



Australian
Competition &
Consumer
Commission

Small business scams

Scams targeting small businesses come in various forms—from invoices for advertising or directory listings that were never requested to dubious office supplies that were never ordered. More recently, overpayment scams and dodgy investment opportunities have been added to the mix.

Small business scams are becoming increasingly sophisticated and scammers will go to great lengths to convince you that the documents they send you or the offers they make are legitimate and genuine. But it's easy to copy or modify letterheads, names and logos to make them look real, and it's simple to create phoney websites, use fake credit cards or cheques and obtain business details such as your name and address through public listings or from your website.

You can protect yourself and your business by being aware of the common scams targeting small businesses.

What they are and what to look for

Overpayment scams

This sort of scam involves scammers making contact to purchase goods and services from you. They then send you a payment by cheque, money order or credit card for far more than the agreed price. The scammer then asks you to refund the overpayment or to pay the scammer's 'freight company'. The scammer is hoping you will transfer the refund or pay for 'freight' before you discover that their cheque has bounced or that their money order or credit cards were phoney.

- ✓ Be suspicious if you are overpaid for products.
- ✓ Be suspicious if a number of credit card numbers are used.
- ✓ Be wary of complicated or unlikely orders.

Trademark publication scam

This scam involves a scammer sending you an unsolicited letter or invoice for payment for a trademark listing. The scammer tries to give the impression that they are connected with the registration of trademarks by IP Australia (the official Australian Government intellectual property agency) or an overseas-based equivalent.

- ✓ Be wary and don't be fooled—publication in IP Australia's database is free and is automatic when a trademark is registered.

Directory entry or unauthorised advertising scam

This scam involves a scammer sending you an invoice by post, fax or email for a listing or advertisement in a magazine, journal or business register/directory which you did not authorise or request.

Scammers will send a proposal for a subscription, disguised as an invoice or 'renewal notice', for an entry on a questionable website or in a questionable trade directory. Often these businesses are based overseas. It may sound like a 'free' entry, but charges can be hidden in the fine print, resulting in demands for payment later.



Another common scam is calling a business to confirm details of an advertisement the scammer claims has already been booked or to ask if you would like a 'free trial'—it's only later that you find your business has actually been charged for the advertisement.

- ✓ Be careful—if you receive a request to confirm details of an advertisement, check your own records to see whether your business made this booking.
- ✓ Be aware that a scammer may quote a genuine entry or advertisement you placed in a different publication or directory to convince you to pay.
- ✓ Be careful—if you receive an offer for a free trial, check for any hidden terms.

If you refuse to pay, scammers often try to intimidate you by threatening legal action. Consult your lawyer if you are concerned about any threats of legal action by scammers.

Investment scheme scams

This type of scam usually involves telemarketing campaigns targeting small business owners. Peddled as tax-free opportunities, these are often sports betting schemes or betting software offers in disguise and are nothing more than gambling.

- ✓ Be wary of unsolicited offers described as ‘tax-free wealth’, ‘strategic investment’, ‘investment not gambling’, ‘recession proof’ or even ‘investing in the thoroughbred racing industry’—these schemes are **not** investment opportunities.

Office supply scam

This scam involves receiving and/or being charged for goods you never ordered or never received, or goods that were not what you thought you agreed to buy. The scammer will call you pretending to be your ‘regular’ supplier, telling you that the offer is a ‘special’ or is ‘available for a limited time’.

- ✓ Be careful—if the caller claims that your business has ordered or authorised something and you do not think it sounds right, ask for proof. Check that goods have actually been ordered and delivered before paying an invoice.

Domain name scam

Under this scam you’ll be sent either an unsolicited invoice or email for an internet domain name registration very similar to your own business domain name or a renewal notice for your actual domain name. The notice could be from a business that supplies domain names trying to trick you into signing up to their service or it could be from a scammer trying to take your money.

If you have a registered domain name and receive a renewal notice, check that it:

- ✓ Matches your current domain name exactly—look for small differences such as ‘.com.au’ instead of ‘.net.au’. Remember, even if the core business name is the same, it could be a completely new domain name.
- ✓ Comes from the company you originally registered your domain name with—and check for the actual expiry date for your existing domain name to confirm if it really is due for renewal.

If you want to take up the new domain name being offered, shop around for the best price first.

Fax back scam

This scam involves sending you unsolicited faxes offering anything from amazing diets to fantastic deals and competition entries. Scammers targeting businesses usually offer directory entries, trade and business lists, and catalogues of goods and services. These offers require you to send a fax back to a premium rate number (starting with 19) to accept.

- ✓ Be careful—premium rate faxes can be charged at more than \$6.00 per minute and the scammers make sure your fax takes several minutes to go through, which means you end up with high, unnecessary phone bills (a single fax could cost you \$20 or \$30!).

Warning signs

Scams succeed because they look like the real thing or try to take advantage of a busy office environment—don’t lose your hard-earned money! Protect yourself and your small business by being aware of the common tricks used by scammers.

Golden rules

Remember these golden rules to help you beat scammers:

- If you become aware of a scam, let other people and your industry association know about it.
- Keep your filing and accounting systems well organised—this will make it easier for you to detect bogus accounts and invoices.
- Never provide personal information and banking details to anybody you don’t know and trust.
- Make sure the business billing you is the one you normally deal with and ask for the name of the person you are speaking to and who they represent.
- Never give out any information about your business unless you know what that information will be used for.
- Do not agree to offers or deals straightaway—always ask for an offer in writing and consider getting independent advice if the deal involves money, time or a long-term commitment. Remember: if it sounds too good to be true, it probably is!
- Ensure that you have clear procedures for verifying, paying and managing accounts and invoices. Limit the number of people authorised to place orders or pay invoices.
- Install reputable computer protection software and a firewall—and keep them up to date.

What if you are scammed or want to report a scam?

If you spot a scam or have been scammed, you can contact a number of Australian Government agencies for advice or to make a report.

To find out which government agency is best placed to assist you, visit the ‘Report a scam’ page on the SCAMwatch website, www.SCAMwatch.gov.au.

SCAMwatch details some of the most common scams around; it’s designed to help you recognise and report scams and protect yourself from being ripped off by scammers.

Still unsure? If you need further advice or information, call the ACCC Infocentre on 1300 302 502.

ACCC contacts

ACCC Infocentre 1300 302 502

ACCC website www.accc.gov.au

Callers who are deaf or have a hearing or speech impairment can contact the ACCC through the National Relay Service, www.relayservice.com.au.

Voice-only (speak and listen) users, phone 1300 555 727 and ask for 1300 302 502.

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Commonwealth of Australia 2010

10 9 8 7 6 5 4 3 2 1

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Moreover, this publication avoids technical language where possible and may contain generalisations to which there are exceptions or important qualifications. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but accepts no liability for any loss or damage whatsoever attributable to reliance on any of that information.

ISBN 978 1 921581 50 2

ACCC 01/10_39679

Illustration by Pat Campbell