

Spam emails

[Share](#)

Please note: The following information has not been updated since the Data Protection Act 2018 became law. Although there may be some subtle differences between the guidance on this page and guidance reflecting the new law – we still consider the information useful to those in the media.

What are spam emails?

Spam emails are emails sent to you without your knowledge or consent, which often contain marketing. It is email that you don't want and didn't ask for, and its content can cause annoyance, embarrassment and even distress. However, it's worth remembering that the sender generally doesn't target recipients personally. The same spam email can be sent to millions of people at the same time and the addresses can often be guessed.

Not all marketing emails sent without consent are spam emails. Marketing emails can be sent without prior consent by organisations who obtained your email address when you bought something from

content and provide you with the opportunity to opt out.

What does the law say?

The Privacy and Electronic Communications Regulations 2003 (PECR) cover the sending of marketing emails. This legislation says that organisations must only send marketing emails to individuals if you have agreed to receive them, except where there is a clearly defined customer relationship.

The ICO can only investigate concerns about marketing emails from identifiable UK senders. As a lot of spam emails come from outside the UK, the Information Commissioner has an agreement with a number of overseas bodies to cooperate and exchange information to try and stop spam emails that are sent from those places.

What can I do if I'm getting unwanted marketing emails?

If you receive a marketing email that you don't want from an identifiable and legitimate UK based organisation that you know and trust, you should first use the 'unsubscribe' link provided on the email. The organisation should then stop sending you marketing emails. Legitimate, well-known companies will offer opt-outs, and in many cases things can be resolved quickly without us getting involved.

However, if you continue to receive marketing emails from the organisation despite using the 'unsubscribe' link you may wish to report this to the ICO:

emails (remembering to keep a copy of any correspondence). You should allow them time to put things right.



The right to object to the use of your data

Your data matters

If you are not sure whether the email is genuine, or if it comes from an organisation you don't recognise, you should avoid replying or clicking on any link as this might confirm your email is live and make you a target for more spam emails. You can report receipt of these emails to the ICO:

What can I do if I'm getting unwanted marketing emails at my work email address?

If the work email address belongs to a sole trader or unincorporated partnership, your work email address is treated the same as your home email address, and you can follow the advice above.

The rules on email marketing are different if the marketing is being sent to a corporate email address. If you work for a corporate body (that is a company, Scottish partnership, limited liability partnership or government body), organisations are allowed to send marketing emails to your work email address without your consent. If you are receiving unwanted marketing emails to your work email address you may wish to use the unsubscribe option if the email you have received is from an identifiable and legitimate UK based organisation that you know and trust. Whilst the law doesn't require organisations to stop sending marketing emails to corporate email addresses, many businesses will do so as a matter of good practice when they have received an objection or opt-out.

under the Data Protection Act. This means that you can write to the organisation asking them to stop any marketing to your work email address. When they receive your request they must stop sending you marketing emails as soon as they can.

What can I do to reduce the amount of spam emails I receive?

- Be careful who you give your email address to.
- Consider having separate personal and business email addresses.
- Choose an email address which is difficult to guess.
- Don't advertise your email address, for example by making it available on the internet.
- Check privacy policies and marketing opt-outs carefully. If you buy something online or subscribe to a service, check the company's privacy policy before giving your email address or any other personal information. Consider how the company uses your information and whether they might send it to other people within their organisation or to other organisations.
- Avoid responding to spam emails if you have any doubts about who has sent them. Replying indicates that your email address is live. You should not reply to emails unless you know and trust the sender, and are confident the email is genuine. However, many complaints received by the ICO are about well known, legitimate companies who offer opt-outs. In most cases responding to the opt-outs in these emails should stop the problem.
- Don't click on the adverts in spam emails. By clicking on spammers' web pages, it shows your email address is live and may make yourself a target for more emails. It can also reveal your computer's IP address.
- Use a spam email filter on your computer. These are programs which work with your email package to sift through new emails, separating spam emails from wanted emails and blocking them.

downloaded before being blocked. New spam email filters are being developed all the time; you can search the internet for one that is suitable for you. Many Internet Service Providers (ISPs) also offer filters which work by examining content and using blacklists to restrict spam emails. Again, these sometimes block good emails as well as spam emails and you might have to pay for them. For more information on the services that are available to you, please check with your ISP.

- Keep your systems well maintained. Hackers and spammers can exploit software problems, so most software companies issue product updates and patches that fix known problems. Updates are generally available through manufacturers' websites and are usually free to download and install. You should also consider using anti-virus software to protect against virus programs that can destroy computer files and are increasingly being exploited by spammers.

Take action

Report spam emails



Further reading



[Nuisance calls and messages](#)

Action we've taken



English





The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

© Copyright Privacy notice
Cookies Disclaimer Publications

Accessibility Contact us

 0303 123 1113

OGL

All text content is available under the Open Government Licence v3.0, except where otherwise stated.