April 2004

ACCC InfoLink

# Protecting your business from cyberscams

Australian Competition & Consumer Commission

## How do I find out more?

Contact the ACCC Infocentre

**Phone**: 1300 302 502
**Email**:infocentre@accc.gov.au

**What is spam?**
Spam is unsolicited electronic junk mail. It is estimated that approximately 50 per cent of all emails are spam. Australia has joined other countries in introducing legislation to try to combat spam. The Australian *Spam Act 2003* became effective on 10 April 2004 and is enforced by the Australian Communications Authority (the ACA).

Under the Act it is illegal to send or cause to be sent 'unsolicited commercial electronic messages' that have an Australian link. The Act covers emails, SMS (mobile phone text messages) and instant messaging but it does not cover fax or telemarketing. For details of the new Spam Act: www.aca.gov.au.

Spam is often used to promote scams. While the ACCC does not regulate the **sending** of unsolicited commercial electronic messages it has powers under the Trade Practices Act to take action against misleading **content** in spam.

### How to report spam or cyberscams

**Australian online scams**
ACCC Infocentre 1300 302 502
ACCC's online slam-a-cyberscam at www.accc.gov.au

**International online scams**
www.econsumer.gov

**Banking and financial scams**
ASIC at www.asic.gov.au

**To report spam**
The Australian Communications Authority at www.aca.gov.au

## Did you know?

Today's cyberscammers don't only rely on bogus websites and scam emails. They also produce computer programs and attachments that can spy on you as you type in your banking password or disable your computer resulting in lost productivity and revenue.

**Online banking scam**
Picture this: you are in the office of a small business. The BAS for this quarter needs to be finalised, someone needs an adjustment to their pay, new forms on changes to super have arrived, the supplier has changed his delivery dates so the month's schedule needs re-adjusting and to top it all off the photocopier has given up!

An email arrives from the bank. They are updating their security information and they ask you for personal information and direct you to log into the website link attached. You log on and confirm your details. Done—one less thing to do!

Unfortunately this small business has just been taken in by a scam. The bank account is now open to fraudulent activities as not only were the email details provided but also other banking security information through a very authentic-looking sham bank website.

Such scams target the small business with its busy office, tight schedule and often overworked staff. These banking scams known as 'phishing' (as in angling for a catch) are currently one of the most publicised email scams. Watch out for scam emails pretending to be from the Australian Taxation Office! If in doubt log onto www.ato.gov.au.

The ACCC uses its educative role to inform businesses about such scams so that they can be alert and avoid getting caught!

**Fake invoices**
Fake invoices requesting payment for domain name renewals, registrations and associated services are still very prevalent. Businesses do get tricked into paying inflated prices for domain name renewal or pay for unnecessary additional domain names such as .com or .net. Some of these domain name reseller scammers are now so well known that they can find it hard to register a .au and now tend to offer .com sites. On 27 April 2004, following ACCC action, the Federal Court restrained Domain Names Australia P/L and its director for a three-year period from sending out misleading and deceptive notices inviting the recipient to register a particular domain name.

**Modem jacking**
Is the email with an attachment that you've just received an order from a new client or spam? Sometimes spam can contain a program that copies itself onto your computer once you open the attachment. In rare cases the program causes your modem to dial a premium or overseas number that can add significant costs to your phone bill.

**Stealing a business name**
Cybersquatting occurs when someone buys up domain names that they think might be valuable to someone else and then try to sell it for large sums of money. In Australia the regulatory authority AuDa offers protection from these occurrences. Where a domain name is in dispute, your right to use it can be assessed by your previous use of the name. Many businesses have used the Trade Practices Act prohibition against 'passing off' to protect their business name from others using similar names.

### Handy tips

Avoid accessing banking sites from email links—use bookmarked links or type in the address yourself. Check emails with your bank first. A little extra effort could protect the money in your account.
Domain name registrations (.au) are renewed every two years. Keep a good record of domain name registration details, including the name of the registrar and the renewal date.

Read the terms and conditions when buying online. Time spent here could save you money and heartache. Check the trader's contact details: Do they have a street address? An email address? Can you contact them with any questions? Do they have security and privacy policies? If the web address does not end in .au the trader may be located overseas and it may be difficult to get a refund or discuss a problem.

Typing the name of a trader or a business scheme into a search engine can sometimes provide extra information. There are also several sites that list scams and bogus traders. Office of Fair Trading websites will sometimes have consumer alerts about traders and FIDO the ASIC consumer site has information on financial scams.

A business search can also be useful to confirm a trader's details although this is not an indicator of the trader's behaviour in the marketplace. Australian business searches can be done on ASIC's 'National Names Index' at www.asic.gov.au. You can find out some basic information—for example a business's ABN and location for free.
A 'whois' search can tell you who has registered the website. These can be done at a number of places e.g. www.samspade.org or for '.au' sites www.ausregistry.com.au.

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 spam is a problem, filtering software may help. Check if your ISP or email service/application provides a filtering option.

### Publications

*Scams and spam* at www.accc.gov.au

*Spam Act 2003: an overview for business* at www.aca.gov.au

*Spam Act 2003: a practical guide for business* at www.aca.gov.au

*Staking your claim on the web* at www.noie.gov.au