



If it sounds
too good
to be true ...

... it probably is

Scams aim to take your money— watch out for:

- unsolicited offers arriving by email, SMS (short message service) or MMS (multimedia message service)
- enticing subjects with promises of lottery wins, wealth or weight loss
- emails using lots of capital letters, bad spelling, different fonts, unusual subject headings or with text appearing in images
- work-at-home schemes offering easy ways to make money
- incredible health claims for difficult-to-cure conditions and illnesses
- ‘phishing’ emails pretending to be from a bank or other legitimate company asking for your account details (usually by providing a link to a fake login page)
- lottery, sweepstakes, or other prize wins—asking you to send money or personal details to claim your winnings
- ‘Nigerian scams’ asking for money or assistance to release a small fortune from a distant country and promising a share of the fortune in return
- modem jacking—make sure ‘free’ adult sites don’t download internet diallers, as you may end up with a big phone bill.

How to protect yourself

- ✗ If you are unsure about the sender, delete the message—don’t reply or try to unsubscribe to the email or SMS as it will confirm your address and you may receive more spam.
- ✗ Never send your personal, credit card or online account details out in an email.
- ✗ Don’t access banking and other online accounts from an email link—use a bookmarked link or type in the address.
- ✓ Always check the website address carefully, scammers often set up fake websites with very similar addresses.
- ✓ Always read the terms and conditions carefully, ‘free offers’ often have hidden costs.
- ✓ Check the business name at www.asic.gov.au (Australian businesses only). You can also search for the business name or scheme through a search engine.
- ✓ Install software that protects your computer from viruses and unwanted programs and keep it up-to-date.

**spam
and
scams**

**SPAM is unsolicited email—
usually promoting a SCAM.**



**For further information
and to report **scams****

ACCC's SCAMwatch website
www.scamwatch.gov.au

ACCC Infocentre
1300 302 502

**For further information
and to report **spam****

Australian Communications and
Media Authority's website:
www.spam.acma.gov.au

