DIGITAL FRONTIERS— E-COMMERCE AND CONSUMERS

Spam is illegal

Spam is unsolicited electronic junk mail. It quickly overloads inboxes and typically contains get-rich-quick cons, scam offers, 'miracle' cures. Current figures estimate that spam constitutes over 50 per cent of all emails received.

To stop this menace, governments across the world have introduced anti-spam legislation. The *Australian Spam Act 2003* was effective from 10 April 2004 and is enforced by the Australian Communications Authority (ACA).

Under the spam legislation it is illegal to send unsolicited commercial electronic messages whether or not the content is itself legal or illegal. The Act requires all commercial electronic messages to contain accurate sender information and a functional unsubscribe facility. The Act covers emails, SMS (mobile phone text messages), MMS (multimedia messaging service or mobile phone graphic messages) and instant messaging with an Australian link, but it does not cover fax or telemarketing.

The internet and e-marketing industries are developing codes of conduct which will detail and supplement the basic prohibitions of the Spam Act. Once presented to the ACA these codes will be considered for registration under the Telecommunications Act.

For more information on spam and the Spam Act 2003

General inquiries about the Act can be made with the ACA on 1300 855 180 or via the ACA website using an online form. Go to www.aca.gov.au.

Report spam

You can report spam to the Australian Communications Authority.

To report or make a complaint about spam visit the ACA website and click on 'Spam'.

If you are concerned about the content in the spam—e.g. pornography—report it to the Australian Broadcasting Authority at www.aba.gov.au.

Too good to be true

This February the ACCC led consumer protection agencies from 24 countries in scouring the internet to uncover shonky websites promoting products which are simply too good to be true.

The joint exercise involved 76 agencies worldwide in what was the sixth annual international internet sweep conducted by members of the International Consumer Protection and Enforcement Network.

The ACCC held a key role in the sweep, dedicating a specialist team in its e-commerce division to designing and developing internet search terms, protocols and evaluation guidelines for colleagues to use worldwide.

> Guaranteed Cash Prize… Make Big Bucks…
> You're a Winner… Internet Millionaire…
> Be Your Own Boss… Become a Distributor…
> Free Diploma… No Qualifications Needed…

These are just some of the terms used by participating agencies to scrutinise websites. Most suspicious websites were work-at-home type schemes and get-rich-quick schemes which grossly exaggerate earnings potential. Others were lottery scams, pyramid selling and multi-level marketing plans, prizes and 'free' offers which were not actually free.

Globally a record 1847 suspicious sites were flagged by sweepers. Participating agencies are now acting on results to educate traders about compliance, advising consumers about how to avoid being duped, seeking settlements and taking enforcement action.

The ACCC has had extremely positive outcomes from the sweep. So far 60 per cent of the 40 traders contacted by the commission for posting websites identified as containing alleged misleading representations have been resolved. This includes traders offering consumers full refunds, the removal of entire sites and amending or removing misleading representations.

Scammers are increasingly using the internet to try and make a fast dollar and take advantage of vulnerable consumers. Heed this caution: if it looks too good to be true, it probably is.

Cyberscam scams

Dear Banking Customer

This email was sent to you by YOUR BANK server to verify your email address. You must complete this process by clicking on the link below and submitting YOUR BANK secure verification form which appears in your browser.

And so begins one banking scam email currently doing the inbox rounds. Known as 'phishing' because the scammers send out bait hoping for a catch, this type of scam has become more sophisticated in recent months—the fake banking sites look more authentic and the email messages sound very convincing. Consumers and businesses are being persuaded to provide personal banking details, leaving their hard earned cash ready for the taking.

Internet scams, like their more traditional cousins, try to appeal to all types of people—those who want to get rich, have a perfect body, get well or even help the needy. Other scams target those who are busy, have trouble with language, are elderly or are too young to understand.

Viruses, worms and trojan horses

Today's cyberscammers not only rely on fooling the consumer through bogus websites and scam emails, they also produce computer programs and attachments that spy on you as you type in your banking password, take over your modem and dial into a premium number or send themselves out to your friends via your email contacts.

Not all security software will protect your computer from all outside attacks. Not all anti-virus software, for example, will protect you from spyware or trojan horses such as internet diallers.

It is best to discuss computer security with a software or computer professional especially if you receive a lot of spam, shop or bank online or you are a regular visitor to adult sites. Remember to keep all your security software and firewall utilities up to date.

Protect yourself

Avoid accessing banking and ticketing sites from email links—use bookmarked links or type in the address yourself. Check with your bank first. A little extra effort could save you your life savings.

Read all the terms and conditions when purchasing online. Check the trader's contact details, security, privacy policy and what recourse is offered if there is a problem. If the trader is based overseas it might be difficult to get a refund.

If you visit adult sites avoid accessing them from spam and be wary of 'free sites'. Regularly check your desktop for signs of internet diallers and when logged onto these sites, check that you have not been switched to a premium number via your modem.

Delete all spam—never reply as this confirms your email address to the spammer. Also some spam will download unwanted attachments that could cause problems with your computer or redirect your modem to premium numbers.

If you feel you are getting a lot of spam, filtering software may help. Check if your ISP or email service/application provides a filtering option. Failing that, you might consider getting a new email address.

Check the trader's credentials online—see our 'Tips to avoid ripoffs' on page 10.

Where to report a cyberscam

The ACCC's *Slam-a-Cyberscam* accepts complaints online at www.accc.gov.au; click on Consumer Rights/internet shopping.

International online scams, go to www.econsumer.gov

More information on cyberscams

The ACCC has published a new consumer guide on *scams and spam*. Copies are available from the ACCC infocentre on 1300 302 502 or go to the ACCC website www.accc.gov.au.

Financial scams

www.asic.gov.au

More information on spam

www.aca.gov.au

Safe sex surfing

Modem jacking and internet dumping occur when a computer user is disconnected from their usual ISP and reconnected via an international or premium number without being informed or agreeing to the new connection. The end result—consumers are unaware they have been 'jacked' or 'dumped' until an alarming phone bill arrives.

A high incidence of internet dumping occurs when consumers are accessing 'free' adult sites. While not all adult sites are run by scammers, this is a lucrative industry with one recent report estimating it as a US$2.5 billion industry. Twenty-five per cent of all internet search queries are related to sex and there are currently more than one million adult domain names registered. Given these statistics it's not surprising that online adult entertainment is a potential scammer's paradise.

How do scammers do it?

This is not a definitive list. New scams are always just around the cyber corner.

Pop-up windows are a common ploy of scammers to trap unsuspecting consumers into a site that has been triggered via spam or unwittingly accessed by random surfing. The windows 'pop-up' in quick succession and in an attempt to close an open window, consumers can be tricked into agreeing to enter a paid site. Sometimes the consumer's only apparent option is to click 'Continue'.

Pop-up windows that appear every time the computer is switched on or whenever the internet is accessed can mean that the computer has an internet dialler or cookie in its system that re-activates the unwanted windows. A dialler is software that is programmed to dial into a number that will take you into a pay-to-view site. Cookies are small files that are saved to your hard drive from websites you have visited. The main purpose of cookies is to identify users and possibly prepare customised web pages for them.

On a well run site consumers are given the option to download a dialler that will dial into a premium number and disconnect them from their regular ISP. When a consumer is 'internet dumped' there is no warning or opportunity for the consumer to agree to a dialler download. Diallers can download themselves either from 'free' adult sites or spam. Some diallers are activated through music or game download sites.

Some scammers do provide warnings or dialogue boxes offering options and explanations but they are often in a foreign language making an informed choice difficult. Sometimes the information is worded in such a way that by clicking 'no' it actually means 'no I don't want to leave' so the user ends up in a premium paid site.

Unauthorised and authorised dialler downloads usually result in a small icon becoming visible on the desktop or task bar. This icon can be used to re-connect to chosen websites. But it is also your clue that you have imported a dialler into your system.

How to protect yourself

Avoid accessing adult sites from spam and be extra wary of sites that offer 'free access'.

When visiting adult sites, be on the alert for any dialogue boxes that may trick you into a paid site.

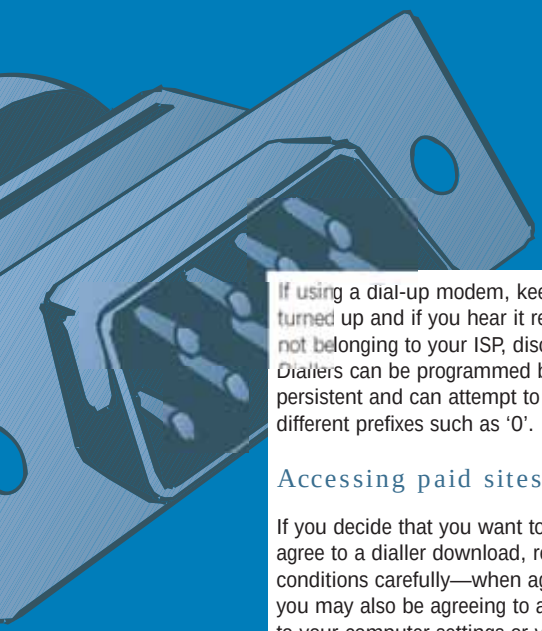
Watch out for internet diallers that are either disguised as innocent downloadable files, such as a games file, or that download automatically.

Check your computer for unusual icons on the desktop especially if adult sites or pop-up windows open whenever you boot-up your computer.

You should run checks for unwanted diallers in the program list on your computer. In a Windows environment this can be done by opening the Control Panel and inspecting 'Add or Remove Programs'. A dialler can be spotted and removed here but they can also imbed themselves deeper into your computer system. Software applications are available to help remove unwanted programs and you should discuss these options with a computer professional or ask for further assistance to remove diallers manually.

Some diallers are programmed to readjust your internet settings via your web browser software. To run a check on Internet Explorer go to 'Tools/Internet Options' where there are a number of options including 'Connections'. A premium number that connects you to a dialler will be visible in these options. Also, if your computer has the option of setting your home page, it is worthwhile checking to see if the connection has been transferred to an adult site.

You can also set your computer not to access cookies. This setting can be done via your web browser.



If using a dial-up modem, keep the modem volume turned up and if you hear it redialling to a number not belonging to your ISP, disconnect immediately. Diallers can be programmed by scammers to be very persistent and can attempt to dial repeatedly using different prefixes such as '0'.

Accessing paid sites

If you decide that you want to access paid sites and agree to a dialler download, read all the terms and conditions carefully—when agreeing to some diallers you may also be agreeing to accept pop-ups, changes to your computer settings or various other future communications from the website/dialler company.

If paying by credit card check that the payment area is secure and, once again, read all the terms and conditions carefully.

Some sites offer short-term access via credit card payment. Check cut-off dates and be very sure of how to 'unsubscribe'.

Keep a check on who uses the internet at home. Large phone bills may result from children accessing paid sites.

A bar on international or premium numbers can help to avoid surprising phone bills but scammers can be very determined. New billing numbers are always becoming available. A bar can be placed on these numbers by contacting your ISP or telephone services provider.

Firewalls and specialised computer security software will help guard your computer from unwanted downloads. Keep these up to date and discuss the best option with a software specialist.

How can I prove I have been dumped?

Consumers who believe they have been 'internet dumped' often find it difficult to prove their case. The billing company insists that a premium service was accessed and it's the company's word against that of the consumer.

Scammers also rely on consumers being too embarrassed to report complaints to a regulator.

You can help prove your claims of dumping by regularly reviewing your internet history plus keeping:

» copies of temporary internet files

» a copy of the dialler software

» a log of internet use from your ISP.

For more information on how to find these files and to copy the dialler software ask a software or computer specialist or go to the Q&A section of the TISSC website www.190complaints.com.au. TISSC is an independent regulatory body that deals with 190 number complaints.

If you visit adult sites regularly you should consider putting a long expiry date on your internet history record to allow you to cross check billing invoices when they arrive at some future date. This can be done through your web browser menu bar.

What else do I need to know before I dispute my bill?

To dispute any bills it will be easier if you keep all the details of your internet surfing well documented. Review and record your internet history and usage as outlined above and keep this information with the original billing invoices and correspondence from the billing company.

Make detailed notes of any conversations with the billing company including time, date and name/s. This same information will be useful if you feel your dispute has not been resolved and you take your complaint to a regulator.

Also check all the details on your bill. Is it your current address, name and phone number? Cross reference the date and time for the service with your internet history and log from your ISP.

To complain or for more information

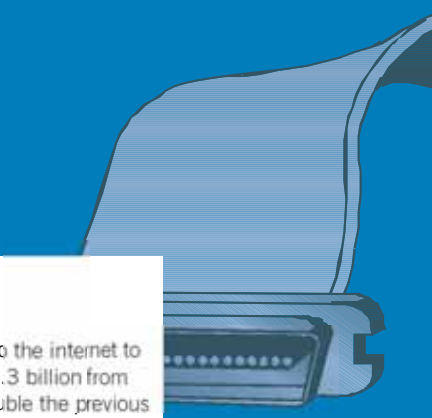
Telecommunications Industry Ombudsman, www.tio.com.au

TISSC, www.190complaints.com.au

Australian Communications Authority website, www.aca.gov.au

ACCC Infocentre, 1300 302 502 or www.accc.gov.au

Office of Fair Trading in your state or territory



Tips to avoid ripoffs

Protect yourself from cyberscams and rip-offs. Before subscribing to a scheme, check the credentials of the cybertrader.

- Run an internet search using your favourite search engine.
- Run a business search to confirm a trader's company details. Australian business searches can be done at www.asic.gov.au.
- Run a 'whois' search. This will tell you who has registered the website. For 'au' sites go to www.auregistry.com.au. For global listings go to www.samspade.org or www.dnsstuff.com.
- Sites that list known scams and bogus traders:
  - SA Office of Consumer and Business Affairs, www.ocba.sa.gov.au/scams
  - WA Dept of Consumer and Employment Protection—ScamNet, www.docep.wa.gov.au
  - NZ Ministry of Consumer Affairs—Scamwatch, www.consumeraffairs.govt.nz
  - ASIC–FIDO for financial tips and safety checks, www.fido.asic.gov.au/fido/fido.nsf
  - UK Dept of Trade and Industry, www.dti.gov.uk/ccp/scams/page1.htm
  - Scambusters, www.scambusters.com
  - Scam Watch, www.scamwatch.com
  - National Consumers League National Fraud Information Center, www.fraud.org
  - UK Trading Standards Centre and UK Dept of Trade and Industry, www.ripofftipoff.net

Other online resources

- www.scamwatch.gov.au
- www.consumersonline.gov.au

Your online rights

More and more Australians are turning to the internet to shop. Australian businesses earned $24.3 billion from online sales in 2002–03, more than double the previous year of $11.3 billion.[1] The ACCC warns consumers that it is increasingly important that they understand their rights when shopping over the internet—consumers have the same basic rights online as they do offline.

Regardless of whether a consumer has clicked 'I agree' to a seemingly endless list of terms and conditions, certain rights cannot be excluded. For example, a vendor must ensure representations made on a website under its control are accurate, and goods must be fit for sale and fit for their purpose.

The ACCC recently surveyed the top 1000 Australian consumer websites and is now sounding the alarm for consumers—their rights under the Trade Practices Act are commonly being misrepresented, often leading consumers to believe they have far fewer rights than they actually do.

A significant proportion of online terms and conditions fail to convey to consumers an appreciation of the protection they have under the Act—consumers have the same protection online as they do in the bricks and mortar world. Under the Act, these obligations can even apply to Australian businesses operating outside Australia.

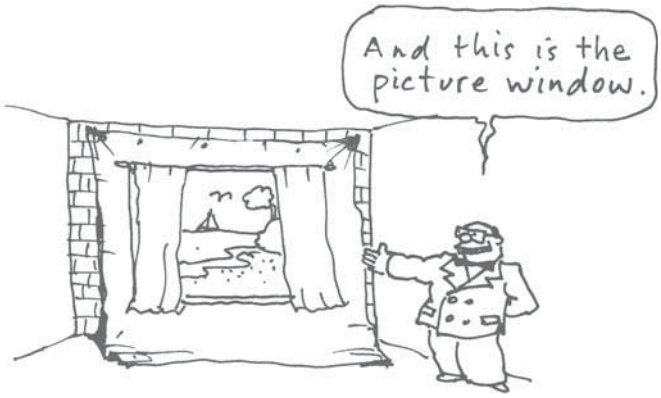
Even though consumer warranties and refund rights can in some cases apply when the trader is overseas, consumers must realise that in particular cases the warranty and refund procedures may be different and they should expect to see these rights stated. Also, if the trader is overseas, the consumer's chances of getting a warranty or refund will be considerably weakened.

The ACCC is responding to concerns raised by misleading online terms and conditions. Initiatives include an awareness campaign for businesses to educate vendors about their obligations when trading online. Particular emphasis is placed on the need for businesses to conduct self-regulated reviews of their online terms and conditions in keeping with the Act.

In April the ACCC launched a consumer education campaign, releasing a brochure and information for media about consumer rights when buying over the internet. The ACCC will continue to investigate top consumer sites to assess the impact of the current education campaigns and develop further strategies to protect consumer rights in the virtual world.

For more information see the ACCC refunds and warranties checklist on page 22 or download a brochure from the ACCC website www.accc.gov.au.

1 The Australian Bureau of Statistics cautions that the method for gathering the sample has changed from previous years, therefore direct comparisons are difficult



Get real

Real estate agents operate in a highly competitive and often cut-throat market-place. Nevertheless, as a prospective home owner, vendor or tenant, you are entitled to get the full picture to make informed decisions when buying, selling or leasing property.

Late last year the ACCC launched a campaign targeting property 'scammers' and has since been inundated with many hundreds of complaints and inquiries about the real estate industry. The ACCC's concerns include:

- misleading conduct by real estate agents and auctioneers, including dummy bidding and misleading photographic representations
- real estate investment seminars
- two-tier marketing
- advice given by financial consultants, solicitors and valuers
- unconscionable conduct by financial institutions.

About two-thirds of property related complaints to the ACCC concern the conduct of real estate agents and auctioneers.

Although most consumers concede that a certain amount of leeway in property advertising must be given to allow for the real estate agent's enthusiastic vision, remember this: anyone who relies on what an agent says or does, or relies on advertising—and is misled or deceived—can take legal action under the Trade Practices Act.

Is this the full picture?

An agent advertises a block of land with a photograph that includes a portion of the unfenced neighbouring block. The photograph has also been modified to remove overhead wires and power poles.

This conduct is likely to mislead or deceive any person relying on the photograph to give them an impression of the land on offer.

Remember—it is not necessarily relevant whether the agent actually intended to mislead anyone to establish a breach of the Act. What is relevant is the overall impression created by the conduct, and its actual or likely effect on the target audience.

Silence can mislead

Linda and David attended an investment seminar and were subsequently flown to a development location to view investment properties. The couple fell in love with one property, particularly the bushland corridor just beyond the back fence. They intended to rent the property until their retirement, then move in and enjoy the lush surrounds. The agent agreed it would be a peaceful place to retire.

The asking price was a bargain as the charts they were shown depicted prices in the area to be around $30 000 more. The agent said there were two other couples coming that afternoon to view the property. Linda and David snapped it up taking advantage of the low conveyancing fees of the onsite solicitor.

One month later, the bushland behind the property was cleared to make way for a four-lane arterial road. Their dream of a quiet retirement home nestled in the trees was shattered faster than the asphalt was laid.

Misleading or deceptive conduct can include acts of silence or omission. In this case, the information provided by the solicitor should have included the proposed road development. The company hosting the investment seminar may also be liable if they knew of the road development.

An agent should ensure a buyer is aware of all the important matters that should be mentioned, especially when silence would create an incorrect impression in the context of what other representations have been made.

The ACCC in conjunction with the Real Estate Institute of Australia (REIA) has produced an industry guide, *Fair and Square: a guide to the Trade Practices Act for the real estate industry*. The guide is available ($10) by contacting the ACCC Infocentre on 1300 302 502. More information can also be located on the ACCC website at www.accc.gov.au or the REIA website at www.reia.com.au.