E-Crime

A Crime Prevention Kit for Small Business
A Message from the Minister

Small business is an integral part of Australia’s social and economic fabric. It builds wealth, creates jobs and is an important part of the Australian community.

The internet, and the development of online trading, have led to new and exciting opportunities for small business. Using the internet, small businesses are able to provide cheaper and more efficient services to a broader range of customers and compete more effectively in a global market.

However, there are also risks for small businesses that sell products and services over the internet. One new threat is electronic crime or e-crime. E-crime can incorporate a range of offences including computer hacking, sending viruses, data and identity theft, and online credit card fraud.

Online credit card fraud is especially costly for small business, as losses from fraudulent online purchases are borne primarily by the small business itself, rather than credit card companies or financial institutions. Fraud has been estimated by the Australian Institute of Criminology (AIC) to cost the Australian Community in excess of $5.88 billion each year.

The Australian Government, through its National Community Crime Prevention Programme and the AIC, is committed to helping small business reduce the likelihood of e-crime occurring to them and reduce the impact if it does.

Simple steps you can take to minimise the risk of e-crime to your business include:

- adopting manual or electronic authorisation systems for orders placed over the internet
- being alert to warning signs that may indicate online fraud, for example, a large order from a new customer, incomplete identification details or a request for duplicates of the same item, and
- requesting the credit card security number to ensure the customer has the original credit card (rather than a counterfeit) in their possession at the time the order is placed.

This kit, E-Crime – A Crime Prevention Kit for Small Business, has been prepared to help business owners and managers take practical steps to prevent their business from becoming an e-crime victim.

I would encourage you to use this kit and share it with friends and colleagues to help prevent e-crime.

Senator Chris Ellison
Minister for Justice and Customs
Senator for Western Australia
What the Australian Government is doing about Crime for Small Business

Since 1999, the Australian Government, through its National Crime Prevention programme, has provided almost $1 million to fund research and assistance programmes for small businesses affected by crime.

As part of the ‘Small Business Against Crime’ project, the Australian Institute of Criminology (AIC) completed a survey entitled Online Credit Card Fraud Against Small Business. This survey has contributed to knowledge about online fraud against retailers. It found that small businesses often do not take precautions against online credit card fraud until they have experienced it. The survey has also helped identify gaps in understanding about who bears the costs of such fraud.

The Australian Government has also funded the AIC to undertake specialised crime prevention research, analysis and advisory services for small business. A number of projects around Australia have enhanced understanding of how crime affects small business and how best to help small business prevent crime and respond effectively to it. These projects have looked at:

- crime against small business in Cabramatta and Fairfield, New South Wales (with Fairfield City Council)
- the success of police beat shopfronts in reducing crime and fear of crime for retailers in shopping centres in Queensland
- robbery of post offices and small businesses acting as agents for Australia Post
- theft rates and risk factors at building sites across Australia, and
- the effectiveness of a Business Watch program in the Northern Territory.

In 1999, the Australian Government also funded the AIC and the Council of Small Business Organisations of Australia to survey the impact of crime against small business. This survey resulted in the following publications:

- Crimes Against Small Business in Australia: A Preliminary Analysis
- Patterns of Victimisation Among Small Retail Businesses
- Robbery against Service Stations and Pharmacies: Recent Trends
- Financial and Psychological Costs of Crime for Small Retail Businesses
- Reporting of Crime Against Small Retail Businesses, and
- two reports on violence in the workplace.

These publications can be found on the Institute’s website at www.aic.gov.au.

Further information about what the Australian Government is doing to help small business prevent crime can be found at the following National Community Crime Prevention Programme website www.crimeprevention.gov.au.
DISCLAIMER

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
Survey of Online Credit Card Fraud Against Small Business

As part of the Australian Government funded ‘Small Business Against Crime’ project, the Australian Institute of Criminology undertook a survey titled *Online Credit Card Fraud Against Small Business*. The aim of this survey was to contribute to the knowledge base on online fraud against small business and to help identify gaps in understanding about liability for online fraud.

Previously it was unknown what proportion of small business trading online experienced fraud, the costs of online fraud, the level of knowledge of liability for online fraud losses, and what measures small business might take to protect themselves from online fraudsters.

The AIC *Online Credit Card Fraud Against Small Business* survey investigated:

- the nature and extent of online fraud against five types of small retail businesses
- the percentage of retailers who currently trade online (accept credit card payments for goods over the internet) and their online trading practices, and
- retailers’ perceptions of online trading, fraud and financial institutions.

Telephone interviews were conducted with 1078 businesses across Australia, randomly selected from the following five business types:

- florists
- booksellers
- recorded music retailers
- toy and game retailers, and
- computer hardware retailers.

Overall, 32 per cent of online retailers experienced at least one incident of online credit card fraud. Although the survey showed that the total number of incidents in 2001 and 2002 was not excessive, many victims experience more than one incident. The potential growth in internet trading also increases the potential growth of online credit card fraud.

The average loss for each victim of online credit card fraud varied according to the type of business. In 2002, the average loss per victim was:

- recorded music retailers—$100
- florists—$500
- computer and hardware retailers—$1450
- toy and game retailers—$2900
- booksellers—$3500

25 per cent of online retailers use automatic electronic authorisation, 67 per cent use manual electronic authorisation and 8 per cent rarely or never authorise electronically.
The survey found that there are considerable gaps in knowledge about who bears the costs of online credit card fraud and that knowledge of business liability increases with experience of victimisation.

The delay between an incident occurring and the business being advised of the fraud can be lengthy. This means that several fraudulent purchases may be processed on the same credit card, which can result in multiple losses for a number of victims.

Crime prevention strategies tend to be implemented only after fraud has occurred. For these measures to be effective, they need to be in place before fraud occurs, since one incident of fraud predisposes a business to another. Businesses should have general e-crime prevention measures in place as soon as they start trading online.

When an incident of online credit card fraud has occurred, the business needs to be advised as soon as possible by their financial institution or a person who becomes aware that their credit card may have been used fraudulently against that business. Otherwise the business may continue to allow multiple fraudulent purchases on the same credit card.

Overall, satisfaction with retailing online was quite high. Of online retailers, 89 per cent were satisfied with their business accepting payments online. Some 56 per cent stated that the level of online credit card fraud they had experienced was lower than they had expected.

DISCLAIMER

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
Online Trading Practices

When a business trades online, it generally uses a website to accept orders and credit card details from customers over the internet. The order is processed without the need for the customer to enter the store or ring up, and the customer does not need to show or swipe the credit card. Because of this, online trading is often referred to as a “card-not-present” transaction.

Different options for online trading are available to small businesses. For example, you can operate solely on the internet, or you can combine internet activities with an existing store.

SATISFACTION WITH ONLINE TRADING

The majority of traders surveyed indicated that they were satisfied with accepting payments over the internet (89%), with only a small minority (7%) disagreeing. Certain demographic characteristics were also found to influence a business’s decision to trade online or not. This includes:

- business size (those with more employees are more likely to retail online)
- sex (male retailers are more likely to retail online than women)
- business type (book, music, toy/game retailers and florists), and
- remoteness (those retailers in accessible areas are more likely to retail online than those located in remote areas).

THE FUTURE OF ONLINE TRADING

Online trading is one of the fastest growing retail sectors in the world. As part of the AIC research into online credit card fraud, retailers were asked if it was likely that they would start trading online within the next two years. Overall, 39 per cent of retailers said it was very likely that they would begin online trading in the next two years, with a further 38 per cent saying it was somewhat likely they would begin online trading. Only 21 per cent indicated that it was somewhat or very unlikely that they would begin online trading within the next two years.

This shows that online trading in Australia is here to stay and is growing at an incredible rate. However with the increased benefits of online trading also comes the risk of e-crime, and as the number of online retailers grow, so does the number of potential victims.

DISCLAIMER

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
E-Crime and Small Business

Electronic Crime or e-crime encompasses a number of offences including computer hacking, sending viruses and nuisance e-mails, data and information theft, identity theft and others. Of particular importance to small business is the use of the internet by individuals or groups to conduct fraud.

*Fraud*, broadly defined, is dishonestly obtaining a benefit by deception or other means. This benefit is usually, but not always, financial in nature.

Online credit card fraud occurs when a customer fraudulently submits credit card details over the internet as payment for goods ordered. The action is fraudulent because they are either:

- using a card of which they are not the authorised operator
- they obtained the credit card fraudulently, or
- they are the cardholder, but claim that they did not make the purchase.

Online fraudsters can obtain goods or services illegally in a number of ways including:

- using a fake identity to apply for a credit card and make purchases
- using a stolen identity to apply for a credit card and make purchases
- using a counterfeit or stolen credit card to purchase goods
- ordering goods using a credit card and then falsely claiming they never received the goods in order to claim a refund or replacement goods, or
- claiming that they did not place the order.

The Australian Institute of Criminology survey, *Online Credit Card Fraud Against Small Business*, found that the rate of online fraud varied depending on the type of business targeted. Across all five types of retailers surveyed, about one third (32 per cent) have been victims of online fraud since they started trading online.

**Percentage of online retailers who have experienced credit card fraud:**

![Graph showing the percentage of online retailers who have experienced credit card fraud across different business types.]

Source: Australian Institute of Criminology survey, *Online Credit Card Fraud Against Small Business*, 2004
Online transactions are particularly susceptible to online fraud, as you never actually see the customer or the credit card. You are therefore at a disadvantage when it comes to identifying whether the card is legitimate, stolen or fake, or whether the customer may be using a stolen identity. Information transmitted over the internet can be intercepted at any point.

Small businesses may be affected by e-crime and related fraudulent activity in a number of ways:

- you may receive a fraudulent order over the internet
- your business computer may be accessed and identifying information of customers stolen, or
- an employee could steal business information, such as customer details, and either sell it or use it fraudulently themselves.

E-security technology reduces the risk that personal information will be taken. A secure online environment benefits small business as funds and customer information, including credit card details, can be exchanged over the internet with confidence.

PREVENTION STRATEGIES

You can take practical steps to prevent e-crime occurring by:

- **securing your business computer or network.** Install:
  - password authentication software to protect sensitive business information. Update your password regularly. Don’t use common passwords such as your telephone number, birth date or mother’s maiden name. The best password is a combination of letters, numbers and symbols
  - anti-virus software, regularly updated—viruses can allow an online fraudster to gain access to information files or can send sensitive information to other email addresses
  - encryption software that converts transaction information into unreadable code, and
  - a firewall (software that keeps unwanted visitors out). This is especially important if you have a high speed internet connection that is connected to the internet 24 hours a day.

- **preventing business information from being stolen.** Be vigilant about how, where and to whom business and customer information is passed and how documents containing business information are disposed of.

- **setting minimum identification requirements for credit card orders received over the internet.** Some details you may wish to ask for are the customer’s name, credit card number and expiry date, credit card security number, street address, phone number, fax number and email address. If you are in doubt about an order, ask for further identification details from the customer or reject the order.

- **screening orders coming in over the internet to ensure that they are legitimate.** For example, phone or email the customer to confirm the order. This increases the likelihood of determining that the person whose credit card number was used is actually the person who placed the order. It also confirms the contact details in case that credit card number is used fraudulently in the future.

- **ensuring that you authorise transactions with your financial institution.** This is commonly done either over the phone or online.
• **maintaining a list or database of lost or stolen credit cards and fraudulent orders.** This should include the customer’s credit card number, address, email address and other contact details.

• **allowing only trusted staff members to have access to computer files containing customer information**, such as credit card details and contact details. These staff members should be trained in the methods of preventing e-crime. When staff members leave your business, make sure that you change the passwords protecting customer information.

• **be wary of unsolicited emails.** Delete them without opening any attached files or clicking on any links. They may contain viruses or other software that could interfere with your computer’s operations or data.

• **wipe the hard drive before you dispose of your computer.** Use specially designed software to ensure that no files containing business information can be retrieved.

Using another individual’s personal information without their consent is called **identity theft**. Using such information to obtain a benefit is referred to as identity fraud. More information on how to prevent identity theft is available at [www.crimeprevention.gov.au](http://www.crimeprevention.gov.au).

**DISCLAIMER**

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
A Guide to Manual Screening

Manual screening measures are the actions that you and your staff take to confirm that orders submitted over the internet are legitimate.

The screening may confirm that the customer is indeed the cardholder (by checking identification details such as addresses) or ensure that particular card numbers which are considered fraudulent are not used repeatedly against your business (by keeping records and rejecting suspicious orders).

**COMMON MANUAL SCREENING PRACTICES**

- **Phone or email the customer to confirm the order.** This increases the likelihood of determining that the person whose credit card number was used is actually the person who placed the order. It also confirms the contact details in case that credit card number is used fraudulently in the future.

- **Ask for the credit card security number.** This is a three or four-digit number printed above the card number or next to the signature strip on the credit card. This ensures that the customer holds the card when the order is made.

- **Check the address provided against the name of the cardholder.** You can do this by checking in the local phone directory or on the White Pages website. This is only possible for orders to be delivered in Australia.

- **Maintain a database of good customers who have previously ordered from you with no trouble.** The database should include the customer’s credit card number, address, email address and other contact details. This assists speedy approval of orders.

- **Maintain a database of bad customers who have defrauded you in the past.** The database with their card and contact details will help you to quickly identify potentially fraudulent orders.

- **Ask for more identification details if you suspect that the order may be fraudulent.** This may include checking that the billing address provided to you by the customer is the same address that is listed with the bank for that credit card.

- **You can always reject an order if it has one or more factors that lead you to suspect that it is fraudulent.** Your decision to accept or reject an order will differ in each case and will depend on the level of risk you are willing to expose your business to. For example, if you suspect an order is fraudulent, you may still be willing to risk accepting it where the goods are worth $20, however in the same circumstances you may choose to reject an order where the goods are worth $2000.
A Guide to Electronic Authorisation

Electronic authorisation allows you to check that the credit card being used by the customer has not expired or been cancelled, and has sufficient funds to allow for the purchase to proceed.

Electronic authorisation does not, however, verify that the customer making the purchase is the actual owner of the card. Also, authorisation does not confirm other information like the customer's name or delivery address. By itself, authorisation does not protect you from electronic fraud or a future chargeback (where the bank takes back the payment for the purchase) because you did not swipe the card yourself or obtain a signature from the customer.

Automatic electronic authorisation involves your business paying to use your bank's internet-based payment system. Some banks may not offer this service. When a customer places an order on your website, their order is transferred to the bank's computer system which automatically undertakes the electronic authorisation and then provides notice of approval both to the customer and to your business.

Manual electronic authorisation requires you or a staff member to process an electronic authorisation manually. This can be done by either entering the credit card details into your EFTPOS terminal or by phoning the relevant authorisation hotline.

WHICH METHOD TO CHOOSE?

The best option for your business will depend on the volume of internet transactions, your staffing and the amount of money you have to spend on online retailing. The use of electronic authorisation by online retailers is shown in the chart below.

If your business processes a large number of internet orders, then an automatic system may be best. If you choose this option, you should be prepared for the added costs. However, these may be less burdensome than having staff spending time manually authorising transactions.

Manual electronic authorisation may be a better option for small businesses which process a small number of internet orders and which already have merchant facilities which they could use for authorising online purchases. The diagram below indicates the type of electronic authorisation used by online retailers.

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>8%</td>
</tr>
<tr>
<td>Automatic</td>
<td>25%</td>
</tr>
<tr>
<td>Manual</td>
<td>67%</td>
</tr>
</tbody>
</table>

Source: Australian Institute of Criminology survey, Online Credit Card Fraud Against Small Business, 2004

DISCLAIMER

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
WHO PAYS FOR ONLINE FRAUD?

When an individual’s credit card is used without their knowledge or consent, financial institutions generally do not hold the cardholder liable for any losses. However, when a retailer does not see the customer’s credit card or signature and does not swipe the card through an EFTPOS terminal, as in internet trading, financial institutions are unwilling to accept the heightened risks associated with online trading. This means that you, the retailer will usually bear the costs of online credit card fraud. This can include:

- the chargeback (the amount your financial institution takes back to cover the cost of the fraudulent purchase)
- the chargeback fee (a fee to cover the costs of reversing the amount charged), and
- any shipping or delivery costs.

The Australian Institute of Criminology (AIC) survey, *Online Credit Card Fraud Against Small Business*, found that many retailers did not know that they were likely to be held liable for the costs of online fraud. The chart below shows that awareness of liability is lower among those who don’t currently trade online or who haven’t experienced fraud.

**Perceptions of liability for e-crime**

![Perceptions of liability for e-crime graph](chart.png)

Source: Australian Institute of Criminology survey, *Online credit card fraud against small business*, 2004
LOSSES

In the AIC survey, businesses were asked about the online fraud losses they had suffered in 2001 and 2002. Losses are defined as costs which could not be recovered through any other means, for example, by resolving the matter with the customer.

For victims who experience online fraud, losses can be considerable (see chart below). This was particularly so for booksellers, toy and game retailers and computer hardware retailers. Since the majority of online traders in this survey had an annual turnover of less than $500,000, it is likely that these losses impacted considerably on those businesses affected.

Average loss for each victim of online fraud who experienced a loss, by business type

![Bar chart showing average loss for each victim of online fraud by business type.]

Source: Australian Institute of Criminology survey, Online Credit Card Fraud Against Small Business, 2004

DISCLAIMER

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
Many small businesses rely heavily on computers to conduct transactions, record information and communicate with customers, staff and suppliers. This reliance on computers brings potential risks in terms of maintaining proper records in the event of legal action.

Should you ever be a victim of e-crime, your computer records will need to be in the correct format to be used as evidence. Computer systems need to be programmed to store records properly and should have the capacity to produce the records when required.

*Information technology evidence* (IT evidence) is the broad term used to describe any records, generated by or stored on a computer system, which may be used as evidence in court.

If you are initiating or defending legal action, or assisting the police in the prosecution of an online fraudster, it is important that the relevant computer records can be identified, extracted from your computer system and, if necessary, translated into a form that people can read. This helps the material to be accepted as evidence.

Practical steps that you can take include:

- ensuring that your procedures and your business computer system can establish the time and author of a record and provide details of any alterations made to the record
- establishing procedures for retaining records (such as daily back-up disks) in safe custody
- ensuring that employees who design, produce, collect, analyse and present IT evidence have the appropriate training, experience and qualifications, and

You will probably need to seek specialist legal and computing advice and help. Try the contacts list at the end of this kit as a starting point.

*If you are a victim of e-crime* – always check with the police before further handling any potential evidence, including on either your personal computer or business IT system. The police may wish to use their own electronic investigations team in order to preserve the integrity of the evidence.

**DISCLAIMER**

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
Useful Contact Numbers

ORGANISATIONS

Your bank or credit card agency

These bodies can advise you on costs, software, your trading website, managing customer information and security procedures. You should discuss your responsibilities and risks in internet trading before you sign a service contract with your bank.

Australian High Tech Crime Centre

The role of the Australian High Tech Crime Centre is to provide a national coordinated approach to combating serious, complex and cross-border high tech crimes. If you believe that you have been the victim of a complex scam on the internet (such as a false banking) or have had your business website mirrored (false e-commerce website – this may not impact on your business in monetary terms – being directed at customers – but may harm your business reputation) or received malicious software (such as a virus), please contact the centre.

Telephone: (02) 6246 2101
Website: www.ahtcc.gov.au

Crime Stoppers

Crime Stoppers allows the community to help police in the fight against crime. By calling Crime Stoppers you can anonymously report e-crime or other crime.

Telephone: mainland Australia 1800 333 000, or Tasmania 1800 005 555
Website: www.crimestoppers.com.au

Australian Communications Authority

The Australian Communications Authority (ACA) is responsible for regulating telecommunications and radiocommunications, including promoting industry self-regulation and managing the radiofrequency spectrum. The ACA also has significant consumer protection responsibilities.

The Federal Parliament has enacted legislation to regulate unsolicited commercial electronic messages, also known as ‘spam’. Under the spam legislation, the ACA is concerned with unsolicited commercial email (and other electronic messages) whether or not the content is itself legal or illegal. However, much email also carries content which is itself illegal under other laws—for example, it is fraudulent, offensive or carries a computer virus.

To report spam that you have received, make a complaint about someone who is not complying with the spam legislation or a general question, go to the ACA website and link to the ‘SPAM’ section.

Website: www.aca.gov.au

For questions regarding the legislation:

Telephone: 1300 855 180
Standards Australia

Standards Australia is an independent company that develops technical and business standards, distributes specialist publications and certifies the standards of products and business systems. Its publication, Guidelines for the Management of IT Evidence, gives information on evidence obtained from computers.

Telephone: 1300 654 646
Website: www.standards.com.au

Office of Small Business

The Office of Small Business manages the Small Business Assistance Program which funds skill development projects and referral and advisory services for small businesses.

Telephone: 1800 024 095
Website: www.industry.gov.au

Australian Competition and Consumer Commission

The Australian Competition and Consumer Commission administers the Trade Practices Act. The Act’s consumer protection provisions which outlaw misleading and deceptive conduct also offer protection to small business. The Act also restricts anti-competitive market practices, regulates mergers and acquisitions of companies and oversees product safety and liability.

Telephone: 1300 302 502
Website: www.accc.gov.au

DISCLAIMER

This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.
FOR FURTHER INFORMATION
TRY THE FOLLOWING

**Australian Government agencies**

- **Australian Federal Police**
  - Telephone: (02) 6256 7777

- **Australian Institute of Criminology**
  - Telephone: (02) 6260 9200

- **Australian Crime Commission**
  - [www.crimecommission.gov.au](http://www.crimecommission.gov.au)
  - Telephone: (02) 6243 6666

- **Consumers Online**
  - [www.consumeronline.gov.au](http://www.consumeronline.gov.au)

- **Consumer Affairs Division**
  - Department of the Treasury
  - [www.ecommerce.treasury.gov.au](http://www.ecommerce.treasury.gov.au)
  - Telephone: (02) 6263 2111

- **National Crime Prevention**
  - Telephone: (02) 6250 6711

- **Ministerial Council on Consumer Affairs**

- **Business Entry Point**
  - Telephone: 13 28 46

- **Australasian Centre for Policing Research**
  - Telephone: (08) 8363 3033

- **Australian Securities and Investments Commission**
  - [www.asic.gov.au](http://www.asic.gov.au)
  - Telephone: 1300 300 630

**State and Territory police and crime prevention agencies**

- **South Australia Police**
  - Telephone: 131 444

- **New South Wales Police**
  - Telephone: 1800 622 571

- **Victoria Police**
  - Telephone: (03) 9247 6666

- **Queensland Police**
  - Telephone: (07) 3364 6464

- **Tasmania Police**
  - Telephone: (03) 6230 2111

- **Northern Territory Police**
  - Telephone: (08) 8922 3344

- **ACT Policing**
  - Telephone: (02) 6256 7777

- **Western Australia Police**
  - Telephone: 131 444

- **Crime Prevention Victoria**
  - Telephone: (03) 9651 6933

- **New South Wales Crime Prevention Division**
  - Telephone: (02) 9228 8307
South Australia Crime Prevention Unit
www.cpu.sa.gov.au
Telephone: (08) 8207 1659

Crime Prevention Queensland
www.premiers.qld.gov.au/securitycrime
Telephone: (07) 3224 2843

Northern Territory Office of Crime Prevention
www.crimeprevention.nt.gov.au
Telephone: (08) 8999 6274

Western Australia Office of Crime Prevention
www.crimeprevention.wa.gov.au
Telephone: (08) 9222 9733

State and Territory small business websites

New South Wales Office of Fair Trading
www.fairtrading.nsw.gov.au
Telephone: (02) 9388 4943

New South Wales Small Business
www.smallbiz.nsw.gov.au
Telephone: (02) 9228 3111

Victoria Consumer and Business Affairs
www.consumer.vic.gov.au
Telephone: 1300 558 181

Victoria Business Access
www.businessaccess.vic.gov.au
Telephone: 13 22 15

Queensland Office of Fair Trading
www.consumer.qld.gov.au
Telephone: 1300 658 030

Queensland Smart Small Business
www.smartsmallbusiness.qld.gov.au
Telephone: 13 26 50 (QLD Callers Only)
Alt Ph: (07) 3225 1915

Western Australia Electronic Commerce Centre—Fair Trading
Telephone: (08) 9327 5555

Western Australia Small Business Development Corporation
www.sbdc.com.au
Telephone: 1800 199 125

South Australia Office of Consumer and Business Affairs
www.ocba.sa.gov.au
Telephone: (08) 8204 9777

Tasmanian Office of Consumer Affairs and Fair Trading
www.justice.tas.gov.au/ca
Telephone: 1300 654 499

Australian Capital Territory Business Gateway
www.business.act.gov.au
Telephone: 1800 244 650

Private bodies

Council of Small Business Organisations of Australia Ltd
www.cosboa.org
Telephone: (03) 6224 0214

Australian consumers Association
www.aca.com.au
Telephone: (02) 9577 3399

Internet Industry Association
www.iia.net.au
Telephone: (02) 6232 6900
**Quick Reference Guide**

More detailed information on any of the topics covered in this quick reference guide is contained in the fact sheets included in this kit.

### HOW DO YOU PREVENT E-CRIME?

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you know what e-crime is and how it may be carried out?</td>
<td></td>
</tr>
<tr>
<td>When you dispose of a business computer, do you ensure that all customer or business information is wiped from its hard drive so that the information cannot be recovered and used fraudulently?</td>
<td></td>
</tr>
<tr>
<td>Do you request complete details from customers placing orders over the internet, including name, credit card number and expiry date, street address, phone number, fax number and email address?</td>
<td></td>
</tr>
<tr>
<td>Have you implemented policies amongst staff to ensure that all orders received over the internet are screened by:</td>
<td></td>
</tr>
<tr>
<td>- phoning or emailing customers to confirm the order?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>- using manual or electronic authorisation methods?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>- checking the address provided against the name of the cardholder in the local phone directory or on the White Pages website?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>- asking for the credit card security number, three or a four digit number printed above the card number or the signature?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>- being aware of the warning signs that may indicate an order is fraudulent?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>- maintaining a database of good customers, to speed approval of their orders? and</td>
<td>Yes/No</td>
</tr>
<tr>
<td>- maintaining a database of bad customers, to identify potentially fraudulent orders?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Do you reject orders which you suspect to be fraudulent?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Do you make sure that only trusted staff can access customer information?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Have you minimised the risk of information being intercepted online and used fraudulently by setting up a secure, encrypted website where customers can place orders?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Have you considered upgrading the security of your computer network by installing a firewall?</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Do you use passwords to control access to files and folders stored on your business computer?</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>
Have you installed and do you regularly update anti-virus software? Yes/No
Before commencing internet trading, did you discuss your responsibilities with your financial institution? Yes/No
Do you ensure that your computer maintains proper records, which can be identified and extracted if you ever need to introduce them into evidence in criminal or civil proceedings? Yes/No

If you have answered ‘No’ to any of the above your business may have a heightened risk of becoming an e-crime victim.

IF YOU ARE A VICTIM OF E-CRIME
Report the occurrence to the police.
Collect all relevant paper documentation and give it to the police.
Check with the police first as to how any electronic evidence should be dealt with. They may wish to use their own electronic investigations team in order to preserve the integrity of the evidence.
Advise your financial institution or the credit card agency.
Check customer records for other orders from the same person, the same credit card or the same address and hold or stop any outstanding orders.
Close any of your accounts that you know have been tampered with.
Review procedures to prevent similar e-crime occurring in the future.

DISCLAIMER
This brochure contains general guidelines for increasing security for small business. The Australian Government, in providing this information, makes no representation nor gives any warranty or guarantee concerning the safety of persons or property, nor does the Australian Government accept any responsibility for any damage or loss, however caused, suffered by any individual or corporation arising from the use or application of these guidelines. Users of these guidelines must satisfy themselves as to the adequacy of the guidelines for the purposes of their own safety and security.