Privacy and security online

Privacy is the term used to describe the keeping of personal details and information confidential or secret. Privacy helps protect an individual, business or organisation from fraud and persecutory and discriminatory actions. The issue of privacy has existed for many years. Many businesses, companies and governments have collected personal details about people and entered these into databases. However, with the advent of electronic commerce, or e-commerce, many people are now concerned about 'computer privacy'.

Concerns about privacy online are centred on the ability of computer programs and applications to collect vast amounts of information electronically from users. The volume of data collected has exploded, with the creation of specific software programs and methods to collect information. This collection of information can be used to create individual user profiles which, in turn, may be used in potentially damaging ways.

Digital technologies have increased the ability of people and organisations to collect and transmit large amounts of data quickly and cheaply. IMM products can be used to gather sensitive and personal information about users and this is often done secretly through software designed to spy on the user.

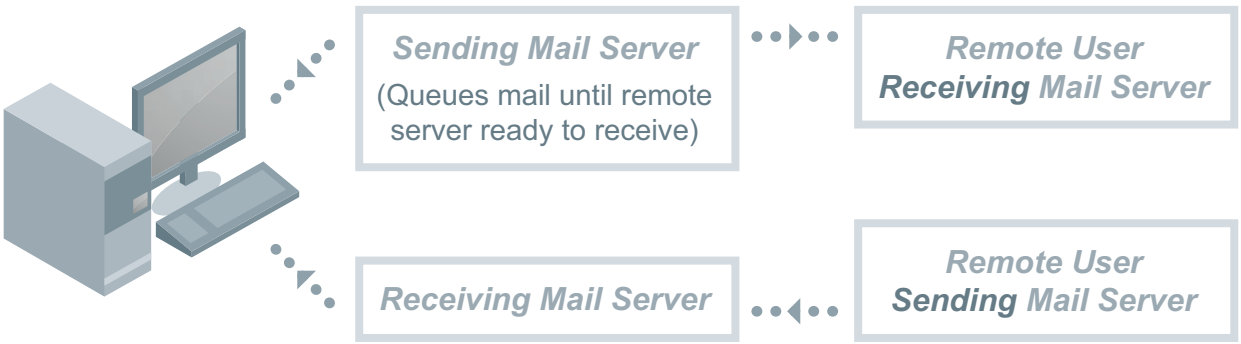
Developers can now place software programs in their products to track how a user moves through a product. This means it is possible to record the pages, buttons and functions a user activates. In the case of a website, it is possible to record how long a person stays on a single web page, which links they click and what content interests the user most. Developers can use this information to improve the functions of their product.

Cookies

Cookies are small program files that contain information about a user and are stored on a computer's hard drive. Many websites will send and share cookies with the user while they are browsing a website. These cookies can record information about the user and store it in a database for use the next time the user visits the website. Cookies can collect personal data, such as the user's name, address, email address and credit card numbers. By using the stored information, the website can improve the transmission of data (by transmitting only new information to the user's computer) and personalise the website for individual users.

Email

Email, or **e**lectronic **mail**, provides users with the capability to send almost any type of digital computer file across the Internet. Email messages are commonly sent directly between two people, using an email address. The nature of email and the way addresses are used to direct messages, lends itself to misuse. Unsolicited emails, or spam emails, are unwanted messages received in a user's mailbox. Often spam emails use computer-generated addresses that use the structure of email addresses to compose and send messages. Often spam emails are from a company attempting to sell goods or services but many are simply scanning for active email accounts. Many unsolicited emails require the user to send a reply to the sender's email address requesting that the messages stop. Unfortunately, when the user sends a reply, it indicates that the email address is, in fact, current and active. Often the result is that the user's email address gets tagged as active and is published on mailing lists, generating even more unsolicited emails. Many email programs contain features that allow a user to attempt to block spam email.



Data mining

Data mining is the practice of automatically searching large databases for patterns. To do this, data mining uses computers to build profiles of computer, Internet and ICT users to provide statistics and patterns based on the individual user's browsing and spending habits. Examples of data mining using computers to gain information include:

- companies investigating the amount of money a client has
- Tax office checking how much money people have in accounts and how much interest they gain
- An employer buying medical records to check a job applicant's health or fitness and to determine whether they are likely to need extended periods of sick leave.

The problem is that, as soon as information is stored using computers, there are always people who have access to, or the ability to read, that information.

Web history and surfing habits

When someone is surfing web pages, user information is transferred from their computer to the server where the website is located. The website collects various information about the user and the computer system they are using. This information may include the type of browser used, the location of the user's Internet service provider and computer system preferences such as language, operating system and email details. It is also possible for the user's website search history to be collected. This means that a list of the sites a user has visited and the words entered into a search engine can be read and recorded by software located on the website's server. The details can be added to a database and used to provide a list of topics, subjects and items searched by that user. This is called online profiling and the user's details are often sold, as such information can be used for effective marketing by businesses and organisations.

Concerns about online profiling include the use by companies of knowledge of a user's website browsing habits to directly contact the user in an attempt to sell them a product.

Users of websites should be aware that their surfing habits can be recorded and websites may collect personal information such as passwords, email address, credit card numbers and details of other websites visited. This information may also be sold to other organisations and added to databases.

Confidentiality

Confidentiality is a term used to describe how information about an individual is used. Confidentiality means that important personal information about an individual is kept suitably private and not widely available. Information treated confidentially is usually only accessible by a small number of people who have been trained to handle sensitive and private information. If confidentiality is breached, companies or organisations may be able to use sensitive information to judge a person and make decisions affecting them based on confidential information.

Protecting users online

Any person, business or organisation that collects, manipulates or stores information about individuals must take measures to ensure they protect the privacy of those individuals. Data is a valuable resource for most organisations. It is often very difficult, however, to put a price tag on such a resource. It is therefore very important that the security of the data within a database is maintained.

Security is a two-stage process.

The first stage is to ensure that the data within a database is secure. This is achieved through the use of passwords and encryption. These can prevent any unauthorised access to information contained within a database.

To learn more about encryption, visit the following web pages:

http://library.thinkquest.org/27158/

The second stage is user authentication. This involves only certain users having access to certain areas of a database because the information contained within it is confidential. This protects the privacy of the individuals whose information is contained within the database. The onus is on the individual or organisation keeping the information to ensure that the database is maintained accurately and data is kept confidential.

Below are some actions which can be taken to help protect users online.

1 Take action to remove or reduce the chances of accidental damage to a computer system or database. Examples include the provision and use of email filters, virus-scanning software, firewalls and proxy servers.

2 Wherever possible, control access to confidential or sensitive information by use of personal identification numbers and passwords. Software that monitors the activities of users and scans for the presence of spy-ware should be used.

3 Use only secure methods for transferring files via the Internet. Use authenticity certificates and encryption technologies whenever possible.

4 Take all necessary measures to guard against attacks from hackers and crackers. A cracker is someone who hacks a computer system with the intention to damage, steal or modify data.

To learn more about privacy online, visit the Office of the Federal Privacy Commissioner website at www.privacy.gov.au