

How do I?



When

authenticating the identity of staff within an organisation or visitors to a website, businesses face a number of choices.

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?



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.

Email security products solve the problems associated with standard email by 'encrypting' ...

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?



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

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

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).

How do I?



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.

Connecting PCs to the Internet allows consumers and businesses to access a wealth of information and resources.

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.

How do I?



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?



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.

Outsourced

e-security services are often referred to as secure managed services, and are usually provided for a fixed monthly fee.

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.

How do I?



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

How do I manage real world security risks?

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?



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.

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

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.

How do I?



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

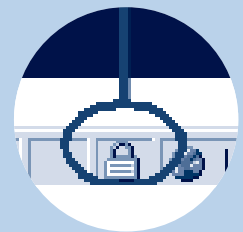
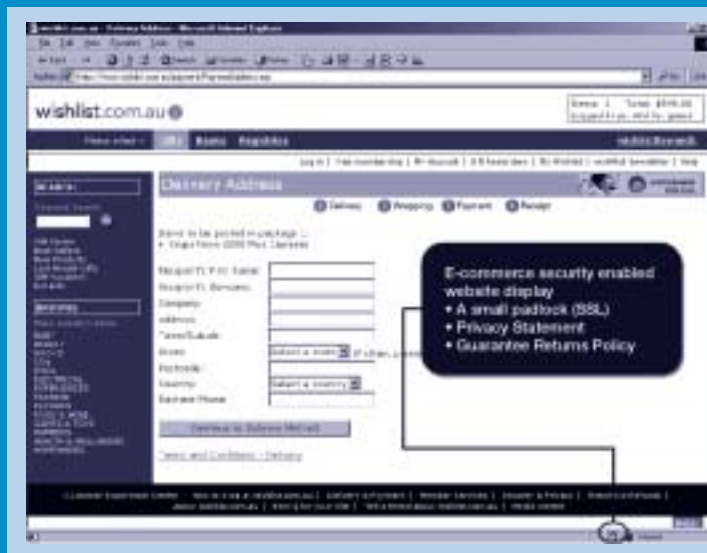
When conducting transactions online, it is important to make sure they are carried out securely.

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?



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.

eSecurity tips



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>

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

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!

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!

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!

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!

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!

eSecurity terms



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.