

trusting the internet



small
business
guide to
e-security



trust

About this guide

This guide describes how to ensure that business transactions carried out on the Internet are safe and secure. It was commissioned by the National Office for the Information Economy (NOIE) to increase awareness of e-commerce security and authentication technologies relevant to small to medium sized businesses.

Disclaimer

Examples of security and authentication technologies and companies in the text are provided purely as illustrative examples. NOIE does not recommend or endorse any product, service or company mentioned.

© Commonwealth of Australia

ISBN 1 74082 009 6

ISBN ONLINE 1 74082 010 X

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without the prior written permission from the National Office for the Information Economy. Requests and inquiries concerning reproduction and rights should be addressed to:

The Chief Executive Officer
National Office for the Information Economy
GPO Box 390
Canberra ACT 2601
Australia

www.noie.gov.au/trustingtheinternet

July 2002

foreword



Small and medium businesses in Australia are making increasing use of Internet technologies.

Small and medium businesses in Australia are making increasing use of Internet technologies, recognising they can be a valuable tool in improving the efficiency and profitability of their businesses. It is therefore important to ensure that the use of Internet technologies is properly understood and effectively managed.

Trusting the Internet is aimed at helping Australian small and medium businesses understand the key issues of Internet security - when browsing a website, sending emails, conducting e-commerce transactions, dealing with government agencies online and conducting e-business activities.

It explains in simple, easy to understand terminology how to ensure that you and your business are secure in the online environment.

Trusting the Internet is the first component of an initiative that aims to accelerate the uptake of e-commerce by small and medium sized business that was announced by the Government in September 2001 as part of a broader assistance package for Australian Small Business.

The publication responds to market research commissioned by the National Office for the Information Economy (NOIE) that indicated that small and medium businesses were confused about emerging Internet security technologies and mystified about how they could secure

e-commerce transactions. The study revealed that business and consumer concerns about security and privacy were in turn impediments to the expansion of e-commerce in the Australian economy.

This guide explains the simple use of secure Internet technologies and aims to make businesses aware of the latest developments in areas such as privacy and the protection of online data. This has become particularly important with the introduction of the *Privacy Amendment (Private Sector) Act 2000* that came into effect on 21 December 2001.

I commend this report to small and medium sized enterprises, and encourage them to adopt a proactive approach to realising their e-commerce goals through *Trusting the Internet*.

Senator The Hon Richard Alston

Minister for Communications, Information Technology and the Arts

contents



Foreword	i
Contents	ii
1. Why do I need e-security?	1
2. How do e-security technologies work?	3
3. How can I send emails securely?	9
4. How can I conduct secure transactions online?	13
5. How can I deal with other e-security threats?	17
6. Why is privacy an important issue for e-security?	21
7. What laws apply to e-business?	25
8. Where can I find more information?	27
9. How Do I?	31
Glossary	43

1. Why do I need e-security?



As the Internet becomes an increasingly important tool for businesses, electronic security (e-security) has emerged as a major issue. Many businesses want to expand their use of the Internet but are not sure how to do so in a secure way. This guide will help you decide which technologies are appropriate for your business e-security needs.

If your business is connected to the Internet, it is essential to ensure that your business data, including customer information, is safe and that your transactions are carried out securely. Otherwise, you risk transactions being intercepted, breaching privacy and losing money.



The potential of the Internet

Originally developed as a network for military communication, the Internet now connects millions of computers all over the world, allowing governments, businesses and individuals to exchange a wide variety of information. Email and the World Wide Web are two of the most popular services to make use of the Internet. An estimated 500 million people are now connected to the Internet, and the number continues to rise.

There are many benefits to doing business over the Internet, including:

- Increased potential customer base;
- Reduced paperwork and administration;
- Reduced time taken to receive orders, supply goods and make and receive payments; and
- Access to a greater range of suppliers.

As well as sending emails and browsing the Internet, specialised business applications you may wish to consider include:

- E-banking (organising your accounts and paying bills);
- E-shopping (purchasing goods from a merchant's website);
- E-tailing (selling goods to shoppers from your website);
- Sending and receiving orders to and from business partners; and
- Lodging your tax return or business activity statement (BAS), or conducting other transactions with government agencies.

An estimated 500 million people are now connected to the Internet, and the number continues to rise.

Why security is an issue on the Internet

Although it offers many benefits to businesses, the Net does carry risks. Because it is designed to offer easy communication between individual computers, it opens up the possibility of outsiders breaking into your computer systems and stealing valuable information such as credit card numbers. Information on how to perform such 'hacking' activity is itself widely available on the Internet, making the risk a very real one. One international gang discovered by the FBI last year had stolen more than one million credit card numbers via the Internet.

Any information transmitted over the Internet can be intercepted at any point if appropriate security precautions have not been taken. You need to take electronic security (e-security) measures for any business activities conducted online, to protect both yourself and your customers. This is particularly important where businesses are using broadband technology because of its continuous connection to the Internet.

Just as you would not open a store without taking measures to ensure it could not be burgled, you should not establish a business presence online without taking appropriate e-security measures. However, securing your business electronically is not quite as simple as installing a padlock on your front door.

Overview of this guide

Businesses need to consider whether they want basic applications such as email to be secured; how they will go about buying and selling online; how to protect computer systems from the threat of data theft; and what the legal issues surrounding e-business are. This guide will help you understand the technologies used in each of these cases, and point you to further information.

Conclusion

The rest of this report will help you choose the most appropriate e-security solutions. For a general overview of e-security, read the next section, 'How do e-security technologies work?' Subsequent sections explain how to implement specific e-security solutions for email, carrying out online transactions, and helping protect your business from cyber threats. The 'How Do I?' section at the end summarises important actions you will need to take for your business.

Additional information on e-security, including fact sheets, case studies and extra copies of this report, can be found on the NOIE website.

Where to go online for further information

Trusting The Internet – www.noie.gov.au

2. How do e-security technologies work?



E-security technologies ensure that business can be conducted online in a secure, authenticated, confidential and verifiable environment. Common choices for security solutions include password authentication systems, secure network or interconnection tools and secure managed services. Each option has different cost and security benefits and each business will need to analyse its requirements individually. Used properly, e-business authentication systems can be more effective than 'traditional' means of conducting business transactions. This chapter should will help you understand these issues and how you can make your business more secure today.



Conducting
business online
requires sending
information safely
between people and
companies.

Conducting business online requires sending information safely between people and companies. When you send information over the Internet (for example, paying a bill via an online banking site or sending an email to a prospective client), there are four basic security principles you should always consider:

- **Authenticity** – “How do I know who sent me this?” For most online transactions, businesses will want to know that the person conducting the transaction is who they claim to be. For example, only authorised signatories should be able to access a business bank account.
- **Security** – “How do I know this hasn’t been tampered with?” Businesses must be confident that transaction details and other valuable commercial information will not be accessible to anyone other than those involved in the transaction. For example, when using online banking, transaction details should not be able to be intercepted.

- **Non-repudiation** – “How do I know they won’t deny sending this?” Businesses need certainty that a transaction conducted over the Internet is irrevocable, and that the person who conducted the transaction will not be able to deny later that the transaction took place. For example, transfers of money between bank accounts must be accurately recorded.
- **Privacy and confidentiality** – “How do I know no-one else will see this?” All businesses have an obligation to ensure that confidential customer data remains private, and that customers have control over how that information is used. As of December 2001, businesses with a turnover of greater than \$3 million must comply with new Federal privacy legislation to protect customers’ personal information.

There are many e-security technologies available, and each addresses these four principles in different ways. When choosing between them, you will need to consider how important each of those principles is for your planned business activity. In many cases, one technology solution

will cover more than one of these areas. For instance, if a transaction has been made securely, then it should not be possible for privacy to be violated either.

Not all these problems can be solved with technology alone. For instance, to ensure customer privacy it is essential for businesses to have a well-thought-out privacy policy. Similarly, you will need to implement an email security policy if you want to ensure that all employees are sending messages securely.

Authentication technologies

Business is built around trust and relationships. For these to work, customers and businesses need to be sure of who they are dealing with. In the physical world, we confirm (or authenticate) people's identities using physical information. For instance, we might recognise a person's face or their voice. If we receive a letter from a business, we will typically check to ensure the letterhead and signature are correct.

Physical checks are not possible on the Internet, so we must rely on other means to confirm identity and that the information we send and receive is not being tampered with.

Most authentication technologies rely on a combination of one or more of the following elements:

Something you know, such as a password or PIN;

Something you possess, such as a smart card or access key; and

Something you are – a unique physical quality, such as your fingerprint or iris (an area collectively known as biometrics).

A familiar form of electronic authentication is the use of passwords to restrict access to PCs or computer networks. A bank PIN is another use of a password, in this instance combined with a secure access device (the card you insert into the automatic teller machine). Biometric systems are rather less common, but have become more affordable in recent years.

Most e-security systems suitable for small businesses rely on password systems. Enhanced options for authenticating identities and communications include:

- Encryption systems provide a means of sending data in encrypted or secure form between different Internet locations. Secure Sockets Layer (SSL) technology is often used for online shopping applications. When used on shopping sites, SSL is, for example, usually represented by a padlock icon that appears at the bottom of your web browser screen.
- Public key infrastructure (PKI), which uses digital signature certificates to authenticate individuals and companies. This technology is being widely adopted by government agencies for online transactions. A simpler version, Pretty Good Privacy (PGP), is often used for emails.
- Virtual private networks (VPNs), which are used by large businesses to allow remote employees to securely connect to central computer networks via the Internet, for example. If you are a small company but supply to larger businesses, you may find you are required to join or transact over their VPN.
- Secure managed services, where security applications (which could include any or all of the above examples) are outsourced to an external provider. Here, service level agreements may be an issue to consider (also see below).

The workings of these different technologies are explained briefly below. A comparison of what they offer and a discussion of how to use them more effectively in your business can be found in the 'E-security Technology Overview' at the end of this guide.

Not all these problems can be solved with technology alone.

Secure access (password authentication)

In password authentication systems, each user of a site or computer is assigned a unique username and password. If the correct password is entered, access to a site or service is granted; if not, access is denied. Passwords are widely implemented in many software packages, but offer only a relatively low level of security.

Password-only systems are generally regarded as being an inadequate form of security for most e-commerce activities. However, they still have a role to play in applications where the need for security is not high and costs must be kept to a minimum.

A very common form of authentication used by banks to secure access to their systems is the use of passwords combined with a security token. Security tokens are physical tokens which have a unique or randomly generated number or password. The combination of passwords and tokens is often called two factor authentication.

Secure connections (SSL)

Secure Sockets Layer (SSL) combines a basic password system with extra security for website access. Once a website verifies that a username and password match up, it creates a secure connection for exchanging confidential information.

SSL is designed to prevent anyone except the intended recipient of the message from being able to read it. It is often used by websites to sell products and services. (SSL is discussed in more detail in the section 'How can I conduct secure transactions online?')

Secure interconnection (PKI)

Public key infrastructure (PKI) is used by government agencies and banks for secure transactions. For instance, the Australian Tax Office (ATO) uses it for handling quarterly Business Activity Statements (BAS) and tax returns. In 2000/2001, 280,000 people used PKI to submit their tax returns electronically.

PKI makes use of a system known as public key cryptography, combined with carefully documented policies, to ensure that transactions are authentic and secure. Public key cryptography uses two keys to scramble and decipher messages. One key is known as a 'public key' and is widely distributed. The other is called a 'private key' and is held secretly by an individual. Messages are protected by scrambling them with the public key of the recipient. Computer algorithms ensure that only the private key held by the person you are mailing can decrypt or unscramble the message. The larger the key files involved, the higher the level of security.

In a PKI system, certificates and keys are issued by Certification Authorities (CAs) under defined guidelines, which ensures a high level of reliability. For greater security, the access keys used by these systems can be stored on security devices such as smart cards or hardware tokens (see the 'E-Security Technology Overview' at the end of this guide for more details). Sometimes, biometric identifiers (such as fingerprints) are also included to add another level of protection. This provides for a very strong level of assurance and would be used for high-value transactions.

Secure Sockets Layer (SSL)

combines a basic

password system

with extra security for

website access.

PKI in action

Bob, the manager of XYZ Car Parts, wants to lodge his Business Activity Statement via the Internet. To enable this process, the ATO issues Bob with special software for this task, which includes the security 'keys' described below.

1. A *signing key*. This key is unique to Bob's business and enables the ATO to verify that Bob is really the person who has sent the BAS when it arrives. It consists of two corresponding keys: a *private key*, which Bob keeps, and a *public key*, which the ATO keeps to check Bob's messages.
2. A *confidentiality key*. This enables the ATO to verify that the information contained in the BAS has not been tampered with on its way from XYZ to the ATO. Like the signing key, it also consists of two corresponding keys: a public key, which the ATO issues to everyone wishing to send messages to the ATO, and a private key, which the ATO keeps to 'unlock' the messages received.

Once Bob has prepared his BAS for sending, he signs the message with his private signing key, encrypts the message with the public confidentiality key provided by the ATO, and sends the message via the Internet.

The ATO receives Bob's message, decrypts the message with the ATO's private confidentiality key and uses Bob's public signing key to check that Bob was the person who signed the message. The ATO then knows that:

- The message genuinely came from Bob;
- Bob cannot deny sending it; and
- The message has not been altered from the time Bob signed it.

While this example uses the ATO, the same process could be used by any business that wanted to carry out secure transactions. However, the keys might not be issued directly by that business; they could come from a trusted third party such as a certification authority.

It is important that Bob is the only person who can sign his message to the ATO, just as he is the only person who can create his real-life signature on paper. To ensure this, he must keep his private signing key secret.

Secure personal connection (PGP)

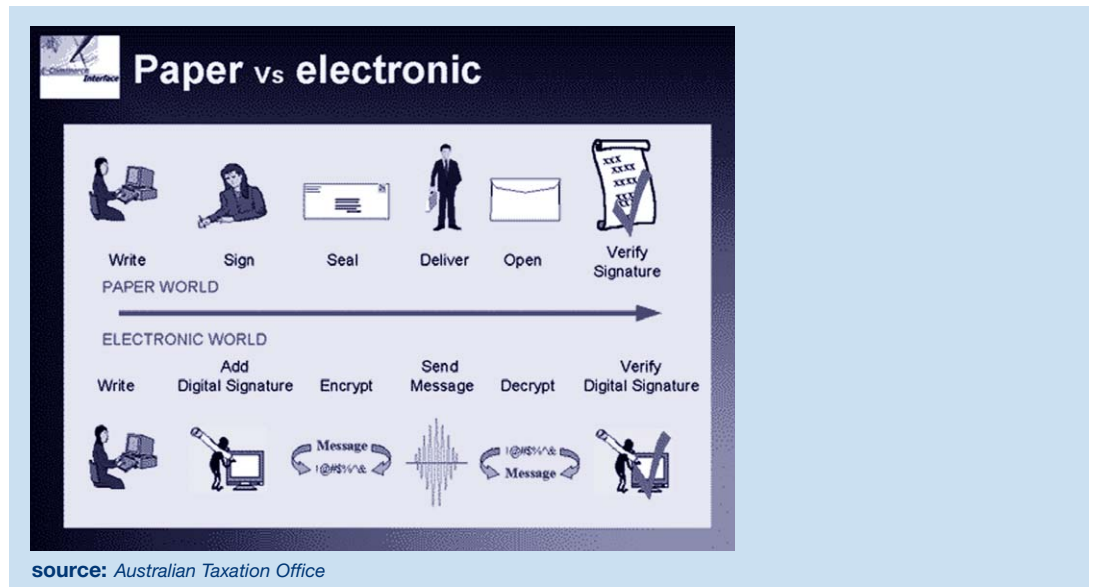
Pretty Good Privacy (PGP) is a popular security option for individuals. Like PKI, it uses public key encryption. However, unlike PKI, it allows users to generate their own public and private keys. This makes it cheaper and easier to implement, but does not offer the same reassurance as a certificate issued by an independent third party.

Secure networking (VPNs)

Virtual private networks (VPNs) use advanced encryption and 'tunnelling' technologies to enable businesses to establish secure private connections between their corporate networks and third-party networks such as the Internet. VPNs allow mobile workers and businesses with multiple office sites to communicate securely at high speeds. They offer one of the highest levels of network and Internet security, but may be an expensive solution for smaller businesses.

Pretty Good Privacy (PGP)

is a popular security option for individuals.



Secure managed services

The main benefit of secure managed services is that small and medium sized companies do not need to invest heavily in e-security technologies or training.

Many small businesses choose to outsource their information technology requirements so they can concentrate on their main business objectives. This approach can be successfully extended to security, especially if an outside company is used to host your business website.

Outsourced e-security services are often referred to as secure managed services, and are usually provided for a fixed monthly fee. Secure managed services can also be an effective way of implementing technologies such as firewalls and anti-virus packages (discussed in the section ‘How can I deal with other e-security threats?’).

The main benefit of secure managed services is that small and medium sized companies do not need to invest heavily in e-security technologies or training. However, the business is still responsible for ensuring e-security is adequate. Any arrangement with a secure managed services provider should be based on a well-developed Service Level Agreement (SLA) that outlines the quality and type of service required and includes penalties for failure to deliver.

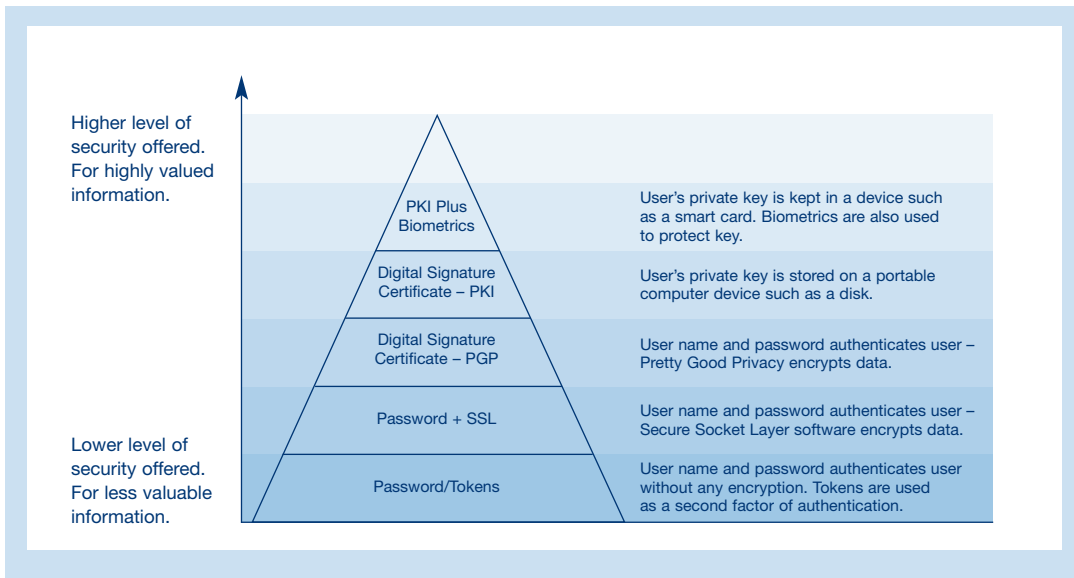
E-security and the real world

While e-security authentication processes may seem new and confusing, they have equivalents in the traditional business world. The diagram above shows how processes in the paper world relate to equivalent processes in the electronic world.

It is also worth noting that online authentication can be much more efficient than traditional processes. For instance, when a business receives a purchase order by fax, they will typically fulfil that order in the belief that the sender of the fax is actually who they claim to be. While a check of the letterhead or signature might be made, these elements can easily be forged. As well, the person who appears to have signed a fax may later dispute having done so, and it may be hard to prove that they did. This scenario is much less likely when electronic authentication is used, especially if both parties use PKI.

At the same time, the use of online systems can promote efficiency. Companies can save valuable time because data does not have to be re-entered from a fax to their computer system. The risk of incorrect data entry is also reduced.

The Pyramid of Authentication Technologies



Choosing the right option

Obviously, not every business needs to invest in every available e-security technology. The level of e-security required will depend on how extensively you wish to take advantage of Internet technologies, and how much you are prepared to spend. The Pyramid of Authentication Technologies (above) shows the trade-offs in security and popularity in the main systems on offer.

Conclusion

There are many solutions available to help introduce e-security to your business. Basic systems such as passwords are low cost and easy to implement, but don't provide the same degree of security as more elaborate systems such as PKI. Your business is likely to need a mixture of solutions. For instance, you might use password protection for most internal business requirements, and PKI to lodge financial documents with your bank and government authorities.

How to make it happen

There are more details on how to implement some of these solutions in the 'E-Security Technology Overview' at the end of this guide.

However, whatever solution you choose, you may decide to get an expert e-security consultant to help you implement it.

Where to go online

for more information Capability Directory of Electronic Authentication Technologies – <http://www.aeema.asn.au/neac>

The Defence Signals Directorate plays a key role in the protection of Australian official communications and information systems and has established the Australasian Information Security Evaluation Program.

E-security products are listed on the Evaluated Products List – <http://www.dsd.gov.au/infosec/>

If you are searching the Web on this topic, try the following search terms:

– e-security, authentication, PKI, PGP, SSL

3. how can I send emails securely?



Email is a key form of business communication, but standard email software offers very poor security. Options for increasing the security of your email include secure Web-based email, dedicated email encryption software, and secure email gateways.



When an email is sent, it is normally impossible to prove who has sent it because emails are very easy to intercept.

Today, there are many more emails sent than letters posted. Sending and receiving email has become an indispensable form of personal, business and government communication. Even if your business has no plans to sell goods online, it is likely that you are using email to keep in touch with staff, customers and suppliers.

Whether you use a Web-based email service (such as Hotmail or Yahoo) or an email package (such as Outlook, Exchange, Eudora or Notes), you need to know about secure email and encryption.

When an email is sent, it is normally impossible to prove who has sent it because emails are very easy to intercept. It is also easy for someone to assume, or fake, another person's email address (this is known as spoofing). Sending an unsecured email message is like sending a postcard – anyone can read it along the way.

Email messages passing between mail servers can easily be captured or copied, viewed and modified by an unauthorised party before the message is forwarded to the next server.

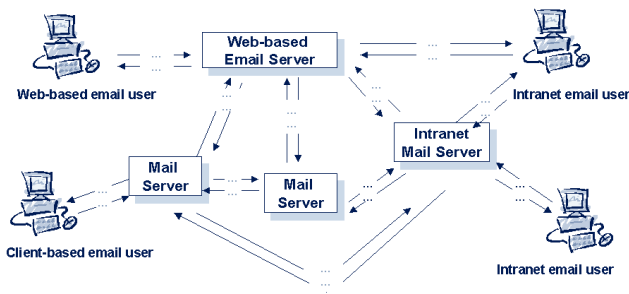
Unsecured email makes it easy for competitors and unauthorised parties to gain confidential information about your operations. In a legal context, an email that has been tampered with during transmission may still be accepted as legally binding.

Email security products solve the problems associated with standard email by 'encrypting' the mail so it cannot be read by anyone other than the intended recipient. Cryptography is the process of putting messages into a 'secret code' so they can't be read if they're intercepted.

Most email security products use a variant on public key cryptography (described in the previous section, 'How do e-security technologies work?'). There are numerous off-the-shelf and downloadable products available to do this. Secure email services can also be accessed online, and some Web-based services are available free of charge for basic functions.

Email can be intercepted at any point during transfer

... Potential opportunity for your email to be viewed, intercepted or hacked



Email Transfer

Email travels to various computers or servers before reaching the person you are sending to. If your email is not encrypted, it can be viewed by a third party without your knowledge.

In most cases, secure email services will only work if both the sender and the recipient are using the same software. For this reason, it will generally be impossible to secure all your email transactions. However, you should be able to agree on a standard approach with key business partners and for your own staff.

Secure Web email

For businesses that require only occasional access to secure email, a free, Web-based service is a sensible choice. A list of some key providers is given below.

Getting a secure email account from these services is normally only a matter of filling out a form online. Many of them are free, but some will charge you for 'premium' services such as technical support or sending large attachments. Remember that these services generally will not guarantee the security of emails sent to non-users of the service. You will need to talk to your key business partners or customers about setting up the same secure email software.

Where to go online

Groove Networks – www.groove.net

HushMail – www.hushmail.com

LokMail – www.lokmail.com

Getting a secure email account from these services is normally only a matter of filling out a form online.

Dedicated email encryption

Encryption-based email software packages use a technique known as public key cryptography (the same system used for PKI and PGP) to 'scramble' messages so that only the authorised recipient can read them. In some cases, security 'plug-ins' can be added to your existing email software. For instance, PGP is available as a plug-in to popular email clients such as Microsoft Outlook, Outlook Express, Eudora and Netscape Messenger. (The workings of public key cryptography are explained in more detail in the 'E-Security Technology Overview' at the end of this guide.)

Email software packages using public key cryptography are very secure and relatively simple to use, especially as there is now a defined security standard (S/MIME) for all email software developers to use. The main difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for them. Some software packages and common operating systems such as Microsoft Windows now include facilities to manage public key information.

Within your business, it is important that everyone's email system is set up to meet the security standards you require. For example, a policy might state that all emails shall be signed and encrypted.

Secure email gateways

Some businesses find that it is more appropriate and efficient for emails to remain unsecured within their own environment and then be secured when they pass out into the Internet. In other words, internal mail is not secure, but external mail is.

To meet this requirement, email gateway security products are available. These 'capture' outgoing email and ensure that it is sent securely. Gateway products are sometimes combined with content analysis tools, which open up emails to check for inappropriate content.

Secure email versus postal mail

Using the analogy of a paper-based transaction, secure email systems provide the following advantages:

- A secure 'envelope' for you to seal your document so no-one except the intended recipient(s) can open it. Each recipient can even put the contents back inside the secure envelope for long-term storage if they want to make sure no-one can read the contents from their PC.
- Inside the envelope is a signed, authenticated document that can be archived along with the signature for non-repudiation. Any attachments are also signed and authenticated.

Conclusion

For electronic mail within your business or simple customer communications, secure electronic mail may not be necessary. However, if you deal regularly with confidential documents or want to take orders via email, then you should consider introducing a secure email system.

How to make it happen

You need to decide how much of your email communication needs to be secured. If you will only require secure email occasionally, a Web-based service or plug-in to your existing email software will suffice.

For more dedicated email security, you may need to change your email software or install a gateway system. You might want to use outside consultants.

Web addresses for some suppliers of secure email products and services are listed below. The Capability Directory of Electronic Authentication Technologies provides a fuller list of organisations that can assist you with this task.

Where to go online for more information

Australian Projects –

www.austprojects.com.au

BeTRUSTed – www.betrusted.com.au

eSign – www.esign.com.au

KPMG – www.kpmgca.com

RSA Security – www.rsasecurity.com

SecureNet- www.securenet.com.au

Telstra – www.telstra.com.au

Capability Directory of Electronic Authentication Technologies –

<http://www.aeema.asn.au/neac>

If you are searching the Web on this topic, try the following search terms:

– email security, cryptography, secure email

4. How can I conduct secure transactions online?

//

Many businesses choose to use Secure Sockets Layer (SSL) to provide secure transactions via their website. SSL provides an easy means of securing transactions, but it does have restrictions that need to be recognised, including limited customer authentication.



SSL and e-commerce

E-commerce can involve any or all of the processes of selling goods, buying goods, making payments or receiving payments. For all of these activities, a secure environment is essential so that funds and customer information can be exchanged with confidence.

For Web-based businesses, the most popular choice remains Secure Sockets Layer (SSL), which provides an easy means of protecting data being transferred between a browser and a website. A key reason for SSL's popularity is that it is supported in most popular Web browsers, meaning customers don't need any additional software.

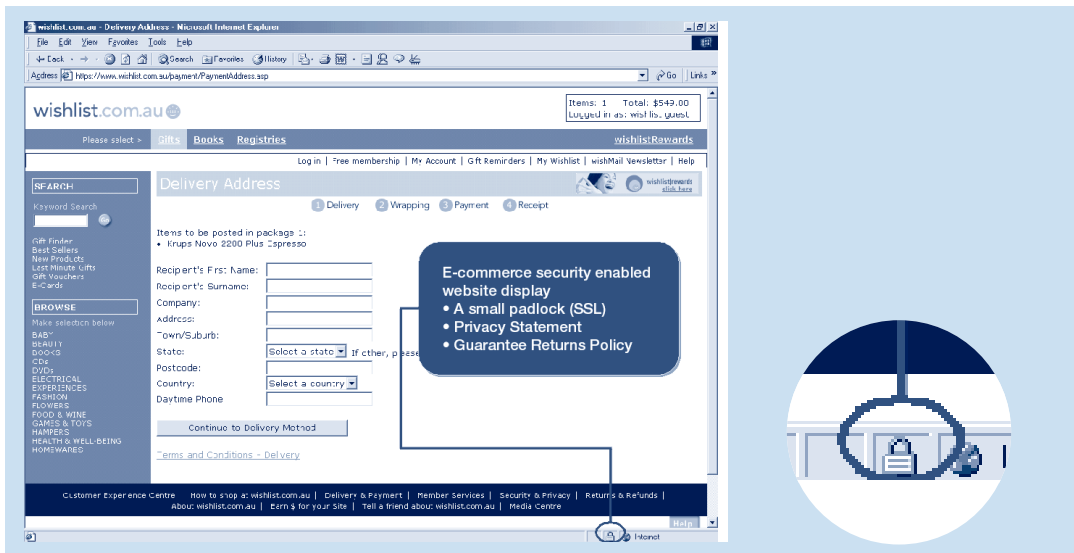
Sites that use SSL often use a password to log users in, but that password information and all subsequent data are sent via a secure SSL session. The session provides an encrypted channel for all data sent between the user and the website.

SSL actually uses the same public key cryptography model as PKI. Each site using SSL will have a public and private key associated with it. These will be queried by the web browser when the secure site is accessed.

In most cases, SSL is virtually transparent to the user. Their browser may display a warning message to tell them they are beginning or ending a secure connection, and a small padlock might appear in the bottom right-hand corner of the screen. (Website addresses for secure sites also generally begin with https:// rather than http://.)

E-commerce

can involve any or all of the processes of selling goods, buying goods, making payments or receiving payments.



What it looks like

To ensure that the website that is selling a product or service is using SSL, look for the small padlock in the bottom right hand corner of the Internet browser as shown in the www.wishlist.com.au example above.

When the padlock in the bottom right hand corner of the Internet browser appears on the screen, the computer has successfully established a secure connection with the Wishlist website (see www.wishlist.com.au). This ensures that personal details, order details, credit card details, delivery address and contact telephone numbers are protected whilst they are sent to the Wishlist online store. In order to verify that the issuer of the Digital Certificate is who they say they are, double click the padlock. This provides information including details on the organisation that issued the Certificate and how long it is valid for.

SSL limitations

While SSL is very useful, it does have limitations. Issues to consider before implementing an SSL site include:

- Data transmitted using SSL is only secure on its way between the browser and the Web server. If that data is subsequently moved to another location, security may be compromised. If, for example, your Web

hosting company collects data via an SSL site but then forwards it to you via email, it may not be secure on the second part of the journey.

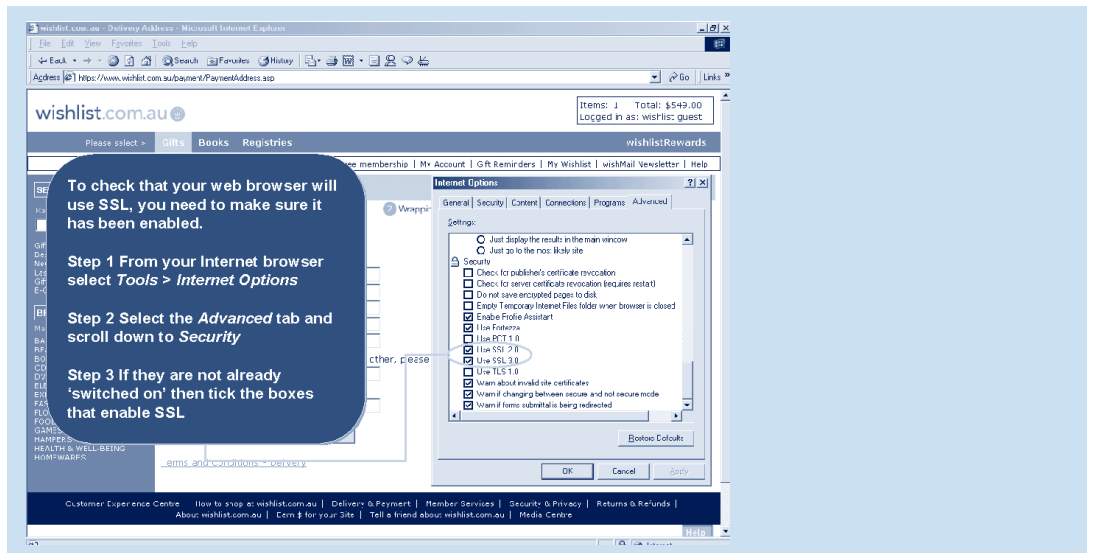
- SSL provides strong authentication for a company website, since it uses public key cryptography. However, it does not guarantee the identity of the customer beyond a basic password check, unless customers are forced to use cryptography as well.

Using the analogy of a paper transaction, SSL provides the following:

- A secure envelope into which you can seal your document when you send it;
- A guarantee to you that the destination address to which the envelope is sent is owned by that business; and
- A signature on the envelope that guarantees it really was you who sent it (if you have been set up with your own keys and certificates).

What SSL does not provide is:

- Any guarantee to you that the destination address is actually operated by the business; or
- Any security processing on the document itself. Once the envelope has been opened (and thrown away), the business is effectively left with an unsigned document.



SSL limitations:

- Some SSL users have been subject to a “**Certificate injection threat**” where a malicious SSL certificate is added to the user’s list of trusted root certificate authorities. A number of publicly disclosed vulnerabilities in Internet Explorer and Windows Media Player have allowed the attacks.
- What to do about it? In an enterprise environment, it is possible to use file and registry permissions to restrict access to the list of trusted root CAs either via software policies or by “hardening” the workstation build.
- Windows 98 users cannot easily protect themselves from this style of attack since the operating system does not support registry or file permissions. A possible mitigation strategy for Windows 98 users would be to run a program which periodically checks critical parts of the registry. Such functionality may be incorporated into a future version of anti-virus software.
- In the meantime, check the Microsoft security bulletins MS02-005 Patch for Internet Explorer at www.microsoft.com/technet/security/bulletin/MS02-005.asp
- Other Security Bulletins for Windows Media Player at www.microsoft.com/technet/security/bulletin/MS01-056.asp
(Reproduced with thanks to Defence Signals Directorate, Computer Network Vulnerability Team, white paper “SSL Vulnerabilities” presented at AusCERT 2002 and available on the NOIE website)

Conclusion

For many small businesses, SSL will provide sufficient security for online shopping and payment processing. However, if you will be dealing with high-value transactions, you may want to consider a more extensive PKI-based solution.

How to make it happen

Many e-commerce software packages already include support for SSL. If you are setting up a retail or payments website, your bank or financial institution may also provide SSL-based shopping services as part of its business banking offerings. Your Internet service provider may also be able to advise you.

If you find setting up an e-commerce-enabled site difficult, you may seek to employ a consultant to help. The Capability Directory of Electronic Authentication Technologies provides a list of organisations that can assist in setting up a secure website.

Where to go online for more information

Capability Directory of Electronic Authentication Technologies – <http://www.aeema.asn.au/neac>

Several useful free guides are at <http://www.esign.com.au/>

If you are searching the Web on this topic, try the following search terms:

- SSL, e-business, secure transactions, electronic banking

5. How can I deal with other e-security threats?



All businesses need to take measures to deal with e-security threats such as hacking and viruses. This is done by installing specialised software such as anti-virus tools or firewalls. By making these elements part of your overall e-security plan you can greatly reduce the threat that such risks pose to your organisation.



Implementing e-security for your business is not simply a matter of setting up authentication systems.

Implementing e-security for your business is not simply a matter of setting up authentication systems. There are also a number of general security issues relating to Internet use that you need to consider, including:

- **Viruses.** Viruses are malicious pieces of computer code that make unauthorised changes to your PCs. They often distribute themselves via the Internet or email.
- **Hacking.** Hacking is where individuals gain or attempt to gain unauthorised access to your computer systems. Potential hacking activities include denial of service (DoS) attacks, port scanning and dumping.

This section outlines how you can deal with these threats. As with all the e-security solutions described in this guide, it is important to tailor the solution to the needs of your business – spending too much can be just as dangerous as spending too little.

Viruses

A computer virus is a program or piece of code that is loaded onto a computer and is capable of attaching itself to other files and replicating itself repeatedly, usually without the user's knowledge or permission. A virus can be transmitted through an attachment to an email, by downloading infected programming from other websites, or through a floppy disk or CD.

Some viruses will activate as soon as the infected file is opened, while others will lie dormant in the computer system until activated by a trigger. The trigger could be reaching a specific date or activating a particular function (such as reading an email). While some viruses replicate themselves without causing any further damage, most will also attempt to carry out other activities (known as the virus 'payload'). This can range from sending random emails to deleting the entire contents of your PC.

Other virus-related attacks include worms and trojans. Worms differ from regular viruses in that they only reside in computer memory, rather than

attaching themselves to system files. Many email viruses (such as Melissa and the Love Bug) are worms. Trojans are pieces of code hidden in what appears to be legitimate software. For instance, a game you download from the Internet may also contain code to monitor which Internet sites you visit.

The best protection against computer viruses is to use anti-virus software. By being proactive and keeping such systems up to date, you can significantly reduce the risk of your business being harmed by viruses. Anti-virus software should be installed on all your business and home PCs, and updated regularly to ensure you are protected when new viruses emerge. Most anti-virus software packages include regular free updates that you can download from the Internet.

Other steps you can take to protect against virus attacks include:

- Being cautious about opening unsolicited emails, especially if they contain attachments;
- Only downloading software from trusted sites; and
- Disconnecting your PC from the Internet when not in use.

Hacking

Hacking is any attempt by an intruder to gain unauthorised access to your computer systems. Without appropriate security measures in place, any PC connected to the Internet can be vulnerable to attack. Systems used to host websites are frequent targets for hackers.

Activities carried out by hackers fall into several categories, including:

- Denial of service (DoS) attacks;
- Dumping; and
- Port scanning and sniffing.

Each of these potential attacks requires slightly different preventative measures.

Denial of service

In a denial of service (DoS) attack, hackers bombard a website (or other Internet-connected PCs) with requests for information, making it difficult for other users to access. In many cases, DoS attacks can render a device or network unusable. Hackers have developed software to automate DoS attacks, meaning they can be launched by relatively unskilled individuals, and even by business rivals.

While many DoS attacks are aimed at large, well-known businesses, a DoS attack could have a damaging effect on your business. Fortunately, there is good anti-DoS attack software available that offers protection from most DoS attack programs. If your website is hosted by an external company, make sure protection against DoS attacks has been implemented.

While many DoS attacks are aimed at large, well-known businesses, a DoS attack could have a damaging effect on your business.

Dumping

Internet 'dumping' is when someone takes control of your computer's modem to place calls to high-cost premium rate or international numbers. This can be achieved by inducing users (often by promising adult content) to download new Internet dialler software, replacing their ISP connection. Proving that dumping is conducted without the user's knowledge can often be difficult.

To prevent dumping, ask your telecommunications company to place a bar on all premium calls starting with 190 (e.g. 1900, 1901, 1902, etc.) and on international phone services. If the problem persists, then you can lodge a complaint with the Telecommunications Industry Ombudsman at www.tio.com.au. If your business PCs are not equipped with modems, dumping should not be a problem for you.

Port scanning and sniffing

Dedicated hackers are constantly on the lookout for new systems to hack into. To try to gain information about computers connected to the Internet, hackers use techniques such as port scanning and sniffing, both of which try to find vulnerabilities.

Even if hackers do not gain access, port scanning can increase your Internet usage as it will cause extra data to be transmitted from your PC. If you are paying for your Internet use by volume, this can result in extra costs. Firewalls (see below) are a useful measure for protecting computers from port scanning, although they do not provide complete protection.

Sniffer software tracks data travelling over the Internet or a corporate network. Unauthorised sniffers can compromise a network's security because they are difficult to detect and can be inserted almost anywhere. In this way, hackers can capture unsecured data travelling over a network. This data could include sensitive information such as passwords or financial documents. Again, firewalls can help to protect against unauthorised sniffers.

Methods of protection – firewalls

Firewalls are used to keep a network secure from intruders.

Firewalls are used to keep a network secure from intruders. Simple firewalls can be implemented as software only; for larger businesses, firewalls may also include dedicated hardware for faster processing. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network.

Small businesses can prevent most of the problems mentioned above with the use of software firewalls. Some are available free of charge, while others are relatively inexpensive. A good firewall will be able to detect trojans, stop entry by hackers and prevent unauthorised network access. Unfortunately, firewalls are not entirely effective in preventing port scanning.

Securing your own PC

Even without special software, there are several steps you can take to make your home or office PC more secure from outside attacks. The exact steps you will take will depend upon the type of operating system you use, but all operating systems can be made more secure with the correct settings.

Settings which you should check include:

- **File sharing.** If your PC is not connected to an office network, you don't need the file sharing features in Windows switched on. To learn how to disable these features, search for 'file sharing' in the Windows help system. This is particularly important if your PC is connected to a broadband network.
- **Browser security.** Web browsers include adjustable security settings to protect your personal information. In Internet Explorer, these can be found under the Tools – Internet Options – Security menu.

The importance of real-world security

No e-security policy can be implemented using technology alone. Two important areas to consider are physical security and personnel policy.

Having a physical security policy for IT equipment is vital for protecting confidential data. You may need to consider approaches such as:

- Ensuring your workplace IT equipment is stored in a secure and lockable location;
- Keeping up-to-date logs of all equipment;

- Taking out appropriate insurance policies and developing emergency repair plans;
- Putting extra measures in place for notebook computers (such as encrypting all data stored on them); and
- Making sure all staff are aware of security policies and report any suspicious activities.

You also need to recognise that internal staff can pose a greater security threat than external hackers, since they already have access to sensitive information. Measures you can take to minimise internal risks include:

- Making sure passwords and access systems are revoked when staff resign;
- Not giving any single member of staff complete access to all data;
- Keeping logs documenting access to key business information;
- Implementing and maintaining a strong password policy (further details on this can be found in the 'E-Security Technology Overview' at the end of this guide);
- Conducting regular internal security audits.

Conclusion

Protection against intrusions into your computer system by outsiders are an essential element of your e-security policy. A combination of suitable software (at a bare minimum, anti-virus and firewall products), along with sensible general business security policies, should ensure your business remains safe.

How to make it happen

Web addresses for some suppliers of anti-virus and firewall products are listed below. The Capability Directory of Electronic Authentication Technologies provides a fuller list of organisations that can help.

AusCERT, a single, trusted point of contact in Australia for the Internet community to deal with computer security incidents and their prevention, is a useful source of information on security threats, and provides businesses and consumers with early warnings and security alerts.

Standards Australia can supply a number of publications detailing IT security standards, which can be helpful when you are deciding on a general e-security policy. Although many of these standards were designed for large corporations, they can also be of enormous benefit to small and medium size enterprises. Standards Australia's publications offer a guide that individual organisations can pick and choose from.

Where to go online for more information

Free-Firewall.org – www.free-firewall.org

McAfee – www.mcafee.com

Internet Security Systems - www.iss.net/netice

Symantec – www.symantec.com.au

Trend Micro – www.antivirus.com

ZoneAlarm – www.zonealarm.com

Capability Directory of Electronic Authentication Technologies – <http://www.aeema.asn.au/neac>

AusCERT – www.auscert.org.au

Standards Australia – www.standards.com.au

If you are searching the Web on this topic, try the following search terms:

- antivirus (or anti-virus) software, firewall software, PC security, security policies

6. Why is privacy an important issue for e-security?



New legal requirements for privacy protection can have an impact on the way you plan for e-security. All business websites should have a well-planned privacy policy, and customer-tracking technologies must be deployed in a manner consistent with that policy. Businesses also need to keep employees informed about any Internet monitoring software in use.



The Privacy Act and e-security

As awareness of Internet privacy issues grows, businesses are also recognising the value of posting privacy policies on their websites.

On 21 December 2001 the *Privacy Amendment (Private Sector) Act 2000* came into effect. The Act increases the privacy protection enjoyed by Australians and extends the requirements for all businesses to respect privacy. As awareness of Internet privacy issues grows, businesses are also recognising the value of posting privacy policies on their websites. Ensuring respect for privacy in the online environment increases the level of consumer confidence and trust – a key aim for all e-security measures.

The new privacy legislation establishes minimum standards for the protection and handling of personal information in the private sector, and will be applied to both conventional and electronic environments. It seeks to establish a co-regulatory approach and provides legislative benchmarks to the private sector.

Under the new Act, a set of National Privacy Principles (NPPs) that describe minimum standards for the handling of personal information now apply to the private sector. These principles relate to the manner in which personal information may be collected and used, and to whom it may be disclosed. The NPPs require that businesses using personal information be open about their information practices and maintain the accuracy of the personal information.

Businesses must make reasonable efforts to keep personal information secure. They must not use government identifiers such as Tax File Numbers to identify individuals and where reasonably practicable, they must allow users to transact anonymously. Additionally, the NPPs give individuals a right to access information that is held about them and a right to correct it if it is inaccurate.

The Act permits individual organisations or industry sectors to develop their own privacy codes. The codes can vary from the NPPs but they cannot impose a lower standard than that required by the NPPs. Codes must be approved by the Australian Privacy Commissioner and must either be enforced through the Privacy Commissioner's Office or through a code adjudicator.

If you are planning to take your business online, you will need to develop a privacy policy and back it up with appropriate technology choices. For instance, using security technologies to protect online transactions will allow you to guarantee your customers that their personal data will not be intercepted by others in transmission.

Website privacy policies

Business privacy policies are not limited to online activities but consumers are coming to expect companies to include privacy policies on their websites. These will usually be fairly short and focus on what will be done with any information the consumer provides.

Many industry associations have developed specific privacy policies for member businesses. The Organisation for Economic Co-operation and Development (OECD) has developed a Privacy Policy Generator which can be used to generate a policy specific to your business needs.

The Privacy Act also controls the sending of direct marketing materials via email. Customers must be given the option of 'opting out' from direct marketing programs via email, even if they supply their email address in relation to an order or other transaction.

While every business website will need a slightly different privacy policy, a typical example would contain the following elements:

- A statement that the website will not disclose any personal information without first obtaining user approval, unless required to do so to satisfy a legal obligation;
- An outline of the circumstances under which personal data might be shared with others;
- Information on what log file information (such as the unique IP addresses of visitors to the site) is stored by the site; and
- Provisions regarding how email addresses submitted to the site will be used.

A popular technology for tracking individual behaviour online is for websites to deploy cookies.

Cookies and Web bugs

Many business websites use 'tracking' technologies to record who has visited their sites, and to allow regular customers to see content or offers specific to their needs. Such facilities can be very useful for customers, and they are often built into website hosting deals or software packages. However, customers need to be made aware that they are being tracked.

A popular technology for tracking individual behaviour online is for websites to deploy cookies. Sites that use cookies store small amounts of data in a file on the hard drives of people who visit the site. This enables the site to recognise when it has been visited before.

Cookies can be used to provide basic password authentication, allowing users to 'log in' to a site. While this can be convenient for users, it can pose a security risk, as the information is stored in unencrypted form on the visiting PC, violating one of the basic principles of password security. For this reason, cookies should not be used for commercial transactions. Instead, a system with a higher level of security, such as SSL or PKI, should be used.

Users can also choose to disable cookies on their PC. This provides a higher level of security, but may restrict the usefulness of some sites.

Web bugs perform a similar tracking function to cookies, but in a more basic way. They use small graphic images to track who has visited a page or document. Specialised software applications such as Bugnosis can be used to disable Web bugs. If your site uses Web bugs, then this needs to be disclosed in your privacy policy.

Monitoring staff online

Another issue that links privacy and e-security is the tracking of employee computer usage and Web surfing habits. Many email gateways and firewall products allow employers to track employee Internet use, or monitor emails sent to ensure that they do not contain inappropriate content. Specialised software such as WebTrends can also be used to process and analyse Internet access log files.

Businesses using this kind of technology should disclose the fact to their employees. The Office of the Federal Privacy Commissioner has developed guidelines for government departments using such technology. Although these guidelines are not compulsory for private businesses, they are recommended by the Privacy Commissioner as being good privacy practice.

Conclusion

Adopting a business privacy policy may not only be a legal requirement, it can make good business sense. For instance, it will help reassure your potential customers that their data is safe and secure. There are many resources available to assist you in developing an effective privacy policy.

How to make it happen

Further information on privacy laws, privacy policies and means for monitoring website visitors can be found at the following websites.

Where to go online for more information

The Office of the Federal Privacy Commissioner (OFPC)
OFPC Guidelines on Workplace E-mail, Web Browsing and Privacy

– www.privacy.gov.au

OECD Privacy Statement Generator –

<http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>

Bugnosis – www.bugnosis.org

Cookie Central.com – www.cookiecentral.com

Guidelines on Workplace E-mail, Web Browsing and Privacy –

www.privacy.gov.au/issues/p7_4.html WebTrends –
www.webtrends.com

If you are searching the Web on this topic, try the following search terms:

– Online privacy, privacy policy, privacy software

7. What laws apply to e-business?



The Federal Government is seeking to implement a legal and regulatory framework to increase confidence in, and certainty regarding, electronic transactions. To that end, e-business is subject to a number of specific laws and regulations that allow electronic transactions to be carried out with confidence and ensure computer crimes can be punished. However, these new rules also impose some obligations on businesses.



There are various laws and regulations that enable and regulate e-commerce in the Australian economy. In particular, the *Electronic Transactions Act 1999* and the *Privacy Amendment (Private Sector) Act 2000* have a role to play in e-security and authentication, while the *Cybercrime Act 2001* aims to penalise computer crime.

Electronic Transactions Act 1999

The *Electronic Transactions Act 1999* (ETA) creates a 'light touch' regulatory regime that enables electronic commerce in Australia and gives businesses and individuals the option of using electronic communications when dealing with government agencies. Consequently, a transaction taking place under a law of the Commonwealth is not invalid just because it was completed electronically. Since 1 July 2001 the

ETA applies to all laws of the Commonwealth unless specifically excluded by the *Electronic Transactions Regulations 2000* (as amended).

The ETA is based on two principles: *functional equivalence* (or media neutrality) and *technology neutrality*. Functional equivalence means that paper documents and electronic transactions are treated equally by the law. Technology neutrality means that the law does not discriminate between different forms of technology. This is intended to allow a certain amount of fluidity in the development of e-commerce technology without placing too high a burden on the business community to comply with particular specifications.

The ETA allows businesses to fulfil, in electronic form, any of the following requirements under a law of the Commonwealth:

- Giving information in writing;
- Providing a signature;
- Producing a document in material form; and
- Recording or retaining information.

There are various laws and regulations that enable and regulate e-commerce in the Australian economy.

The ETA also stipulates a uniform method for attributing the time and place of dispatch and receipt of electronic communications. This can be important in many transactions. Generally, a contract is taken to have been formed at the place where acceptance of the offer to transact is received. The ETA provides that receipt of an electronic communication occurs at the *place of business* of the addressee or, if the addressee does not have a physical place of business, at the addressee's ordinary place of residence. The time of receipt is the time when the electronic communication *enters an information system* designated by the addressee. If no such system has been designated, then an electronic communication is received when it comes to the attention of the addressee.

At the time of publication, all States and Territories with the exception of Western Australia have passed Electronic Transactions Acts that complement the Commonwealth's ETA. It should be noted that not all of these Acts have come into force and that unlike the ETA, state legislation applies to purely private sector transactions. This coordinated approach goes a long way toward establishing a national uniformity of laws relevant to e-commerce transactions. This legislative framework will allow businesses to enter into binding, enforceable agreements with government departments and agencies, and with other businesses, electronically.

Privacy Amendment (Private Sector) Act 2000

In December 2000, the *Privacy Amendment (Private Sector) Act* was passed through Federal Parliament. This amends the *Privacy Act 1988*, which applied primarily to public sector agencies. As a result of the amendments, which came into force on 21 December 2001, the *Privacy Act* applies to the private sector as well as the public sector. The impact of this Act on e-business is discussed in the previous section, ('Why is privacy an important issue for e-security?')

The amendments do not apply to businesses with an annual turnover of \$3 million or less, unless those businesses:

- Choose to 'opt-in' voluntarily;
- Trade in personal information;
- Provide a health service and hold health information; or
- Provide contractual services to the Commonwealth.

There are also exemptions for handling of personal information by the media, personnel records, and transfer of personal information between related parties.

Cybercrime Act 2001

Agreement has been reached between the Commonwealth and the States and Territories to implement in all jurisdictions new laws to address shortcomings in existing computer offences. The *Cybercrime Act 2001* outlaws activities such as the unauthorised access of commercial or confidential information, spreading computer viruses and trading in technology that is designed to either hack into or damage another person's computer.

Conclusion

Numerous laws have been enacted in recent years to ensure that online transactions enjoy the same legal status as their paper counterparts, and to recognise new types of computer crime. This regulations mean you can be confident in conducting business online.

Where to go online

The Office of the Federal Privacy Commissioner
The Privacy Amendment (Private Sector Act) 2000
Information Sheets
www.privacy.gov.au

The Trade Practices Act 1974
Cybercrime Act 2001
The Australian Securities and Investments Commission
Act 1989
www.law.gov.au

The Electronic Transactions Act 1999
www.law.gov.au/publications/ecommerce/pamphlet.html

8. Where can I find more information?



The following organisations can help you find more information about e-security technologies. Please note that details are current as of the time of publication but may change over time.

Australian security and privacy forums and associations



Industry and user associations

Australian Information Industry Association (AIIA)

AIIA represents the information industry in order to maximise the sector's contribution to the Australian economy.

Contact

AIIA

10-12 Campion Street (PO Box 246), Deakin, ACT 2600

Telephone: 02 6281 9444, Facsimile: 02 6285 1408

Internet: www.aiia.com.au Email: aiia@aiia.com.au

Australian Electrical and Electronic Manufacturers' Association (AEEMA)

AEEMA aims to enable the ICT, electronics and electrical manufacturing industries to prosper. AEEMA comprises all major suppliers of IT&T security products and applications, major Certification Authorities, government agencies and other major users of certification technologies.

Contact

AEEMA

1st Floor, 6 Lonsdale Street, Braddon, ACT 2612

Telephone: 02 6247 4655, Facsimile: 02 6247 9840

Internet: www.aeema.asn.au Email: webmaster@aeema.asn.au

Australian Internet Industry Association

The Internet Industry Association is Australia's national Internet industry organisation.

Members include telecommunications carriers; content creators and publishers; web developers; e-commerce traders and solutions providers; hardware vendors; systems integrators; banks, insurance underwriters; Internet law firms, ISPs; educational and training institutions; Internet research analysts; and a range of other businesses providing professional and technical support services.

Contact

IIA

Postal address:

PO Box 3986, Manuka, ACT 2603, Australia

Street address: Unit 3, 20 Bougainville Street, Manuka, ACT 2603, Australia

Telephone: +61 (02) 6232 6900

Internet: www.iaa.net.au/ Email: info@iaa.net.au

Small Enterprise Telecommunications Centre Limited (SETEL)

SETEL is a national non-profit consumer association advancing the telecommunications and e-commerce interests of Australian small business.

Contact

SETEL

PO Box 58, Jamison, ACT 2614

Telephone: 02 6251 7848, Facsimile: 02 6251 7835, Free Facsimile: 1800 622 733

Internet: www.setel.com.au Email: setel@setel.com.au

International security and privacy forums and associations

APEC e-Security (formerly Electronic Authentication) Task Group

APEC e-Security is a task group under the APEC Telecommunications working group, which proposes, implements and monitors projects and activities to advance the overall goals of APEC. Each steering group addresses a specific priority area: liberalisation; business facilitation; development cooperation and human resource development.

Contact

APEC

1-1 Juam-Dong, Kwachun, Kyunggi-Do, Korea

Telephone: (82) 2 570 4416, Facsimile: (82) 2 570 4419

Internet: www.apectelwg.org/apec/atwg/preatg.html

OECD – Working Party for Information Security and Privacy and the Committee for Information, Computer and Communications Policy

The Organisation for Economic Co-operation and Development (OECD) provides research on information security and privacy. Australia chairs the Working Party on Information Security & Privacy. For updates on global developments and various publications visit the NOIE and OECD websites.

Contact

NOIE

GPO Box 390, Canberra, ACT 2601

Telephone: 02 6271 1099, Facsimile: 02 6271 1098

Internet: www.noie.gov.au/projects/international/OECD/index.htm and www.oecd.org/dsti/sti/it/secur/

The OpenPGP Alliance

The Californian-based OpenPGP Alliance is a growing group of companies and other organisations that are implementers of the OpenPGP standard. The Alliance works to facilitate technical interoperability between OpenPGP implementations.

Contact

Phil Zimmermann, Chairman

Telephone: +1 650 347 9743

Internet: www.openpgp.org

The PKI Forum

The PKI Forum was established in 1999 to foster support for standards-based, interoperable public-key infrastructure (PKI) as a foundation for secure transactions in e-business applications.

Contact

401 Edgewater Place, Suite 600, Wakefield MS 01880, USA

Telephone: +1 781 876 8810

Internet: www.pkiforum.com Email: info@pkiforum.org

9. How do I?

//



How do I choose the best authentication system?

When authenticating the identity of staff within an organisation or visitors to a website, businesses face a number of choices. The table below summarises the main options available, how they work and their pros and cons. Remember that these are not necessarily exclusive choices; for instance, SSL technology used for securing transactions with websites is often employed in conjunction with passwords.

Technology	How it works	Pros	Cons
Password authentication	Matches user name and password to restrict access and authenticate identity	<ul style="list-style-type: none"> • Inexpensive • Well understood by users • Can be readily changed 	<ul style="list-style-type: none"> • Can be compromised by users • Does not authenticate data • Often transmitted insecurely
SSL (Secure Sockets Layer)	Creates a secure connection between Internet application and user	<ul style="list-style-type: none"> • Widely supported in Web browsers • Offers protection for all data transmitted between servers 	<ul style="list-style-type: none"> • Customers cannot choose when it is used • Relies on passwords for initial access
PGP (Pretty Good Privacy)	Uses public key cryptography; keys can be generated and authenticated by individual users.	<ul style="list-style-type: none"> • Keys provide higher levels of authentication • Supported by many software packages • Cannot be easily changed 	<ul style="list-style-type: none"> • Private keys can be compromised • Public keys required to send information
PKI (Public Key Infrastructure)	Uses public key cryptography; keys are generated by certificate authorities	<ul style="list-style-type: none"> • Keys provide higher levels of authentication • Used by governments and major companies • Cannot be easily changed • May be used with biometrics to access private keys 	<ul style="list-style-type: none"> • Issuing certificates can be costly • Businesses may require multiple certificates • Private keys can be compromised • Public keys required to send information
VPNs (Virtual Private Networks)	Create encrypted 'tunnels' between corporate networks and the Internet	<ul style="list-style-type: none"> • Give easy access to remote users • Can provide sophisticated access controls 	<ul style="list-style-type: none"> • Expensive to implement • Does not support transactions with consumers

How do I ensure my emails can't be intercepted?

While email has become a popular form of business communication, the standard email packages used by many organisations do not provide a high level of security. When an email is sent, it is normally impossible to prove who has sent it because emails are easy to intercept and can be readily faked. Email messages passing between mail servers can easily be captured or copied, making it easy for competitors and unauthorised parties to gain confidential information about your operations.

Email security products solve the problems associated with standard email by 'encrypting' the mail so it cannot be read by anyone other than the intended recipient. Cryptography is the process of putting messages into a 'secret code' so they can't be read if they are intercepted.

There are two main choices available for organisations seeking secure email:

- For businesses that require only occasional access to secure email, a free, Web-based service is a sensible choice. Getting a secure email account from these services is normally only a matter of filling out a form online. Many of them are free, but some will charge you for 'premium' services such as technical support or sending large attachments. Some free secure email providers include Groove.Net (www.groove.net), HushMail (www.hushmail.com) and LokMail (www.lokmail.com).
- If you want to use secure email encryption on a more regular basis, it can be added to your normal email software package in the form of a 'plug-in'. You can also purchase an email 'gateway' which ensures that all mail sent from within your business is secure. A list of companies which can advise you on installing such software is included below.

For electronic mail within your business or simple customer communications, secure electronic mail may not be necessary. However, if you deal regularly with confidential documents or want to take orders via email, then you should consider introducing a secure email system.

Terms you should know

Cryptography – Converting information into a secret code, using complex mathematical algorithms, so that it can't be read by anyone who does not already understand the code.

Encryption – The process of applying cryptography to an email message or document so that it can be safely transmitted over networks such as the Internet.

For electronic mail within your business or simple customer communications, secure electronic mail may not be necessary.

Where to go online for more information

Australian Projects – www.austprojects.com.au

BeTRUSTed – www.betrusted.com.au

eSign – www.esign.com.au

KPMG – www.kpmgca.com

RSA Security – www.rsasecurity.com

Secure Net- www.securenet.com.au

Telstra – www.telstra.com.au

Capability Directory of Electronic Authentication Technologies – <http://www.aeema.asn.au/neac>

If you are searching the web on this topic, try the following search terms:

– email security, cryptography, secure email

How do I make sure my digital certificates and keys are secure?

To ensure the security of online transactions, many companies make use of public key cryptography, which uses digital certificates and a pair of unique 'keys' to identify a business or individual involved in a transaction. (This is the system used by the Australian Tax Office when tax documents are submitted electronically).

Digital certificates and keys provide a strong degree of security for electronic business. However, as with any security device, they can be compromised if not protected properly. When using digital certificates, a major concern is to make sure that only the person or business they identify can access and use them.

For instance, if the key issued to a user is simply stored as part of their email program, anyone with access to their personal computer (PC) will be able to send or tamper with emails. If the machine is connected to the Internet, this might happen even if someone doesn't have physical access to the machine.

A basic method of protecting stored keys is to assign them with a password. When a user wants to sign a message, they enter the password to make the key available. However, a skilled hacker might be still able to read the key from the PC without knowing the password.

A more secure method of protecting a private key or certificate is to lock it into an electronic smart card, which can be accessed on a PC via a smart card reader. A smart card is usually password-protected as well, so that simply having possession of the card does not enable anyone to use it. This is a more costly solution, as it needs a smart card reader added to the PC.

A similar approach uses a hardware 'token' which plugs into the USB (Universal Serial Bus) port which found on most modern PCs. These tokens are compact, and can often fit on a key ring. Because most new PCs have a USB port, they also don't need a separate reader.

Terms you should know

Cryptography - Converting information into a secret code, using complex mathematical algorithms, so that it can't be read by anyone who does not already understand the code.

Encryption - The process of applying cryptography to an email message or document so that it can be safely transmitted over networks such as the Internet.

Digital certificates - An electronic file that contains information which uniquely identifies an individual or business when using online services.

Public and private keys - For maximum security, digital certificates are used in conjunction with public and private keys. When a message is encrypted, the system uses both a public key (which is freely supplied to anyone who needs to receive information from the sender) and a private key (which is known only to the sender, and ensures that messages from that sender can't be forged by others).

Digital certificates and keys provide a strong degree of security for electronic business.

How do I make sure my PC is secure?

Why is PC security important?

A survey of Australian companies found that 98% had been subject to some form of computer abuse in 2001. Taking basic safety precautions is essential to minimise the risk to your business.

Connecting PCs to the Internet allows consumers and businesses to access a wealth of information and resources. However, it also creates the risk that PCs may be tampered with by hackers, or attacked by viruses distributed via email. It is important to protect yourself against these risks.

Specialised software packages are available to protect against many of these risks. For instance, you should make sure that your PC includes an anti-virus software package and that this is updated regularly. If you have a permanent connection to the Internet, then you may also want to install a 'firewall', which stops unauthorised intruders from trying to access your PC.

Even without special software, there are several steps you can take to make your home or office PC more secure from outside attacks. The exact steps you follow will depend upon the type of operating system you use on your PC, but all operating systems can be made more secure with the correct settings.

Settings which you should check include:

- **File sharing.** File sharing allows different computers connected to a network to access each other's files. If your PC is not connected to an office network, you don't need the file sharing features in Windows switched on, and leaving them switched on may put your machine at risk of being hacked. To learn how to disable file sharing, search for 'file sharing' in the Windows help system. This is particularly important if your PC is connected to a broadband network.

- **Browser security.** Web browsers include adjustable security settings to protect your personal information while you are browsing the Internet. Setting these on the 'High' level will ensure that information remains confidential. In Internet Explorer, these can be found under the Tools – Internet Options – Security menu. For other browser software, check the Help file (which can normally be accessed by hitting the F1 or Help key).

Further details on "hardening" your system can be found at www.cert.org

Remember, if you do install additional security or computer products, such as a firewall, always change the factory settings off the default option to add an additional level of security.

Terms you should know

Viruses - Malicious pieces of computer code which make unauthorised changes to your PCs, causing them to malfunction or deleting data. They often distribute themselves via the Internet or email. Well-known recent examples include Melissa and the Love Bug. They can be prevented with anti-virus software.

Hackers - Someone who attempts to gain unauthorised access to a computer system, often for fraudulent purposes.

Firewalls - Software or hardware systems to protect PCs and networks from unauthorised access.

A survey of

Australian companies found that 98% had been subject to some form of computer abuse in 2001.

How do I make sure my passwords are appropriate and secure?

Why is PC security important?

A survey of Australian companies found that 98% had been subject to some form of computer abuse in 2001.

A survey of Australian companies found that 98% had been subject to some form of computer abuse in 2001. Taking basic safety precautions is essential to minimise the risk to your business.

Many businesses use passwords to protect their internal computer systems, and to ensure the security of customers using their websites. Passwords can be an effective mechanism against unauthorised access. However, it is important to follow a few simple guidelines to make sure they work properly, and to make all your staff aware of these rules.

To make password systems more effective, follow these guidelines:

- Passwords should not be a common or familiar name, since these can be easily guessed. Common password choices which should be avoided include first and last names, the names of relatives or pets, telephone numbers or the words 'password' or 'secret'.
- Passwords should be made up of a combination of upper and lower case letters, numbers and symbols e.g. T4iN9c#2. Ordinary dictionary words can often be cracked by experienced hackers working with large lists of words.
- Allowing users to set their own passwords makes it more likely that they will remember them. However, the rules given above should still be enforced if users are allowed to select their own passwords.

- Users should not share their passwords with anyone else. If a password is revealed to someone else, it should be changed immediately.
- All passwords should be changed on a regular basis. At least every 90 days is the recommended minimum.
- Passwords should not be stored on the computer hard drive or written down in a location at or near the computer.
- Password authentication systems should reject users after a set number of wrong passwords to minimise the risk of attack.

How do I manage my e-security when the service is outsourced?

Many small businesses choose to outsource their information technology requirements so they can concentrate on their main business objectives. This approach can be successfully extended to e-security, especially if an outside company is used to host your business website.

Outsourced e-security services are often referred to as secure managed services, and are usually provided for a fixed monthly fee. Secure managed services can also be an effective way of implementing technologies such as firewalls and anti-virus packages.

The main benefit of secure managed services is that small- and medium-sized companies do not need to invest heavily in e-security technologies or training. However, the business is still responsible for ensuring e-security is adequate. Any arrangement with a secure managed services provider should be based on a well-developed Service Level Agreement (SLA) that outlines the quality and type of service required and includes penalties for failure to deliver.

You should also make sure that you have an internal policy for overall business security, and that the secure managed services provided are consistent with these. The policies that have been developed must be clear, concise and effectively cover all relevant security issues. You should also review security policies on a regular basis, and discuss any concerns with your provider.

Staff education is also important. No matter how effective the service provided to you, it can be compromised if staff are not aware of security policies on issues such as creating and protecting passwords, sending email securely and carrying out transactions online.

Terms you should know

Outsourcing - Paying an outside company to provide services such as information technology management, rather than employing internal staff.

Firewalls - Software or hardware systems to protect PCs and networks from unauthorised access.

Viruses - Malicious pieces of computer code which make unauthorised changes to your PCs, causing them to malfunction or deleting data. They often distribute themselves via the Internet or email. Well-known recent examples include Melissa and the Love Bug. They can be prevented with anti-virus software.

Hackers - Someone who attempts to gain unauthorised access to a computer system, often for fraudulent purposes.

Many small businesses choose to outsource their information technology requirements so they can concentrate on their main business objectives.

How do I manage real world security risks?

No e-security policy can be implemented using technology alone.

While introducing appropriate software is an important consideration in electronic security, many businesses fail to consider other issues involved in protecting confidential data stored on personal computers. No e-security policy can be implemented using technology alone. Two important areas that all businesses should consider are physical security and personnel policy.

Having a physical security policy for IT equipment is vital for protecting confidential data. A good physical security policy will cover issues such as the following:

- Ensuring your workplace IT equipment is stored in a secure and lockable location;
- Keeping up-to-date logs of all equipment and when it was purchased;
- Taking out appropriate insurance policies and developing emergency repair plans;
- Keeping backups of important data in a separate, secure business location;
- Putting extra measures in place for notebook computers (such as encrypting all data stored on them); and
- Making sure all staff are aware of security policies and report any suspicious activities.

You also need to recognise that internal staff can pose a greater security threat than external hackers, since they already have access to sensitive information. Measures you can take to minimise internal risks include:

- Making sure passwords and access systems are revoked when staff resign;
- Not giving any single member of staff complete access to all data;
- Keeping to a minimum the number of staff authorised to alter or delete sensitive information;
- Keeping logs documenting access to key business information;
- Implementing and maintaining a strong password policy;
- Carefully reviewing the background of new staff before you hire them; and
- Conducting regular internal security audits.

How do I protect my company from viruses?

How common are viruses?

A recent study found that 85% of all businesses have detected viruses on their systems. The estimated cost of virus damages to businesses worldwide in 2001 was US\$13.2 billion.

A computer virus is a program or piece of code that is loaded onto a computer and is capable of attaching itself to other files and replicating itself repeatedly, usually without the user's knowledge or permission. A virus can be transmitted through an attachment to an email, by downloading infected programming from other websites, or through a floppy disk or CD.

Some viruses will activate as soon as the infected file is opened, while others will lie dormant in the computer system until activated by a trigger. The trigger could be reaching a specific date or activating a particular function (such as reading an email). While some viruses replicate themselves without causing any further damage, most will also attempt to carry out other damaging activities. This can range from sending random emails to deleting files from your PC.

The best protection against computer viruses is to use anti-virus software. By being proactive and keeping such systems up to date, you can significantly reduce the risk of your business being harmed by viruses. Anti-virus software should be installed on all your business and home PCs, and updated regularly to ensure you are protected when new viruses emerge. Most anti-virus software packages include regular free updates that you can download from the Internet. Your computer reseller will be able to advise you on available anti-virus packages.

Other steps you can take to protect against virus attacks include:

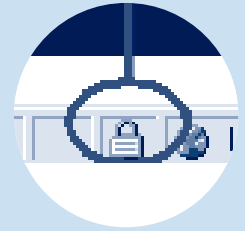
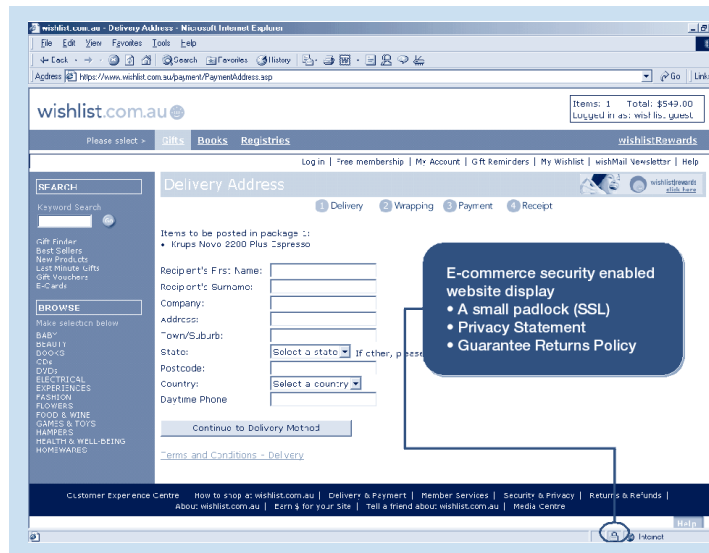
- Being cautious about opening emails from unknown sources, especially if they contain attachments;
- Only downloading software from sites and developers you trust; and
- Disconnecting your PC from the Internet when not in use.

AusCERT also provides a single, trusted point of contact in Australia for the Internet community to deal with computer security incidents and their prevention. Their aims are to reduce the probability of successful attack, to reduce the direct costs of security to organisations and lower the risk of consequential damage.

Terms you should know

Viruses - Malicious pieces of computer code which make unauthorised changes to your PCs, causing them to malfunction or deleting data. They often distribute themselves via the Internet or email. Well-known recent examples include Melissa and the Love Bug. They can be prevented with anti-virus software.

A recent study found that 85% of all businesses have detected viruses on their systems.



How do I tell if I'm completing a secure transaction?

When conducting transactions online, it is important to make sure they are carried out securely.

When conducting transactions online, it is important to make sure they are carried out securely. The most common mechanism for ensuring secure transactions on websites is Secure Sockets Layer (SSL). SSL is widely used because it is supported in all the major web browsing software packages.

To ensure that a website that is selling a product or service is using SSL, look for the small padlock in the bottom right hand corner of the Internet browser as shown in the www.wishlist.com.au example below.

When the padlock in the bottom right hand corner of the Internet browser appears on the screen, the computer has successfully established a secure connection with the website. This ensures that personal details, order details, credit card details, delivery address and contact telephone numbers are protected whilst they are sent to the online store.

Apart from the padlock, using SSL is virtually an invisible process. You will also notice that most sites using SSL have an address that begins with <https://> rather than <http://>.

Terms you should know

SSL (Secure Sockets Layer) - The most widely used security protocol on the Internet, often used for online shopping sites. SSL creates a secure channel so that data can be sent between a website and an individual PC without being intercepted by others.

How Do I Set Up a Secure Web Site?

There are a number of issues that a business needs to consider when setting up for secure e-business.

Westpac has provided the following suggestions:

- A domain name. Plain English is better than cute, and if “.com.au” has been registered by someone else, check out other suffixes such as .net. Go to www.ausregistry.com.au to check if your name is available.
- An Internet service provider (ISP) to host your domain, or website.
- If you're a medium-to-large site with more than a dozen items on sale, you need a “shopping cart” – software which tracks what is bought, calculates quantities and extras such as GST and shipping.
- A payment gateway, which encrypts the cardholder details, and takes the request for payment from your online store to the bank (card acquirer) in a secure browser session.
- Digital certificate encryption through Secure Sockets Layer (SSL), which further ensures the security of your customer's credit card details.
- An e-commerce merchant facility from a bank, which works with the gateway to handle real-time (immediate) authorisation of the credit card transaction and which will ensure the funds are placed into your nominated business account each day.
- A shipping solution, which can range from Australia Post's through to your own fleet of trucks.

Digital certificate encryption requires the installation of a digital certificate on your server, such as the VeriSign Server ID, which will allow you to enable secure communication with customers using Microsoft and Netscape browsers by making use of Secure Sockets Layer technology.

Implementing Secure Sockets Layer

To implement SSL sessions on your company web site you will need to obtain a digital certificate for your server. Digital certificates are issued by trusted third parties, called Certificate Authorities, who must authenticate the identity of your organisation before a certificate can be issued to you.

Once the certificate has been loaded into your server, you will have the ability to establish SSL sessions on your web site, providing encrypted transmission between your server and a customer's computer.

Secure Payments

Establishing a secure payment gateway on your web site will involve working with a payment gateway provider and/or your bank to establish the necessary systems to provide end-to-end encryption of customer credit card information between the customer computer, your web site and your bank's e-commerce merchant facility.

To implement SSL sessions on your company web site you will need to obtain a digital certificate for your server.

Top Ten eSecurity Tips

The following security tips have been prepared by the US-based National Cyber Security Alliance and can be found online at <http://www.staysafeonline.info/sectips.adp>

Use protection software “anti-virus software” and keep it up to date.

Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognise these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!

Don't open email from unknown sources.

A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment. Even if you do know the person sending you the email, you should exercise caution if the message is strange and unexpected, particularly if it contains unusual hyperlinks. Your friend may have accidentally sent you a virus. Such was the case with the “I Love You” virus that spread to millions of people in 2001. When in doubt, delete!

Make sure you have anti-virus software on your computer!

Use hard-to-guess passwords.

Passwords will only keep outsiders out if they are difficult to guess! Don't share your password, and don't use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places. The golden rules of passwords are: (1) A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters and numbers, e.g., xk28LP97. (2) Change passwords regularly, at least every 90 days. (3) Do not give out your password to anyone!

Protect your computer from Internet intruders – use “firewalls”.

Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorised or potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorised persons can't gain access to your computer while you're connected to the Internet. You can find firewall hardware and software at most computer stores nationwide. Don't let intruders in!

Don't share access to your computers with strangers. Learn about file sharing risks.

Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to “share files”. This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don't pay close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers!

Disconnect from the Internet when not in use.

Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet. Be safe and disconnect!

Back up your computer data.

Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Most people make weekly backups of all their important data. And make sure you have your original software start-up disks handy and available in the event your computer system files get damaged. Be prepared!

Regularly download security protection update “patches”.

Most major software companies today have to release updates and patches to their software every so often. Sometimes bugs are discovered in a program that may allow a malicious person to attack your computer. When these bugs are discovered, the software companies, or vendors, create patches that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites on a regular basis for new security patches or use the new automated patching features that some companies offer. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you. Stay informed!

Check your security on a regular basis. When you change your clocks for daylight-savings time, re-evaluate your computer security.

The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year – do it when you change the clocks for daylight-savings! Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you. Set a high bar for yourself!

Make sure your family members and/or your employees know what to do if your computer becomes infected.

It's important that everyone who uses a computer be aware of proper security practices. People should know how to update virus protection software, how to download security patches from software vendors and how to create a proper password. Make sure they know these tips too!

*You should
evaluate your
computer security
at least twice
a year*

Glossary

//



Authentication

Verifying the identity of a user logging onto a computer system or verifying the integrity of a transmitted message.

Biometrics

A security technique for checking and verifying identities that employs digitally created 'maps' of an individual's physical characteristics (eg. thumb prints, voice recordings or iris scans). These are stored by a security system and are later compared when accessed by the individual.

CA (Certification Authority)

An organisation that is responsible for the distribution of Public Key Certificates and associated private keys.

Cookies

A packet of data stored on a computer hard disk by a website, used to track visitor behaviour.

Cryptography

The mathematical process of converting information into a secret code so that it can be safely transmitted over a public network such as the Internet.

Digital certificate

A data file that is issued by a Certification Authority to an individual or organisation to identify them to online services.

Digital signature

Data included within a digital document that identifies who produced it. It can also be used to detect and track any changes that have been made to the document.

Dumping

The process of installing a phone dialler on a PC which diverts ISP connections to a high-charge number, without asking the users' permission.

Encryption

Encryption is the conversion of data into a secret code for transmission over a public network. The original (plain) text is converted into a coded equivalent called 'cipher text' via an encryption algorithm. The cipher text is decoded (decrypted) at the receiving end and turned back into plain text. The encryption algorithm uses a key, a binary number that is typically from 40 to 128 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would take to break the code. The data is encrypted, or 'locked', by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to 'unlock' the code and restore the original data.

Firewall

Firewalls are used to keep a network secure from intruders. Simple firewalls can be implemented as software only. For larger businesses, firewalls may also include dedicated hardware for faster processing. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network.

Gatekeeper

The Federal Government initiative to make all services available online in a secure fashion.

Hacker

Someone who attempts to gain unauthorised access to a computer system, often for fraudulent purposes.

IP addresses

The unique numerical addresses assigned to every computer connected to the Internet.

Log file

A file used by websites to record the date, time and IP address of each user that visits it. Log files can be analysed through software that provides the website owner with an intelligence report of the traffic, usage and areas visited within the website.

Passwords

A word or code that protects against unauthorised access to data. The word or code is entered in order to access the data.

Plug-in

An auxiliary program that works with a major software package to enhance its capability. For instance, PGP security systems can be added to email programs.

PGP (Pretty Good Privacy)

A popular form of cryptography often used to encrypt email.

Public key cryptography

A system of securing data that uses two keys to scramble and decipher messages. One key is known as a 'public key' and is widely distributed. The other is called a 'private key' and is held secretly by an individual. Messages are protected by scrambling them with the public key of the person you are sending a message to. Computer algorithms ensure that only the private key held by the person you are emailing can decrypt or unscramble the message.

Public Key Certificates

The key in public key cryptography that is kept private by an individual or organisation.

PKI (Public Key Infrastructure)

The policies and procedures that exist for establishing a secure method for exchanging information within an organisation, an industry, a nation or worldwide. It makes use of Certification Authorities (CAs), Registration Authorities (RAs) and digital signatures, as well as all of the hardware and software used to manage the process. This infrastructure, consisting of policies, legislation and facilities, creates a system of trustworthy CAs and RAs that enables e-commerce to occur with an extremely high level of confidence.

Private key

The key in public key cryptography that is kept private by an individual or organisation.

Public key

The key in public key cryptography that is openly available and is not kept private.

RA (Registration Authority)

An organisation that confirms the claimed identity of those who are applying for a digital signature.

Spoofing

The process of sending an email from a faked address.

SSL (Secure Socket Layer)

The most widely used security protocol on the Internet, often used for online shopping sites. SSL creates a secure channel over which data can be exchanged.

S/MIME

A standard for allowing emails and attachments to be sent securely.

TLS (Transport Layer Security)

An alternative name for SSL.

Viruses

Viruses are malicious pieces of computer code which make unauthorised changes to your PCs. They often distribute themselves via the Internet or email.

VPN (Virtual Private Network)

A system to allow businesses to access their internal networks and computers over the Internet or other public network, using encrypted tunnels to ensure that data cannot be accessed without authorisation.

