

# A guide to help you protect your mobile phone from spam and scam



This is a guide to help you protect your mobile phone from spam and scam. It also explains where you can get help.

## What is spam?

There are three main types of illegal spam messages you can receive on your mobile:

- Unsolicited messages that have been sent to you without your consent.
- Unidentified messages sent to you without clear identification of the sender.
- Unstoppable messages that don't have a working "unsubscribe" facility.

## What is a scam?

Mobile scams are designed to trick you into:

- Using 19x (SMS and MMS services) numbers that are charged at a premium rate for every message you send and receive.
- Calling 190x (voice services) numbers that are charged at a premium rate.

## Steps you can take to help guard against spam and scams

### 1. Protect your number – prevention is the key

- Be careful when registering your mobile phone details with any organisation, signing up or giving out your details. Do they need your number and what will they use it for?
- Read the fine print carefully to find how your mobile number will be used if you register your contact details. Companies can legitimately send you advertising with your consent, but you can opt out. Is there a box you can tick to say you don't want to receive advertising about "similar products or offers"?
- Use caller ID blocking to hide your number when calling.
- Check how much it will cost before dialling a premium voice number (190x) or using a premium text (19x) number – especially if it's a response to an unsolicited voice call or text message.

### 2. Ask questions

Ask questions if you have any doubts or you don't understand. A company offering genuine products and services should answer all your questions.

**Who and where is the message from?** If you receive an SMS or MMS message offering a product or service, does it include:

- The name of the organisation or individual who sent the message?
- Contact details?
- A way of opting out?

Legitimate commercial messages sent from Australian businesses are required by law to include this information. If they don't, it could be scam or spam.

**What, when and how much?** If you receive an offer sent to your mobile phone, ensure that you know how much it will cost.

- Is it a one-off cost or are you signing up to the ongoing cost of a subscription service?
- If it is a subscription service, is there a minimum term?
- How does the pricing work? Are you paying to receive calls and messages as well as send them?
- What is the total cost of the service?
- How do you opt out or cancel the subscription?

Australian  
Mobile Telecommunications  
Association  
ABN 98 065 814 315  
First Floor  
35 Murray Crescent  
Griffith ACT 2603 Australia  
PO Box 4309  
Manuka ACT 2603 Australia  
Ph +61 2 6239 6555  
Fax +61 2 6239 6577  
Web [www.amta.org.au](http://www.amta.org.au)

**Does the offer sound too good to be true?** If you have received an offer that is too good to be true – it probably is!

- Be wary of “free” offers. Are they really free or are you paying for them elsewhere?
- If you read the words “T&Cs apply” or “Conditions apply”, find out what they are because the offer may not be so tempting when you consider all the terms and conditions.

### **3. Check before you reply**

If you receive an unusual text message from a number you don't recognise:

- Check the number before replying, particularly if all you can see is a name.
- If the number begins with “19” it is a premium rate service and you are likely to be charged a higher rate for a text or call. You may be charged for future text messages that you receive as well as messages you send.
- If you don't think you subscribed to the service, it could be a scam.
- Check if your mobile phone company offers a service allowing you to check a number to find out which company sent the text.

### **4. Check your bill**

Always check your bill for any charges you did not authorise. Premium rate calls and subscription services should be included on your bill. Contact your mobile phone company if you have any questions.

Check if your mobile phone company can place a monthly spending limit on premium SMS services. Some mobile phone companies impose an automatic monthly spending limit on the total bill, which they may be able to reduce.

## **Help and further information**

If you think you've been spammed or scammed, your carrier may be able to help. In addition, you can make complaints about spam to:

### **Australian Communications and Media Authority (ACMA)**

ACMA is responsible for enforcing the *Spam Act 2003* (Cth) and a range of telecommunications regulations. Contact ACMA on: 1300 850 115 or via their website at [www.acma.gov.au](http://www.acma.gov.au)

The following organisations may also be able to assist:

### **Australian Competition and Consumer Commission (ACCC)**

The ACCC is responsible for administering the *Trade Practices Act 1974* and has a wealth of information to help consumers identify and deal with scams, including a free newsletter, Consumer Express, which provides information on the latest types of scams.

See: [www.scamwatch.gov.au](http://www.scamwatch.gov.au)

Or phone the ACCC infocentre on: 1300 302 502

### **Fair Trading**

Your local Office of Fair Trading is responsible for administering consumer-based laws and looking after the rights of consumers. They also have information about the latest scams.

Contact details for all Fair Trading Offices can be found at: <http://www.scamwatch.gov.au/content/links/links.asp>

### **Australian Securities and Investments Commission (ASIC)**

ASIC enforces and regulates company and financial services laws to protect consumers, investors and creditors. If you want to check if a company is legitimate, you can look at the ASIC website at [www.asic.gov.au](http://www.asic.gov.au), or phone ASIC on 03 5177 3988.