



## Small business scams

### The Set-Up

You receive an invoice for goods or services.

### The Hook

You don't check that you have ordered the goods or services that you have been invoiced for.

### The Sting

You pay invoices for things you never ordered.

## What a small business scam looks like

Running a business makes you a target for all kinds of scams, from being billed for advertising or directory listings you never ordered, through to non-existent offers for office supplies, and even claims for payment from make-believe government departments. Stay wary.

## Variations on small business scams

### False billing scams (also known as Pro-Forma Invoicing)

You receive a bill for a directory entry or for the placement of advertising. You pay it, not realising that the directory or magazine is either completely non-existent or printed solely for the purpose of perpetuating the scam on unsuspecting businesses.

Sometimes the bill is doctored to look like an invoice from a major media company.

Alternatively you may be offered free advertising, but in fact the order also covers further entries that must be paid.

Another spin on this is for the scammer's staff to call to confirm details of an advertising order ... even though your company or organisation never made such an order. The scammer may try to confuse you or your staff by referencing a real advertisement or entry you have made in a genuine publication.

The scammers may even try to tell you that the government has made it compulsory to be listed in their register.

If you refuse to pay, the scammers may try to intimidate you with threats of legal action. These threats are usually completely empty, but many businesses pay out before they realise the scammers will back down in the face of resistance.

More information:

- request proof of purchase before payment
- check with your colleagues
- ask for evidence that the publishing company has been commissioned by an organisation to publish the magazine on their behalf, if that is the claim. Check with the organisation
- keep records of contacts and requests regarding advertising, including emails and phone calls
- inform the company in writing that the advertisement they are charging you for was not authorised and will not be paid for
- seek legal advice if threatened with legal action.

### Fax back scams

1. You receive a fax describing what sounds like a great deal: fantastic prices, big discounts or entries into competitions. However, the fine print (if there is any) has been blurred by the fax process, disguising excessive hidden costs. Plus, the order needs to be confirmed by faxing back ... and the fax back number is an expensive premium rate 0900 line that will put very high charges on your phone bill.
2. You receive a fax giving an impression that you can receive a free listing in a business directory. In small print you will find there is a cost which is for processing and administering your 12 month listing (eg \$19.95). Sending a fax back to the number indicates acceptance of this charge. If you fax them back asking to be removed from their list they will bill you an amount (eg \$40). Don't respond - throw away the fax or you will incur costs.

## Office supply scams

This is another spin on being charged for items you did not order. People often fall for these because they are being invoiced for items they buy regularly ... which is why it is so important to ensure you only use suppliers you know and trust.

Scammers will even claim to be your regular supplier, offering you a limited-time deal. If you agree to buy any of these supplies, they will turn out to be overpriced and bad quality.

## Protect your small business from scams

- Limit the number of people in your business who have authority to make purchases or write orders.
- Keep written records of all orders and purchases.
- Reconcile all invoices against actual orders. Check that you have received what you paid for.
- If an invoice seems to reference an advertisement or directory entry you genuinely made, make sure you are correct. False billing scammers may use your real advertising as the basis for their fake invoices.
- Ask for a copy of any periodical or directory in which you have paid to advertise.
- Deal only with people and companies you know and trust.
- If you agree to buy from a new supplier, make sure you know exactly what they are offering, at what price, quality, terms and conditions.
- Don't accept business proposals over the phone. Ask to see offers in writing before you accept them.
- Seek advice when making a significant purchase. Don't take the seller's word about competing products or prices.
- Be careful to read the fine print on any offer you receive. If the print is on a fax and is blurry, request a proper copy ... but only use a non-premium telephone or fax number.
- Check any number you call or fax at a seller's request, to make sure it is not a high-charging premium number. If in doubt, call your telephone service provider.
- Don't be intimidated by the scammers' in-your-face tactics such as:
  - bullying
  - threats of legal action
  - confusing references to dealings with other members of your staff
  - negotiations to lower your price
  - blatant charging for unordered goods.

## Help protect others from small business scams

If your business has been targeted like this, please share your story with us. We will treat your report in the strictest confidence and remove your personal details before posting your story on our site.

[Report your scam story to us.](#)