

## Common Small Business Scams

Digital scams are getting more sophisticated these days. Modern scammers often target smaller businesses because they tend to have high trust in their customers, so scammers take advantage of that.

Knowing how to identify small business scams is the first step to keeping your business safe against cybercriminals. Here are some of the common scams targeting small businesses:

### **False Billing**

False billing scams request you or your business to pay fake invoices for directory listings, advertising, domain name renewals or office supplies that you did not order.

### **Overpayment Scam**

Overpayment scams work by getting you to 'refund' a scammer who has sent you too much money for an item you are selling.



### **Whaling or Spear Phishing**

Whaling or spear-phishing scams target businesses or organisations in an attempt to get confidential information for fraudulent purposes.

### **Online Shopping Scam**

Online shopping scams involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on a genuine retailer site.

### **Investment Scam**

Investment scams involve promises of big payouts, quick money or guaranteed returns. Always be suspicious of any investment opportunities that promise a high return with little or no risk – if it seems too good to be true, it probably is – and is highly likely to be a scam.

### **Malware and Ransomware Scam**

Malware tricks you into installing software that allows scammers to access your files and track what you are doing, while ransomware demands payment to 'unlock' your computer or files.

**Source: [scamwatch.gov.au](https://www.scamwatch.gov.au)**