

Scammers continue to target businesses

k Principal Update



PRINCIPAL UPDATE 14/05

 Scammers don't only target consumers – they target small businesses too.

Scams can reach any business, regardless of its size, age, location or industry sector, and cause that business to lose money.

The ACCC's Targeting scams report 2013 reveals that over 90,000 Australians reported scams to the ACCC last year, with almost \$90 million reported lost.

The most common scam affecting small businesses is the false billing scam, which includes advertising, directory and domain name scams. In 2013, over 3,600 reports were received about this scam – an increase of 45 per cent from 2012 – and almost \$725,000 was lost.

This type of scam targets small businesses by tricking them into paying for unwanted or unauthorised listings or advertisements in magazines, journals, business registers or directories.

Common scam tactics are to send a business a subscription form disguised as an outstanding invoice to get the business to sign up for unwanted ongoing advertising services. Scammers also falsely claim that the directory or publication is well known or has a high readership.

Another common false billing approach used by scammers involves sending invoices for the renewal of domain names. Scammers will send businesses an invoice to renew their current domain name registration, however the domain name will be different, such as '.com' instead of '.com.au'. Other scams that target small businesses include office supply scams, overpayment scams and investment scheme scams.

If you run or work in a small business, protect yourself from scammers by following these golden rules:

1. Ensure you have clear procedures for verifying, paying and managing accounts and invoices. Limit the number of people authorised to place orders or pay invoices.
2. Make sure the business billing you is the one you normally deal with. Check whether all the details on the invoices you receive are the same as usual or whether some are subtly different.
3. Never provide personal information and banking details to anybody you don't know and trust.
4. Don't let anyone pressure you into making decisions involving payments or ongoing contracts. If you are unsure, always seek independent financial or legal advice.
5. Install reputable computer protection software and a firewall – and keep them up to date.

To learn more about false billing scams, watch this [SCAMwatch warning video](#). To keep aware of common scams and current scam trends, visit the [SCAMwatch website](#), sign up for [SCAMwatch radar alerts](#), and read the ACCC's [Small business scams factsheet](#) or [2013 Targeting scams report](#).

And if you become aware of a scam or are scammed, report it to the SCAMwatch Infocentre on 1300 795 995. Your report helps the ACCC to monitor scams and take action where appropriate, including to educate other small businesses on new or emerging scams.