

Small Business - Protecting Your Business Information Online



Small businesses are increasingly opting to do business via the Internet and are opening their business and telephone lines to customers and suppliers through electronic trading. They are opting to do business online because it is convenient, opens the business 24-hours a day, can lead to lower overheads and access to a wider potential market.

However, this new way of doing business can expose the business to risks through the very medium that is providing tremendous advantage and access to customers and suppliers not previously imagined. This fact sheet prepared by the Australian Bankers' Association and the Australian High Tech Crime Centre provides useful information for any business seeking to use the Internet and in particular, to protect access to your systems and business records from the outside, when Internet trading, either in or out, is conducted by your business.

HOW CAN I PROTECT MY BUSINESS

It's important to put in place some measures to reduce risk and protect your business information.

Security tips:

1. Install reputable anti-virus software and keep it up-to-date.
2. Install reputable firewall software & keep it up-to-date.
3. Keep software patches up-to-date.
4. Keep your password secret, make it complex, and change it regularly.
5. Delete without opening any suspicious e-mails - curiosity is a tool used often by hackers.
6. Download software only from reputable sources.
7. Have a backup of your critical data that is separate from your Internet connected computers and burn the data to CD or some backup device.
8. Test that you can recover with that backup data.

Important Note: This fact sheet gives information of a general nature and is not intended to be relied on by readers as advice in any particular matter. Readers should consult their own advisers on how this information may apply to their own circumstances.

BUSINESS RISKS ONLINE

As small businesses' sales and revenue collection processes, financial records and cash management systems are crucial to their success and security, the ability to protect them from hackers, virus and other threats is vital for long-term viability of the business. It is better to be prepared than ignore these risks.

An unprotected small business can be an easy target for a hacker – a criminal which penetrates an organisation's security systems, proving they can get in and do harm or mischief to the system. Hackers may target small businesses as a means of achieving competitive advantage for a less scrupulous competitor or for the thrill of bringing down your system.

SMALL BUSINESS – YOUR OBLIGATIONS TO PROTECT INFORMATION ONLINE

The small business operator has very strict and onerous requirements to guard the information at its disposal and a careless attitude to hacker access may create very serious liabilities on the small business owner.

The small business operators' obligations to protect information in its possession against potential use or abuse include:

The Privacy Act: Your business may be required to protect the personal information it holds from misuse and loss, unauthorised access, modification or disclosure. Serious fines apply for non-compliance or a careless attitude.

Corporations Act 2001: Under the Corporations Act, you must have 'adequate protection' over information at your disposal. Also, the Corporations Act imposes obligations to keep copies of business records for a number of years.

Trade Practices Act: The business operator may be sued by another party if they incur loss or damage through a security breach at your business.

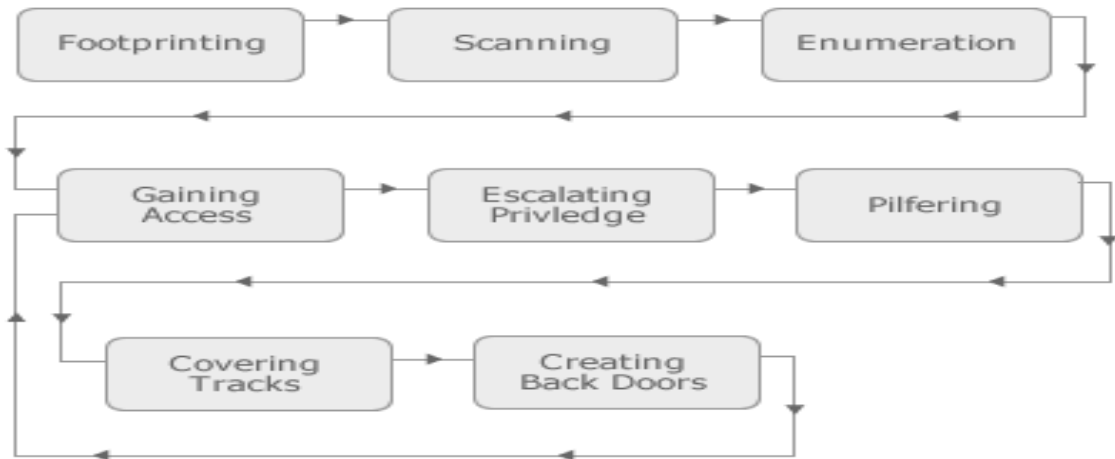
Directors' Liability: A director is obliged to protect the corporate assets at their disposal, otherwise civil, Australian Securities and Investments Commission (ASIC) and criminal proceedings may result. As most small businesses now have some form of corporate entity structure or protection, this is now more relevant.

Criminal Liability: If delegated employees act in a criminal manner, the business operator may be held responsible for their activities.

So you can see that your small business has very significant obligations to protect the personal and business information and records at its disposal as a result of dealing with various parties. It is not an acceptable excuse to claim that these records only came into risk through the actions of a hacker. The risk is now well accepted and it must be managed by your small business.

HOW DOES A HACKER GAIN ACCESS?

The following diagram describes the various methods by which a hacker gains access to a business.



1. Footprinting is information gathering in order for the hacker to obtain sensitive details about the business.
2. Scanning is the search by the hacker for a crack in the business defences, looking for the most promising avenue of entry.
3. Enumeration is the use of the business information, now acquired by the hacker to attempt to gain access to the business system, by, for example, testing passwords.
4. Gaining Access is the act of the hacker breaking into your system.
5. Escalating Privilege is the hacker's attempt to higher levels of access to collect more important information, once the system is penetrated.
6. Pilfering is the ability of the hacker to see which businesses that you use and use that information to attack them as well.
7. Covering Tracks is the hacker's ability to hide themselves in your system, so that they can come back later and obtain more information.
8. Create Back Doors is the hacker creating many ways to come back later and attack the business without your knowledge.

HOW DOES A BUSINESS KNOW IF IT HAS BEEN HACKED?

The following is a useful list of potential indicators that your small business has been hacked and can be used to monitor your exposure:

- Your website has been changed to whatever the hacker wants.

FACT SHEET

- You may notice that your computer system performance is exceptionally slow.
- Some secrets of your business have been exposed to the general public or to competitors.
- Transactions have been changed, for example, an account had a balance of \$1000, now it's \$950 without your authorisation.
- There is odd activity in a log and the more it's investigated the more the business becomes convinced that something is wrong. The business processes are not being followed and it may be that someone is operating outside of your control and is using your business.
- You are no longer receiving e-mails and no-one receives e-mails you have sent.
- The entire system shuts down.
- There is a new program on your computer you didn't install.

To enable a business to assess its risk to hacking, you may want to engage the services of an external independent Internet security organisation, specialising in 'ethical hacking'. These organisations can help assess and mitigate the risks for Internet security, independent of any vendor or supplier. By doing this you take a positive step to understand your risks and install programs to test for their effectiveness.

HOW DO BANKS HELP PROTECT YOUR BUSINESS INFORMATION?

Banks use a combination of safeguards to protect your information such as employee training, strict privacy policies, rigorous security and encryption systems. Banks have systems in place to constantly monitor online transactions. If banks come across a suspicious transaction, they will investigate it to ensure there is no breach of security. Occasionally, this may involve a bank staff member contacting you to verify a transaction. Banks will communicate with their customers regarding Internet security issues, often by publishing important information on their websites.

Some banks are working on the next step in security - two factor authentication systems. That means customers will identify themselves twice: first with something they know and then with something that they have. For example, using a password to logon to Internet banking and the bank might send an SMS message with a unique number to enter and authenticate the transaction. This unique number could also be generated by a device known as a security token.

The Australian Bankers' Association (ABA), its member banks, State and Federal police are working closely to tackle the problem of cybercrime. Bank staff have been seconded to the Australian High Tech Crime Centre (AHTCC) as part of a new team to continue the fight against fraud that occurs online. They are providing analytical assistance to police who will use this information to identify and prosecute criminals.

Banks work closely with State, Territory and Federal police to prosecute criminals who misuse customers' personal information or commit cybercrime. Each State and Territory jurisdiction has a range of offences which cover identity crime, including the unlawful possession of

Important Note: This fact sheet gives information of a general nature and is not intended to be relied on by readers as advice in any particular matter. Readers should consult their own advisers on how this information may apply to their own circumstances.



documents, operating accounts in false names and obtaining monies by deception. The penalties vary across each State and Territory but include large fines and incarceration, in some circumstances for up to ten years. Banks also work closely with other organisations such as the Australian Crime Commission and the anti-money laundering regulator, AUSTRAC.

WOULD YOU LIKE TO READ MORE?

Most banks have detailed information on their websites on how bank customers can protect themselves from Internet fraud attempts perpetrated by criminals. Take a look at your bank's website or give them a call for more information.

For further information:

Organisation	Website Address
The Australian High Tech Crime Centre investigates crimes, which involve a computer or other piece of technology. It plays a significant role in reducing crimes such as hacking, denial of service (viruses, worms, Trojans), terrorism and money laundering.	www.ahtcc.gov.au
The Australian Securities and Investments Commission's consumer website FIDO has information on scams and swindles.	http://www.fido.asic.gov.au/fido/fido.nsf
The Australian Competition and Consumer Commission has a consumer protection role and their website publishes information about consumer rights. State and Territory Consumer Affairs and Fair Trading - the role of these offices is to safeguard consumer rights and to advise businesses and traders on fair ethical practice.	www.accc.gov.au
Australian Capital Territory	www.fairtrading.act.gov.au
New South Wales	www.fairtrading.nsw.gov.au
Northern Territory	www.nt.gov.au/caft/
Queensland	www.fairtrading.qld.gov.au
South Australia	www.ocba.sa.gov.au
Tasmania	www.tas.gov.au
Victoria	www.consumer.vic.gov.au
Western Australia	www.docep.wa.gov.au

Important Note: This fact sheet gives information of a general nature and is not intended to be relied on by readers as advice in any particular matter. Readers should consult their own advisers on how this information may apply to their own circumstances.



FACT SHEET

Commonwealth Attorney-General's
Department Identity Fraud
Prevention Kit

http://www.crimeprevention.gov.au/agd/WWW/ncpHome.nsf/Page/Publications_All_Publications_Public_Safety_ID_Theft_-_A_kit_to_prevent_and_respond_to_identity_theft

Created: February 2005

Australian Bankers' Association: Free-call 1800 009 180 www.bankers.asn.au
Australian High Tech Crime Centre: Telephone 02 6246 2101 www.ahtcc.gov.au

