enews

INFORMATION SHEET

FALSE BILLING

Small business owners are often busy, with many different tasks on their hands. At times, unscrupulous operators may take advantage of this and attempt to trick a small business owner into making a payment for something they didn't order, or to agree to goods or services that they don't need.

Typically, this trick involves an unscrupulous business sending realistic-looking invoices with what appears to be an official looking letterhead or logo. Other tricks include sending unsolicited facsimiles, emails or letters and follow-up invoices to entice businesses to subscribe to, and pay for, entries or advertising in online business directories or other publications.

These tricks generally rely on time-poor employees unwittingly paying invoices without checking if they know the sender or if they actually agreed to the advertising or directory listing.

There are several steps you can take to protect yourself and your business such as:

be wary of unsolicited offers, particularly those claiming to provide a free service, make sure you carefully read any fine print to fully understand the offer.

- make sure you know who you are dealing with before responding to any offer–do an internet search on the name of the product or company and verify contact and company details.
- look into the legitimacy and profile of a directory or publication – for example, ask for details of other local businesses who have previously listed or advertised and check with them that they received what they paid for.
- retain written records of authorisations for advertising or directory entries so that if you receive an invoice or a telephone call, you can go back to your records to check it.
- ensure that only authorised employees are responsible for payments and they should have ready access to important dates and suppliers. You should also keep these employees updated on any scam or unsolicited service that may target your business.

If you believe you have been targeted by an illegitimate trader or if you have already given sensitive information to an illegitimate source, you should immediately report it to the police and the Scamwatch website.