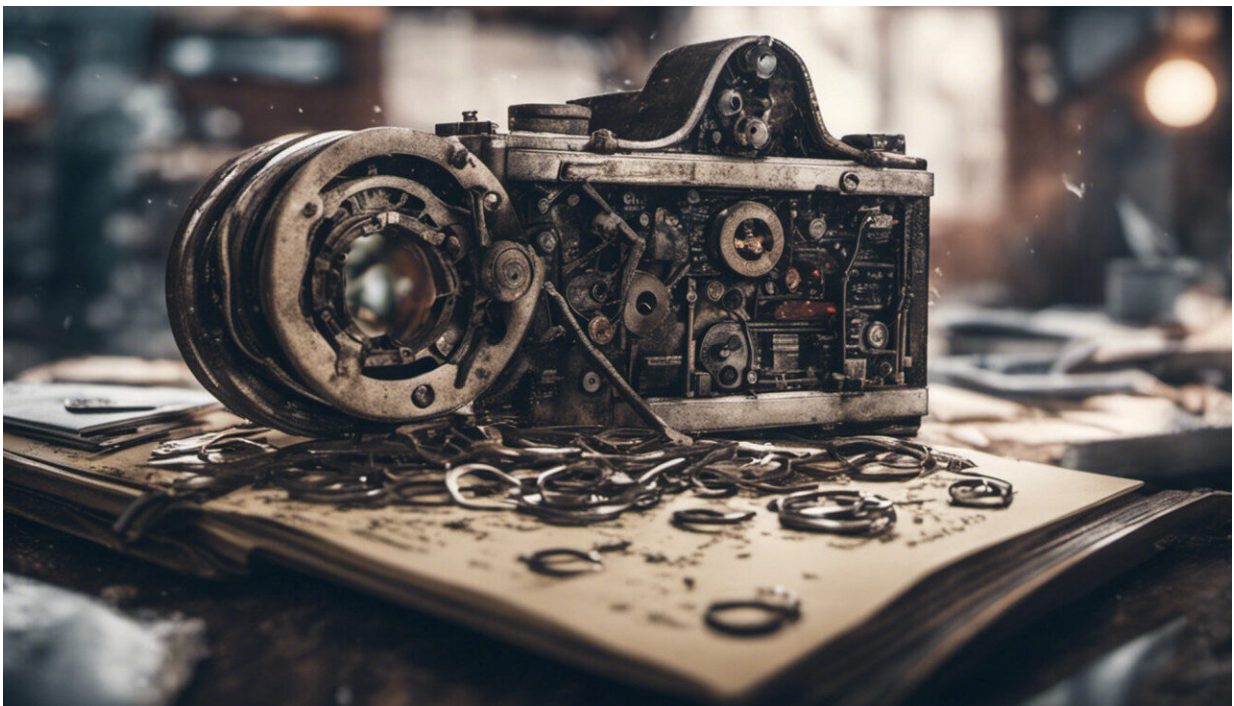# Why do I get so much spam and unwanted email in my inbox? And how can I get rid of it?

September 21 2023, by Kayleen Manwaring

Credit: AI-generated image (disclaimer)

Spam might not have brought an end to the internet or email, as some dire predictions in the early 2000s claimed it could—but it's still a massive pain.

Despite all the spam being removed by spam-filtering technologies, most people still receive spam every day. How do these messages end up flooding our inboxes? And are there any legal consequences for the senders?

What is spam?

The Organization for Economic Co-operation and Development (OECD) noted in 2004 "there does not appear to be a widely agreed and workable definition for spam" across jurisdictions—and this remains true today.

That said, "spam" generally refers to unsolicited electronic messages. These are often sent in bulk and frequently advertise goods or services. It also includes scamming and phishing messages, according to the OECD.

Most people think of spam in the form of emails or SMS messages. However, what we now call spam actually predates the internet. In 1854, a spam telegram was sent to British politicians advertising the opening hours of dentists who sold tooth-whitening powder.

The first spam email came more than 100 years later. It was reportedly sent to 600 people on May 3 1978 through ARPAnet—a precursor to the modern internet.

As for how much spam is out there, the figures vary, possibly due to the various definitions of "spam". One source reports the average number of spam emails sent daily in 2022 was about 122.33 billion (which would mean more than half of all emails were spam). As for text messages, another source reports a daily average of 1.6 billion spam texts.

Where do spammers get my details?

Each time you enter your [email address](#) or [phone number](#) into an e-commerce website, you may be handing it to spammers.

But sometimes you may even receive spam from entities you don't recognize. That's because businesses will often transfer customers' contact information to related companies, or sell their data to third parties such as data brokers.

Australia's Privacy Act 1988 somewhat limits the transfer of personal information to third parties. However, these laws are weak—and [weakly enforced](#).

Some entities also use "address-harvesting" software to search the internet for electronic addresses that are captured in a database. The collector then uses these addresses directly, or sells them to others looking to send spam.

Many jurisdictions (including [Australia](#)) prohibit these harvesting activities, but they are still [common](#).

Is spamming against the law?

Australia has had legislation regulating spam messaging since 2003. But the [Spam Act](#) surprisingly does not define the word "spam". It tackles spam by prohibiting the sending of [unsolicited commercial electronic messages](#) containing offers, ads or other promotions of goods, services or land.

However, if the receiver [consented](#) to these types of messages, the prohibition does not apply. When you buy goods or services from a company, you will often see a request to click on a "yes" button to receive marketing promotions. Doing so means you have consented.

On the other hand, if your phone or inbox are hit by commercial messages you haven't agreed to receive, that is a breach of the [Spam Act](#) by the sender. If you originally signed up to receive the messages, but then unsubscribed and the messages kept coming after [five business days](#), that is also illegal. Senders must also include a [functioning unsubscribe facility](#) in every commercial message they send.

Spammers can be penalized for breaches of the Spam Act. In the past few months alone, [Commonwealth Bank](#), [DoorDash](#) and [mycar Tyre & Auto](#) were fined more than A$6 million in total for breaches.

However, most spam comes from outside Australia where the laws aren't the same. In the United States spam is legal under the [CAN-SPAM Act](#) until you opt out. Unsurprisingly, the US [tops the list](#) of countries where the most spam originates.

Although spam sent to Australia from overseas [can still breach](#) the Spam Act—and the Australian Communications and Media Authority (ACMA) co-operates with overseas regulators—overseas enforcement actions are difficult and expensive, especially if the spammer has disguised their true identity and location.

It's worth noting that messages from political parties, registered charities and government bodies aren't prohibited—nor are messages from educational institutions to students and former students. So while you might consider these messages as "spam", they can legally be [sent freely without consent](#). Factual messages (without marketing content) from businesses are also legal as long as they include accurate sender details and contact information.

Moreover, the Spam Act generally only covers spam sent via email, SMS/MMS or instant messaging services, such as WhatsApp. Voice calls and faxes aren't covered (although you can use the [Do Not Call Register](#)

to block some commercial calls).

Staying safe from spam (and cyberattacks)

Spam isn't only annoying, it can also be dangerous. Spam messages can contain indecent images, scams and phishing attempts. Some have malware (malicious software) designed to break into computer networks and cause harm, such as by stealing data or money, or shutting down systems.

The Australian Cyber Security Centre and ACMA provide useful tips for reducing the spam you get and your risk of being hit by cyberattacks. They suggest to:

1. use a spam filter and block spammers—email and telecommunications providers often supply useful tools as part of their services
2. unsubscribe from any emails you no longer want to receive—even if you originally agreed to receive them
3. remove as much of your contact details from websites as you can and always restrict the sharing of your personal information (such as name, birth date, email address and mobile number) when you can—beware of pre-ticked boxes asking for your consent to receive marketing emails
4. install cybersecurity updates for your devices and software as you get them
5. always think twice about opening emails or clicking on links, especially for messages promising rewards or asking for personal information—if it looks too good to be true, it probably is
6. use multi-factor authentication to access online services so even if a scam compromises your login details, it will still be difficult for hackers to break into your accounts
7. report spam to your email and telecommunications providers,

and to [ACMA](#).

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation