

Things you
need to
know and do
to operate
safely online

INTERNET SECURITY ESSENTIALS FOR SMALL BUSINESS



Australian Government

Department of Communications,
Information Technology and the Arts

Contents

Introduction	02
Internet security tips	03
Summary of our top 10 Internet security tips	04
1. Develop a ‘culture of security’	07
2. Install anti-virus software and keep it updated	10
3. Install a firewall to block unauthorised access to your computer	12
4. Protect yourself from harmful emails	14
5. Minimise spam	16
6. Back up your data	18
7. Develop your system with secure passwords	20
8. Keep your software up-to-date	22
9. Make sure your online banking is secure	24
10. Develop and maintain a security policy	26
Resources	27
Internet security essentials checklist	28

Introduction

The Internet is proving to be a valuable tool for doing business. If your business is operating online, you need to make sure you and your staff are using the Internet in a safe and secure way.

Information, tools and resources, many of which are outlined in this booklet, are available that will help you identify, develop and maintain good Internet security practices for your business.

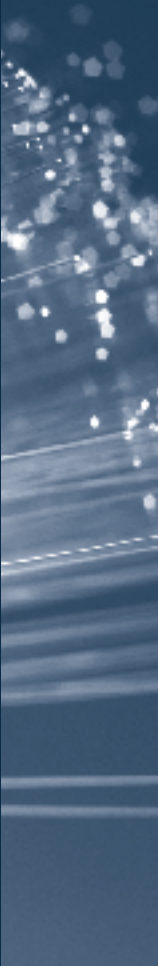
What are the Internet security threats to my business?

If your business is connected to the Internet it is important to secure your business data and information against unwanted intruders who might:

- introduce viruses that can destroy your records or slow down your computer
- intercept financial transactions, steal credit card details and access customer information
- mimic your online identity and pretend to be you (identity theft)
- insert malicious spyware that can sit on your computer without your authorisation or knowledge
- take over your website and modify it
- piggy-back on your Internet connection and make use of it at your expense.

While there are dangers out there—Internet security professionals can provide many examples of websites and computer systems that have been breached—they can often be prevented if your business adopts some simple Internet security measures.

Internet security tips



Summary of our top 10 Internet security tips

Consider the following tips. They will help you secure your computer and make sure your business is using the Internet safely.

1. Develop a 'culture of security'

Businesses need to have Internet security measures in place and make sure staff are aware of and follow Internet security practices.

2. Install anti-virus software and keep it updated

Anti-virus software scans and removes known viruses your computer may have contracted. It will help protect your computer against viruses, worms and trojans.

3. Install a firewall to stop unauthorised access to your computer

Firewalls work like a security guard to protect your computer from intruders.

4. Protect yourself from harmful emails

Be cautious about opening emails from unknown or questionable sources.

5. Minimise spam

While it is not possible to completely stop spam from entering your email box, it is possible to take steps to prevent a large amount of spam.

6. Back up your data

Creating a copy or back-up of data is a sensible way to ensure that you can recover all of your business information from your computer or website quickly and easily.

7. Develop a system for secure passwords

Creating effective passwords can provide additional means of protecting the information on your computer.

8. Keep your software up-to-date

If your software is out of date, you are more vulnerable.

9. Make sure your online banking is secure

If you bank online you should follow security advice provided by your financial institution.

10. Develop and maintain a security policy

You need to monitor and test security policies.

e-security and broadband

Given the 'always on' nature of broadband, you are more likely to leave your computer connected to the Internet when you are not using it. A sensible security precaution is to disconnect your computer from the Internet when you don't need to be online.

A glossary of e-business and e-security terms is available at www.e-businesssguide.gov.au

The e-businesssguide website provides a comprehensive resource designed for those with some knowledge and experience of e-business.

1. Develop a 'culture of security'

Many business people simply do not include Internet security as part of their day-to-day business. It is important, though, to develop a 'culture of security'.

Businesses need to not only have e-security measures and programs in place, but also make sure staff are aware of and follow Internet security policy.

No matter how good your business procedures, people will make mistakes. Managers and staff forget to log off, do not change their passwords, or neglect to download and install the latest software patches because they are too busy.

Raising awareness about online security is an important part of protecting your online business. Never assume that staff understand the security risks they might be taking.

What you can do

Many simple and cost-effective security devices are available to ensure your computers and information systems are safe from hackers and viruses. There is a lot of information out there which can help you to develop an appropriate security program.

Create a security culture in your business by:

- having all of your current staff (and, as part of their induction, new staff) read *Internet Security Essentials* and follow up the resources mentioned here
- setting up a security awareness program for all system users that includes things like briefings, training sessions, clauses in employee contracts and security awareness days

- developing security procedures for your business, covering topics such as:
 - what to do if the computer is infected with a virus
 - what to do with unknown email messages or attachments
 - the need for staff to disconnect their computer from the Internet when not in use to reduce exposure to unauthorised access
- making Internet security a permanent item for discussion at regular staff meetings
- using the Safety Net Online tutorial to test your current Internet security safety measures.

Here are some Internet security resources you can find on the web:

Safety Net Online is an interactive online training course. It is available on the Asia Oceania Electronic Marketplace Association website: www.aoema.org.

The Organisation for Economic Co-operation and Development (OECD) has brought out a document titled *Guidelines for the security of information systems and networks*. Australia helped develop these guidelines, which are available on the OECD website: www.oecd.org. Once you are in the website, type the phrase 'guidelines for the security of information systems' into the search box and click on 'exact match' and then 'search'.



Home-based businesses often share their computer resources with family members.

They should make sure that family members as well as employees who are using the business computer follow your security measures.

2. Install anti-virus software and keep it updated

A virus can be transmitted through email attachments, by downloading infected programs from websites, or through an infected floppy disk or CD. Some viruses have been programmed to remain dormant for extended periods. Anti-virus software should be installed on your computer to protect it against known viruses, worms and trojans. Anti-virus software scans and removes threats such as these that your computer may have contracted. The software can also be set to automatically scan disks for malicious code.

What you can do

The best way to prevent viruses, worms and trojans from infecting your computer is to:

- ensure that you install both firewall (see tip 3) and anti-virus software
- ensure that you have up-to-date anti-virus software installed on your computer
- ensure that all security patches for operating systems and application software on your network are up-to-date
- use caution when working with files from unknown or questionable sources
- not open email attachments if you do not recognise the sender
- ensure you scan the attachment with anti-virus software before opening it
- only download files from reputable Internet sites, and be wary when exchanging files with friends
- never click on hyperlinks in emails received from unknown sources

Further information

Detailed information is available on the security website developed by the Internet Industry Association: www.security.iaa.net.au.

The Australian Computer Emergency Response Team (AusCERT) provides free alerts on computer viruses to small businesses. Information about the AusCERT National IT Alert Service can be found at: www.national.uscert.org.au.

What is a virus?

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge or permission. Once loaded, a virus is capable of reproducing itself by travelling from file to file and from computer to computer, often destroying information files in the process.

What is a worm?

A worm is a computer program that replicates itself and spreads from machine to machine across the Internet. Like viruses and Trojans, worms are a form of malicious code which may perform some harmful function in the process on infected machines. Worms often spread by exploiting software vulnerabilities in operating systems and applications software.

What is a trojan horse?

A trojan horse, as the name implies, secretly carries often-damaging software in the guise of an innocuous email attachment. The file attachment name itself is normally misleading to entice you to open it. When the attachment is opened the program can do all sorts of things, from erasing files to changing your desktop, or installing a keystroke logger that can monitor every letter you type.

What is malicious code?

Malicious code is software designed to damage the user's data, steal information or compromise the ability to use the computer. It is often hidden as a trojan.

3. Install a firewall to block unauthorised access to your computer

Firewalls work like a security guard to protect a computer.

A firewall blocks unauthorised access to your computer from the Internet, and the downloading of information from your computer.

Firewall access rules are set by the firewall's user to determine whether to allow or disallow a connection.

A computer without a firewall is like a building without a security guard—nothing controls who and what can enter or leave. For increased security, any computer or computer networks connected to the Internet should have firewall protection.

What you can do

To obtain and use an appropriate firewall effectively:

1. Purchase firewall software

Firewall software often comes with a computer's operating system. It may be downloaded via the Internet from reputable websites or purchased anywhere you buy your computer software. Hardware firewalls can also be purchased from the place where you buy your computer network equipment. Internet service providers are also a good source of firewall hardware and software.

2. Install and activate your firewall

Having an active firewall is very important for security, so install and activate your chosen firewall as soon as possible. Depending on how complex your needs are, you may require help from the vendor or from an Internet security consultant. Internet service providers may be able to help with installation.

3. Maintain your firewall

Firewalls must be updated regularly to protect your computer effectively. Ideally your firewall software will have an automatic update feature. Be sure this option is turned on, and check regularly to make sure you are using the latest version of the firewall.

Further information

You will find detailed information on the security website developed by the Internet Industry Association at: www.security.iaa.net.au.

What is a firewall?

A firewall is a system designed to prevent unauthorised users from accessing your computer or network connected to the Internet.

4. Protect yourself from harmful emails

Email is one of the easiest and fastest means of communicating via the Internet. It can also distribute harmful electronic viruses, worms and trojans through malicious code in attachments and commands embedded in apparently normal messages.

Email borne viruses, worms and Trojans are capable of harming your business computer system and with it your ability to conduct your business.

One of the ways to safeguard your computer systems is to be cautious about opening email attachments or clicking on hyperlinks in emails from unknown or questionable sources.

Installing a firewall is an important and effective first step (see tip 3) to prevent access to your network by unauthorised users. But firewalls do not check the content of email being sent and received by those authorised to use the computer. This means that email viruses, worms and trojans can still pass through this level of security.

Installing anti-virus software protects against most email viruses, worms and trojans. To protect against the latest threats you need to regularly update your anti-virus and firewall software (see tips 2 and 3).

What you can do

To protect against harmful emails:

- always use firewall and anti-virus software
- perform a complete virus scan on your computer at least once a week
- keep all filtering and security software up-to-date

- install security patches for all operating system software and application software and keep them up-to-date
- apply common sense before opening any email, especially if the title of the email attachment appears vague or unfamiliar
- be wary of opening email attachments, especially from anyone you do not know
- be suspicious of email that creates a false sense of urgency, or that makes offers that sound too good to be true
- do not open web links in any email if you suspect that the email is vague or unfamiliar (often such emails trick you to download a virus, worm or trojan)
- use a filter to automatically scan your incoming email for spam (see tip 5)
- do not have an 'email preview' option as a default viewing option in your email inbox.

Further information

You will find useful information on the AusCERT website under 'Protecting your computer from malicious code': www.auscert.org.au/3352

You can find detailed information on the 'security' website developed by the Internet Industry Association: www.security.iaa.net.au

5. Minimise spam

Spam is the Internet equivalent of junk mail in your letter box.

Spam emails are commercial electronic messages that have been sent to you without your consent. Senders often attempt to buy, sell or advertise goods, services, land, investment opportunities and so on through spam. Spam not only clogs up your inbox with annoying, unwanted messages, but also creates a time cost to you in deleting it, and if the problem is particularly bad there are increased download costs. As well, spam can often contain viruses, worms and trojans.

Software is available to help reduce the inflow of spam. It detects unsolicited and unwanted emails and prevents them from reaching your inbox by searching for suspicious word patterns or other clues that may indicate spam. The filtering software then diverts these messages to (in some cases) a special mail box or location so that you can check through them later and delete those that are spam.

What to do

It is not possible to completely stop spam from entering your email box, however, it is possible to take steps to prevent a large amount of spam:

- install spam filters to stop spam emails getting to your inbox
- when you receive spam, add the address to 'junk senders'—most mail programs have the ability to block senders, or add them to a 'junk senders' list
- do not respond to unsolicited mail
- if the source of an email appears dubious, do not use the 'remove' or 'unsubscribe' link. (These links can be used to confirm that an email account is active, and can lead to even more spam being sent)

- do not open attachments in messages if the source of the message is unknown or is suspicious
- report spam to the Australian Communications Authority (ACA) at www.aca.gov.au.

Further information

Spam legislation

The Australian Government is concerned about the growth of spam and has implemented the *Spam Act 2003* as one part of its approach to combating the widespread problem of spam. The Act is available at the Scaleplus website: scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

A guide to the *Spam Act 2003* specifically designed for small business is available at: www.dcita.gov.au/spam.

Consumer and business guides

The Australian Communications Authority (ACA) is the government agency responsible for enforcing Australia's Spam Act. The ACA provides online information and downloadable guides on the many things you can do to reduce the amount of spam you receive, as well as advice on compliance with the Act: www.aca.gov.au.

6. Back up your data

A back-up is a copy of the data and certain programs on your computer. Creating a copy or back-up of data is a sensible and easy way to ensure that, in the event of a fire, computer theft or virus infection you can recover all of your business information from your computer or website quickly and easily.

You may either back up all the data and certain programs on your hard drive each time you back up or you may do incremental back-ups. This means that you back up only the files that have changed since the last time you backed up.

It is good business practice to assess your level of risk by asking yourself the following questions:

What are the consequences of a disaster occurring?

If the worst case scenario were to happen, what would be needed to get the business running again quickly?

Use the answers to formulate your strategy and then ensure that you implement a schedule for rehearsing the recovery strategy.

What you can do

Here are some key points for effective data back-up:

- develop a disaster recovery plan by first assessing your level of risk
- ensure back-up procedures are in place and tested and remember to test the actual data and restoring of data process
- ensure that you keep the back-up copies in a safe, fire-proof location away from your computer systems—usually these conditions can be met simply by storing the back-up in another place away from your business premises
- ensure back-up procedures include systems such as finance and payroll
- all third-party software should be copied prior to its initial use (software licensing allows for the making of copies for legitimate back-up purposes). These master copies should not be used for ordinary business activities but should be reserved for recovery purposes. They should be stored in a secure off-site location.

7. Develop your system with secure passwords

A password is a string of numbers and letters used to verify your identity when you log into a computer system or access websites or other computers on the Internet.

If your business does not use passwords at all, or uses passwords that are easy to guess or easy to crack, then an intruder to your office, or someone who steals a laptop left in your car, will have access to your files, email, personal information and business details. The intruder may modify or destroy your files, send email in your name, or subscribe to unwanted services which you would have to pay for.

You are responsible for securing data in the computer you use. The use of strong passwords acts as a deterrent against password guessing. The security of each individual user is closely related to the security of the whole system. Creating effective passwords can provide additional means of protecting the information on your computer.

What you can do

Develop a password protection system for your business. You and your staff should:

- avoid passwords that would be readily identifiable or easy for anyone to guess (such as family names, birth dates)
- use a mix of upper and lower case alpha, numeric and special characters
- memorise your passwords and make sure that you do not write down your password or store it in easy to find places or file on or near your computer
- use a completely new password every time you change your password and never reuse old passwords
- avoid using dictionary or foreign words because hackers have many tools, such as dictionary programs, to assist them. A hacker will launch a dictionary attack by

passing every word in a dictionary (which can contain foreign languages as well as the entire English language) to a login program in the hope that it will eventually match the correct password

- never share your password with anyone
- never send your password via email
- change your passwords regularly, at least every three months.

What is password cracking?

Password cracking is the process of breaking passwords to gain unauthorised access to a computer system.



8. Keep your software up-to-date

When computers were first introduced on a large scale by small businesses, the software being used was often updated only once or twice a year and sometimes not at all until a new computer was purchased. This was acceptable in the 1980s and early 1990s as there were fewer businesses reliant on computers connected to the Internet.

As many computers are now connected to the Internet, security of data is becoming an important issue. It is essential that computer software is kept up-to-date with the latest security patches. As hackers are always trying to find new ways to break into computers that are online, software companies release updates and corrective patches to software via their websites. Updates are usually provided free if you have bought a legitimate version of the software.

What you can do

To be sure your critical software is up-to-date:

- draw up a list of all the critical software you use—e.g. operating system, email, firewall, spam filters, anti-virus
- access the relevant vendor's website and check to see that you have the latest version
- as part of your security plan, check for new security patches and updates on a regular basis
- whenever possible, use software that provides an automatic updating feature and make sure you turn it on. Usually this will automatically explore the vendor's website for new updates and then download and install them automatically whenever you log on to the Internet.

Further information

The supplier of your software, computers and your Internet service provider may provide information on the latest in software updates and security risks. It would be useful to visit their websites for new information and to subscribe to newsletters for software upgrades and other security issues in general.

What is a patch?

A patch is a solution provided by a vendor to address vulnerabilities in existing software. It is vital to install any new patches that are made available. Patches can usually be downloaded from the relevant vendor's website.

9. Make sure your online banking is secure

Banking online provides a convenient way for Internet users to manage their accounts.

Internet banking fraud

If you bank online you should be aware of the dangers of attempts to steal your credentials by using fraudulent email messages that appear to come from legitimate businesses.

These authentic-looking messages often create a sense of urgency, and are designed to fool recipients into divulging personal data such as account numbers, passwords and credit card numbers.

Phishing

'Phishing' is a technique used to gain personal information for the purpose of identity theft. 'Phishing' emails give themselves away by telling you that there is a reason why you must provide personal details such as your Internet banking log-on, password, credit card number or personal identification number by reply email or through a website. It is common for 'phishing' emails to contain links to a website that is a convincing replica of the financial institution's home page.

Financial institutions do not communicate with customers about account details by email.

If you are concerned that you have been affected by a 'phishing' or other email scam, you should contact your financial institution immediately. You should also contact the Australian High Tech Crime Centre (AHTCC). You will find AHTCC's contact details on their website: www.ahfcc.gov.au.

What you can do

To make sure that your online banking is secure, there are some things you can do:

- always type the address of your bank website into your browser; never use a link that has been sent to you by email
- be suspicious of email that creates a false sense of urgency
- follow the rules for secure use of passwords that appear in this document
- follow the tips on virus protection, firewalls and harmful emails
- ensure that you are aware of the security advice provided by your financial institution.

Further information

‘Phishing - don’t take the bait!’ is at www.dcita.gov.au/e-security

‘Australian Bankers’ Association warns customers of cybercrime’ can be found at www.bankers.asn.au/ABA/Online/default.asp. Click on ‘news’ and then ‘media releases’.

Ensure that you are aware of the security advice provided by your financial institution.

If you do happen to experience a ‘phishing’ incident, you should inform your financial institution and the Australian High Tech Crime Centre (AHTCC)—www.ahtcc.gov.au

10. Develop and maintain a security policy

Developing good security practice is simply a matter of establishing and following some basic security procedures that suit your business needs.

Once the security policy is implemented, it needs to become an integral part of day-to-day business activities and general business culture.

You and your staff need to keep abreast of information on current Internet security issues so that the security policy you develop stays up-to-date.

Maintaining the security policy is a day-to-day business activity for everyone, for example, checking email for viruses and logging off the computer from the Internet at the end of the day.

Monitor and test the security policy you have in place to identify potential and actual security problems before they become issues that may cost your business time and money.


What you can do

In order to have and maintain a good security policy:

- analyse and assess your business requirements and determine the appropriate security measures
- develop and implement a security policy, making sure all staff are aware of the security policy and provide training
- install security measures on all new computers.

Resources





Internet security essentials checklist

Things you should have

- antivirus software
- appropriate firewalls
- spam-filtering software
- a disaster recovery plan in place
- strong passwords

Things you should do

- regularly install security updates for your anti-virus software and firewall applications
- use caution when introducing external software/hardware
- apply common sense when dealing with any emails
- see what services your Internet service provider can offer, i.e. software updates and security alerts, spam filters and firewalls
- ensure that back-up procedures are in place and tested
- ensure security patches for your operating systems and application software are up-to-date and updated regularly
- change your password regularly, at least every three months

Things you should avoid

- opening any email attachments from unknown or questionable sources
- clicking on links in any email if the content of the email is suspicious or unfamiliar
- using passwords that can be easily cracked, guessed or associated with you
- storing back-up files at your premises

