvested when you list it on a website, register a domain name, post a message to a mailing list or contribute to an Internet chat room.

Avoid giving out your email address where possible. If you must do so, look for options such as tick boxes that indicate you won't be sent further offers or information.

Check an organisation's terms and conditions or privacy and consent policies before disclosing personal information online, and check that they commit not to pass your information on to other parties.

Consider using separate email addresses for different purposes, such as a personal 'friends and family' email address. This will help you sort and prioritise your email.

Spammers also send out bulk emails to random addresses in the hope of hooking a genuine recipient—a tactic known as 'dictionary attacks'.

Protect your email address when posting it on a website

If you want to post your contact details on your website but don't want to be flooded with spam, you have several options:

- Give a non-personal email address, such as info@example.com or my-business address@example.com.
- Use a web-based form for site visitors. When a visitor submits the form you'll receive an email and you can reply as if the person had emailed you directly. These forms defeat spammers' automated mailing systems.
- Write your email address so that it is harder to 'harvest'. For example, post it as an image, rather than text, or omit the '@' symbol (instead of 'my-name@example.com', write 'my-name at example dot com').

Use filters

A filter is a piece of software that sorts incoming email messages and blocks those it thinks are spam.

Filtering is very useful, but it's not perfect. Sometimes filters fail to identify spam, other times they mistakenly block a genuine, non-spam message. Adjusting the filter settings can help minimise these risks.

You can also choose to direct your spam into a 'spam folder' rather than automatically blocking it. This means you can periodically scan for genuine messages that your filter may have mistakenly identified as spam.

If you use web-based email such as Hotmail or Yahoo, your provider will probably offer an anti-spam setting. You can buy filtering software from your Internet service provider (ISP) or computer shop, and some ISPs offer a free spam filtering service.

Don't become an 'accidental spammer'

If you don't have good security measures in place, spammers can take over your computer and use it to send spam to other people without your knowledge. To avoid becoming an accidental spammer adopt these good security practices:

- Use anti-virus software and update it regularly.
- Use personal firewall software.
- Download and install the latest security patches for your computer system.
- Use long and random passwords.
- Email attachments can be dangerous. Only open an attachment if you know what it is and who sent it. If you don't know, delete it immediately. Before opening any attachment run it through up-to-date anti-virus software first.

To learn more about good security, visit the ACA website at www.spam.aca.gov.au, the Department of Communications, Information Technology and the Arts website at www.dcita.gov.au/e-security, the Australian Internet Industry Association website at www.security.iia.net.au or a computer bookshop. Anti-virus and personal firewall software is available from your ISP and computer shops.

Protect your mobile phone number

Mobile phone spam can be particularly annoying. Exercise caution when disclosing your mobile phone number—could you be sent commercial messages as a result?

Beware of email scams and fraud

Email spam is often used to carry out fraud. Beware of any offer that sounds too good to be true—it probably is!

'Phishing' emails are a common example. They pretend to come from your bank and urge you to click a link to the bank's website and enter your account details. Don't be fooled—these websites are clever fakes and typing in your details could result in your account being emptied by the fraudsters.

To learn more about email scams visit the government's Scamwatch website at www.scamwatch.gov.au. To report scams contact the Australian Competition and Consumer Commission (ACCC) website at www.accc.gov.au.

What can I do if I receive spam?

Some spam is sent by professional spammers. Other spam is sent by legitimate businesses that are not complying with Australia's spam laws. If you have been spammed, you have several options.

Do not respond if the message seems dubious

If you receive an email that seems dubious—for example, the subject line or sender look suspicious—it is safest to delete it immediately without opening it. Do not reply and do not click on any links, including 'unsubscribe' links. Doing so may result in even more spam. Do not buy spam-advertised products or services—many are fraudulent and buying them only encourages more spam.

If the source seems genuine, contact the business to make a complaint

If you have already opened the message and it promotes a legitimate Australian business, you may wish to contact them by phone or in writing to make a complaint and ask them to take you off their mailing lists. As legitimate businesses do not operate in the same way as professional spammers, unsubscribing to their emails can also be a low-risk and quick way to prevent future spam.

Report the spam

You can report spam to the ACA through the ACA website at www.spam.aca.gov.au (click on 'Reporting, Complaints & Enquiries'). Your spam report will assist the ACA to reduce spam and identify patterns of spamming activities affecting Australia.

Spam that contains illegal content, including pornography and online gambling, can be reported to the Australian Broadcasting Authority (ABA) by emailing online@aba.gov.au.

What are the government and industry doing about spam?

The Spam Act is enforced by the ACA. The ACA is also working with industry, promoting public and business education and developing technical solutions to spam.

Most spam comes from overseas, so international cooperation is vital. The Australian government is at the forefront of developing international anti-spam agreements.

Australia's e-marketing and ISP industries are developing codes of practice to reduce spam.

Where can I find out more?

For more spam-related information, including frequently asked questions and useful links, visit the ACA website at www.spam.aca.gov.au.

www.aca.gov.au

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