

# Business Security

Small Business Development Corporation

**A well planned security strategy is essential protection for small business. Taking pre-emptive action in potential risk areas will minimise the exposure to fraud and assist with crime prevention.**

## Fraud minimisation

Check that the proper safeguards are in place to minimise the potential for business fraud and take pre-emptive action to minimise fraudulent activities. Your fraud prevention strategy could cover:

### Internet Security

- Make sure you keep your antivirus programs updated & activated daily
- Always type in your bank web address in full, do not use "favourites" or "pop up" web addresses
- Do not gain access to your bank's website via a search engine
- Make sure sites visited are secure i.e. Shows an "s" after the http and a "lock" somewhere on the browser window
- Never use a public computer (internet cafes, libraries) to do internet banking
- Only use secure payment sites i.e. PayPal
- Never share your login & passwords - use strong passwords and change these regularly
- If you have staff using the internet, make sure you have a clear acceptable use policy in place. Staff should have their own login & passwords.
- Beware of phishing emails attempting to steal your personal information
- Appropriately secure client information
- Use software from reputable sources
- Have a back up strategy for your critical data (this includes backing up your website)

Further advice is available at [www.digitalbusiness.gov.au](http://www.digitalbusiness.gov.au) or [www.staysmartonline.gov.au](http://www.staysmartonline.gov.au)

### Cheque misuse

- Only allow authorised persons to sign cheques.
- Cross drawn cheques with 'not negotiable – account payee only'.

- Use cheque writing software applications where possible.
- Eliminate unnecessary spaces on manual cheques to avoid fraudulent changes.
- Keep unused cheques in controlled custody - particularly those with pre-printed signatures.
- Never sign blank cheques.
- Consider a second signature where appropriate.

### Cash and petty cash

- Use an imprest reimbursement system for petty cash.
- Use surprise cash counts by independent staff from time to time.
- Rotate duties where possible.
- Keep cash floats to the minimum practical level.

### Credit card fraud

- Always check the signature of the card holder – staff can overlook this.
- When processing a telephone order, ask for the last three security digits (sometimes four) on the reverse of telephone purchaser's credit cards to confirm they are physically holding the credit card.
- Never disclose your last three security digits (sometimes four) on the reverse of your credit card in response to a telephone call that you did not initiate.
- Be wary when purchasing unsolicited 'bargains' (especially cheap software) over the Internet from people that just want your credit card details.
- Be wary of 'phishing' which means receiving an email that falsely claims to be from a particular enterprise (like your bank) and asking for sensitive financial information including user name and password.

### Crime prevention

Take a look at the business design, layout, cash controls, employee awareness and overall security systems and take action to improve all areas of potential risk. For example your:

### **Design and layout**

- Keep the business visible from the outside and on the inside. Make sure windows are not covered with marketing material, aisles are uncluttered and shelves low enough for you to see what customers are doing.
- Make sure that there are no signs blocking the view of the cash register.
- Mark equipment with identification numbers.
- Install proper lighting both inside and outside.
- Carefully consider the placement of the point of sale material. Keep it away from entrances and exits where possible.

### **Work practices**

- Greet and pay attention to every customer entering the business. Good customer care will put thieves off.
- Avoid staff working alone – have more than one staff member opening and particularly closing the business where possible.
- Move around the store if not making a sale.
- Alert all staff members when groups enter the shop.

### **Cash controls**

- Leave the cash register empty and open after hours.
- Open and close the cash register only when necessary.
- Keep a minimal amount of cash in the register, putting the excess in a secure area or safe.
- Do not leave the cash register unattended for long periods of time.
- Count money out of view of the public.
- Use a bank close to the business and vary the banking times and routes.
- Do not use a bank bag to carry money.

### **Employee awareness**

- Provide training for all employees so that they know the security systems and procedures and what they are expected to do in the event of a crime taking place.
- Instruct employees to immediately report any suspicious activity or person to management and police.

### **Surrounding businesses – know your neighbours**

- Get to know people who operate surrounding businesses. By working together you can help keep each other safe.

### **Overall security**

- Use deadlocks on entry doors and windows that open.
- Use visual deterrents such as security cameras and mirrors. Advertise their existence with signage inside and outside the business.
- Consider the cost of each security measure you take as potential savings against reduced losses.

### **After a crime takes place...**

- Call the police immediately on 131 444.
- Do not touch anything that the robber may have touched. Block off areas where the robber was, if necessary.
- Lock up the store.
- Ask witnesses to stay until the police arrive.
- Obtain names and addresses of anyone who can not wait so that the police can contact them.
- If you have seen the robber, try to recall as much as possible about their appearance, speech and mannerisms. Make notes and get your witnesses to do the same.
- When the police arrive, step outside the store so that they know the robber is gone and you are safe.
- Let the police answer inquiries from news media.
- Do not discuss the amount of money taken with anyone other than police.
- Record all incidents of crime; this may help you spot trends and will help the police if you have to call them.
- Review your security practices and measures.
- Contact your insurance company promptly.

### **Obtain further information and guidance from the Small Business Development Corporation (SBDC)**

- Arrange a free appointment or telephone consultation with an SBDC specialist small business services officer on managing and building your business. Telephone 13 12 49.
- Purchase a small business publication from the SBDC. Telephone 13 12 49 for a publications catalogue or visit the online bookshop at [www.smallbusiness.wa.gov.au](http://www.smallbusiness.wa.gov.au).

#### **Small Business Development Corporation**

Gordon Stephenson House

Level 2, 140 William Street

PERTH WA 6000

Tel: 13 12 49

Fax: (08) 6552 3399

Email: [info@smallbusiness.wa.gov.au](mailto:info@smallbusiness.wa.gov.au)

Website: [www.smallbusiness.wa.gov.au](http://www.smallbusiness.wa.gov.au)

This publication is also available upon request in alternative formats such as large print, electronic format, audio, or braille.

#### **Disclaimer**

This publication has been prepared by the Small Business Development Corporation to provide general guidance and direction on aspects of business security. The information contained herein is provided voluntarily as a service to our clients and is made available in good faith and is derived from sources believed to be reliable and accurate at the time of publishing. However, the information is provided solely on the basis that readers will be responsible for making their own assessment and that they should verify all relevant representations, statements and information. Neither the Corporation nor its officers take any responsibility for statements or representations, nor shall the Corporation or any of its officers be liable in respect of any such statement or representation, whether by reason of negligence, lack of care, or for any other reason whatsoever.