European

Computer

Driving

Licence

IT Security

Contents

Courseware compiled by
James Cilia
2014

■ SECURITY CONCEPTS

Data & Information

Most of us use the words 'data' and 'information' to refer to the information which is handled by the computer. However, the two words have different meanings. We will explain the different meanings using the following example:

The 8-digit number 02062014 is 'data'. However, when this number is interpreted as a date, then this number has a meaning and this will be referred to as 'information'. The word 'information' is used to refer to the processed 'data'.

Data is raw, unorganized facts that needs to be processed. Data can be something random and useless until it is organized. Data may be a collection of unprocessed numbers, text or images.

When data is processed, organized, structured or presented in a given context so as to make it useful, it is called information. **Information** is the processed output of data making it meaningful to the person who receives it.

Cybercrime

Cybercrime refers to any crime that involves a computer and a network (e.g. the Internet).

Cybercrime includes anything from downloading illegal music or video files to stealing personal information from other users. Other examples of cybercrime include creating and distributing viruses. There are other types of cybercrime which will be explained later on in this module.

Hacking, Cracking & Ethical Hacking

Hacking involves gaining access to a computer or network without authorisation. Hackers are persons who use their computer expertise to break through the security levels of a computer system or network. This may involve using somebody else's password or writing a program to break another computer's security software.

From time to time, software manufacturers e.g. Microsoft and Adobe release security updates to minimise hacking of their products. Typically these security updates are available for download from the Internet. The users do not pay for these security updates.

Password cracking involves recovering passwords from data that has been stored in or transmitted by a computer system. The purpose of password cracking might be:

- to help a user recover a forgotten password;
- to gain unauthorized access to a system, or
- as a preventive measure by system/network administrators to check if their users are making use of passwords that can be easily cracked.

Software cracking involves modifying a computer program to remove or disable features such as copy protection, serial numbers, hardware keys, date checks etc. For example, cracking the trial/demo version of particular software so that this will start functioning as fully licensed software. The distribution and use of cracked copies of software is illegal.

Ethical hacking involves gaining access to a computer or network with authorisation from a company or organisation. The ethical hacker helps the company identify weak points (also known as vulnerabilities) in the security of the computer or network. The findings of the ethical hacker will help the company improve the security of the computer or network. This will minimize potential hacker attacks on the computer or network.

Threats to Data

The following represent some threats to data:

- **Force majeure** is an event or effect that cannot be reasonably anticipated or controlled by a company. For example data can be damaged or destroyed because of natural disasters (e.g. a fire, floods and earthquakes) or war.
- **Employees** may intentionally steal or damage company data such as client details or product information. They could use this data to their advantage such as selling this data to other competing companies. Employees can also accidentally lose or delete company data.
- **Service providers** involved in storing the data of companies on their servers can lose, destroy or steal valuable data. Loss of data may be intentional or accidental.
- **External individuals** can also gain access to a computer or network and steal, damage and delete the data. As indicated in the previous section these individuals are often referred to as hackers.

Protecting Personal Information

It is important that every person protects sensitive personal information like passwords, bank card details and personal identification numbers. We should take precautions against identity theft and fraud.

Identity theft occurs when someone steals the identity of another person and uses this to gain access to resources and other benefits in that person’s name. This will lead to acts of **fraud**.

Example 1: John steals the password that Mario uses to access his mailbox. John will use the password (a) to read Mario’s email and (b) to send messages from Mario’s email address.

Example 2: Maria steals Rita’s bank card details including the security code at the back of the card. Maria can use Rita’s card details to shop online.

Protecting Commercially Sensitive Information

Companies protect commercially sensitive information such as client details, data about their products and financial information.

Companies safeguard details about their clients because of data protection obligations and also to safeguard their commercial interests.

Example 1: Company A will safeguard contact details of their clients from Company B. This is because Company B may end up contacting the clients and take the business of Company A.

Example 2: Company A will safeguard details about the recipe used for a drink which they produce. Otherwise competing companies may develop a similar recipe that results in a similar drink available on the market. This will affect the business of Company A.

Encryption & Passwords

One can prevent unauthorised access to data using encryption and strong passwords.

Encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. To read encrypted data, you must have access to a secret key or password that enables you to decrypt it. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Encryption is used to safeguard confidential data:

- on portable devices such as laptops and removable storage media (e.g. USB disks).
- whilst this as being transmitted over the Internet.

Strong passwords minimise unauthorised access to data. Your password should be at least 6 characters long. It should consist of a mix of upper- and lower-case letters, one or more numbers and one or more special characters (e.g. $, @, !). Your date of birth, phone number or any word that can be found in a dictionary do not constitute a strong password. Passwords should be changed regularly. Never share or disclose your password to any other person including colleagues, family members etc. Do change your password if you suspect that somebody knows it.

Characteristics of Information Security

The policies for information security within an organisation are based on these characteristics:

- **Confidentiality** is a set of rules that limits access to information. Confidentiality prevents sensitive information from reaching the wrong people, while making sure that the right people can get it. Some methods used to ensure confidentiality include data encryption, passwords, two-factor authentication and biometric verification.

- **Integrity** is the assurance that the information is trustworthy and accurate. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed whilst being transmitted. Steps must be taken to ensure that data cannot be altered by unauthorized people. In addition, processes must be in place to detect any changes in data that might occur as a result of computer failure (e.g. server crash). Backup copies of data must be available to restore data when this is damaged, changed or lost.

- **Availability** of information refers to ensuring that authorized people are able to access the information when needed. Information is unavailable when it is lost, or when access to it is denied or delayed. For example, information on a website may not be readily available to users because the web server is over loaded by a denial-of-service attack. Measures to ensure that information is available include regular maintenance of hardware, implementing emergency backup power (e.g. uninterruptible power supply & generators), keeping off-site backup of data, providing adequate communications bandwidth, guarding against denial-of-service (DoS) attacks.

Data Protection Legislation

The ease with which computers can process, store and transfer data (including personal data) has necessitated some form of legislation to protect the privacy of individuals. Computer users dealing with personal data are required to treat this data according to the legal framework outlined in the Data Protection Act.

The Data Protection Act (2001) ensures the protection of individuals against the violation of their privacy and personal integrity by the processing of personal data.

Data controllers (users having personal data on their computer) should ensure that:

- Personal data is processed fairly and lawfully;
- Personal data is always processed in accordance with good practice;
- Personal data is only collected for specific, explicitly stated and legitimate purposes;
- Personal data is not processed for any purpose that is incompatible with that for which the information is collected;
- Personal data that is processed is adequate and relevant in relation to the purposes of the processing;
- No more personal data is processed than is necessary having regard to the purposes of the processing;
- Personal data that is processed is correct and, if necessary, up to date;
- All reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;
- Personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

Guidelines & Policies for ICT Use

Many organisations draw up guidelines and policies related to the use of IT facilities/services and to ensure the protection of data. The purpose of these guidelines and policies is to outline the acceptable and appropriate use of ICT resources within organisations. The policies provide a standard that employees/users are expected to follow. The guidelines and policies ensure that there is a clear position on how ICT should be used to ensure the protection of the organisation's data. The guidelines and policies are usually developed by the IT department of the organisation.

Social Engineering

Social engineering is the process of manipulating people to perform some action that will lead unauthorised users to break into a computer or network. This process is usually non-technical and relies heavily on human interaction and often involves tricking people to divulge confidential information e.g. passwords.

Typically social engineering is used:

- To **gather information** that may be confidential or valuable.
- To gather information to commit an act of **fraud**.
- To facilitate **unauthorised access to a computer system or network** that may reveal confidential data.

Social engineers often rely on the natural helpfulness of people who may not be aware that it is dangerous to give out sensitive information. Social engineers use methods to gain the confidence of people and trick them to release information that may be used to break into a computer or network.

Examples of social engineering include the following:

- **Phone calls** – Misleading someone about your identity in a phone call to gain valuable information.

  Example: You receive an unsolicited (unexpected) phone call from a person claiming to be an employee at the IT department of the organisation you work for. S/he informs you that urgent maintenance is needed to the organisation's network and therefore s/he requires your username and password to access the network. You provide the requested details which s/he will use to access data on the company's network.

- **Phishing** – A type of online identity theft. It uses email and fake websites that are designed to steal your personal data or information such as bank card numbers, passwords, account data, or other information.

  Example: You receive an email that appears to be sent from the bank claiming that there is a problem with your account. The email requests you to provide your credit card number and the security code at the back of the card. Typically the email will contain a link to a fake web page that seems legitimate. The fake webpage will contain the bank logos and a form which you will use to send the requested credit card details. After you respond, these credit card details will be used to make purchases.

- **Shoulder surfing** – This involves watching someone use his/her computer from "over his/her shoulder" to get sensitive information such as username and password.

  Example: You are at the cash point in the supermarket making a payment with your bank card. The persons behind you may be able to see you keying in your personal identification number. To prevent shoulder surfing, you should cover the keypad from view by using your body or cupping your hand.

Social engineering is probably the greatest threat to any security system. Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate.

Identity Theft

Identity theft occurs when someone steals your personal information and uses it without your permission. This can create serious problems.

- **Personal** – Someone may steal the username and password that you use to access a social networking site e.g. Facebook. S/he will use these details to take over your profile account and may start communicating with your friends and posting messages on your wall. These actions may harm your reputation.

- **Financial** – Someone may steal the username and password that you use to access your online shopping mall e.g. Amazon. S/he will use these details to take over your profile account. If you have saved your credit card details in the profile, s/he may be able to purchase goods and pay for these using your credit card.

- **Business** – Someone may steal the username and password that you use to access the network of the company you work for. S/he will gain access to sensitive data such as client data or company accounts etc.

- **Legal** – Someone may steal your personal details and use these to fraud a company. This may lead the company to take legal action against you.

Identity theft can occur through the following methods:

- **Information diving** – The practice of recovering sensitive information from discarded material. For example, recovering data from hard disks of computers that have been thrown away. Some people replace their computer and forget all about erasing all data from its hard disk. Another method to collect personal information is going through the garbage from businesses and homes. People may throw away dated documents e.g. bank statements in the garbage. Documents and CDs/DVDs containing sensitive information should be shredded before being thrown away. Hard-disks should have all the data erased before these are thrown away.

- **Skimming** – This involves the illegal copying of information from the magnetic strip of a credit card. This information is copied onto another blank bank card's magnetic stripe. This fake bank card may be later used to make purchases and withdraw money from the victim's bank account. Skimming occurs by using a counterfeit (fake) card reader that records all data on the bank card as it passes through it. Card skimming may occur in different places including restaurants, shops and businesses etc. where the employee will typically take the card away from the actual account holder in order to run the charge. One must also be careful when asked to swipe the bank card through more than one machine.

- **Pretexting** – This involves gaining personal information through deception. The victims are tricked into giving away information that will be used to steal their identity. For example you receive a call from a person who claims to be a bank employee. S/he informs you that there is some problem with one of your bank accounts and asks you for specific information to solve the problem. S/he will use this information for example, to claim that s/he has forgotten the account number or needs information about the account history. To protect yourself from pretexting, never provide personal, confidential, or financial information when you receive unsolicited (unexpected) calls. If the callers tell you that they are representing a company/bank you do business with, tell them that in order to protect yourself against identity theft, you will contact the company/bank yourself.

Macro Security Settings

A **macro** is a sequence of instructions that make a computer program perform a specific task. This set of instructions can be started with a single command or keyboard stroke.

A macro can also be a small program or script that automates common tasks. These scripts are usually run within programs and can often be created by the user. For example, a user might record a macro in Microsoft Word that formats tables in a specific way e.g. grey shading and double line bottom border for header rows etc.

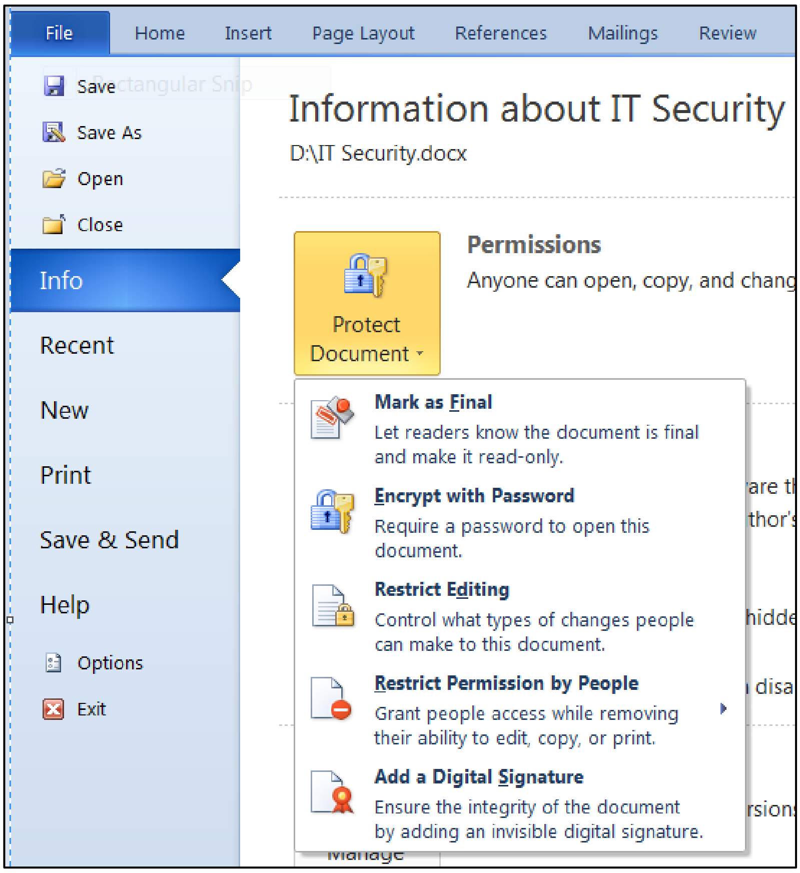
Macros are meant to make the computer experience more efficient. However, one must be careful when enabling macros written by third parties. Some macros are written with malicious intent and these will harm your computer.

Enabling a macro will ensure that the macro will run but may harm your computer if the source file is unknown. Disabling a macro will ensure the macro will run but may prevent you from using all the features in a file.

Setting Passwords for Files

To set a password for a Microsoft Word document

1. Open the document to add a password to.
2. Click the **File** tab.
3. Click **Info**.
4. Click **Protect Document**.
5. Click **Encrypt with Password**. The Encrypt Document dialog box is displayed.
6. In the Password: field type a password.



Information about IT Security

D:\IT Security.docx

Permissions

Anyone can open, copy, and chang

Mark as Final

Let readers know the document is final and make it read-only.

Encrypt with Password

Require a password to open this document.

Restrict Editing

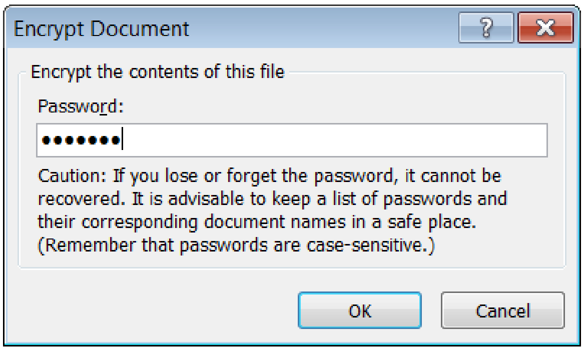
Control what types of changes people can make to this document.

Restrict Permission by People

Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature

Ensure the integrity of the document by adding an invisible digital signature.

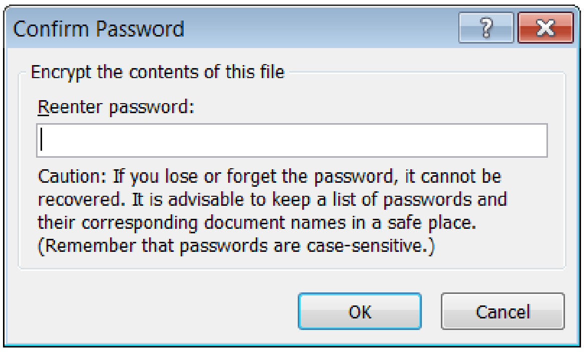


Encrypt the contents of this file

Password: •••••••

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

7. Click **OK** button. The Confirm Password dialog box is displayed.



Encrypt the contents of this file

Reenter password:

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

8. In the Reenter password: field type the same password you used in step 6 above.
9. Click **OK** button.

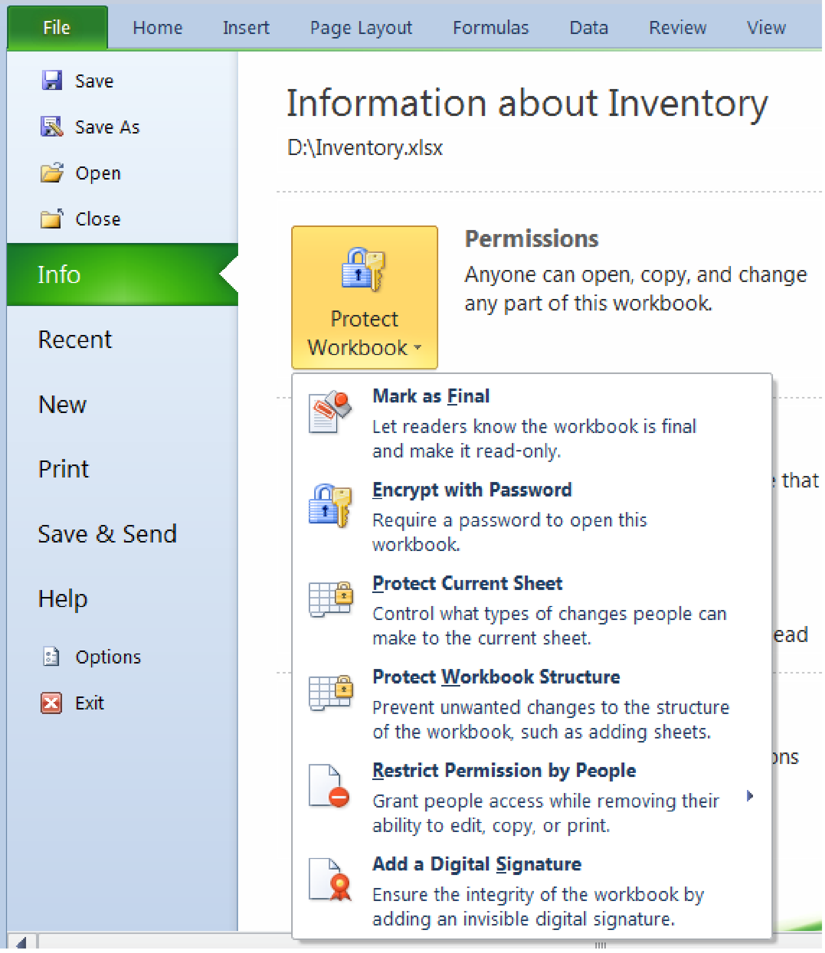
Each time you open a password locked document you will need to enter the password.

To remove the password from a MS Word document:

1. Open the password protected document. You will be prompted to enter the password to open the document.
2. Repeat steps 2 to 4 as above.
3. In the Encrypt Document dialog box, click in the password field.
4. Delete the content of the password field by pressing deleting/backspace key.
5. Click **OK** button.

To set a password for a Microsoft Excel workbook

1. Open the workbook to add a password to.
2. Click the **File** tab.
3. Click **Info**.
4. Click **Protect Workbook**.
5. Click **Encrypt with Password**.



Information about Inventory

D:\Inventory.xlsx

Permissions

Anyone can open, copy, and change any part of this workbook.

Mark as Final: Let readers know the workbook is final and make it read-only.

Encrypt with Password: Require a password to open this workbook.

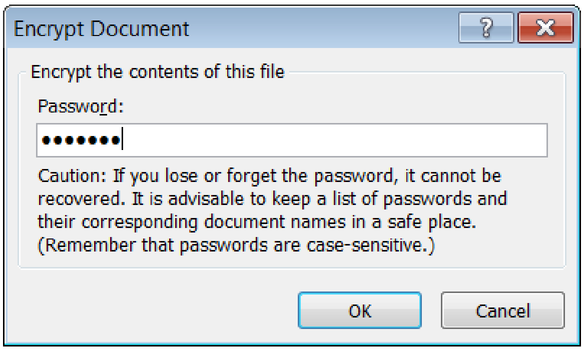
Protect Current Sheet: Control what types of changes people can make to the current sheet.

Protect Workbook Structure: Prevent unwanted changes to the structure of the workbook, such as adding sheets.

Restrict Permission by People: Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature: Ensure the integrity of the workbook by adding an invisible digital signature.

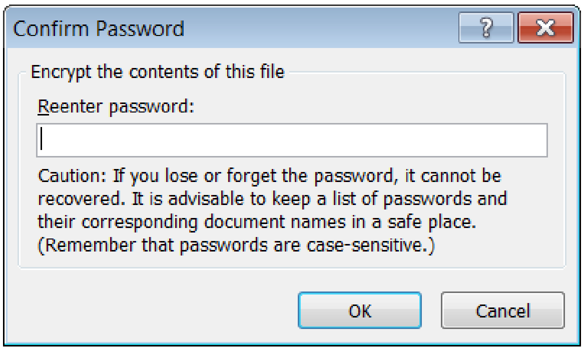
6. In the Password: field type a password.



Encrypt the contents of this file

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

7. Click **OK** button. The Confirm Password dialog box is displayed.



Encrypt the contents of this file

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

8. In the Reenter password: field type the same password you used in step 6 above.
9. Click **OK** button.

Each time you open a password locked workbook you will need to enter the password.

To remove the password from a MS Excel workbook:

1. Open the password protected workbook. You will need to enter the password to open the workbook.
2. Repeat steps 2 to 4 as above.
3. In the Encrypt Document dialog box, click in the password field.
4. Delete the content of the password field by pressing deleting/backspace key.
5. Click **OK** button.

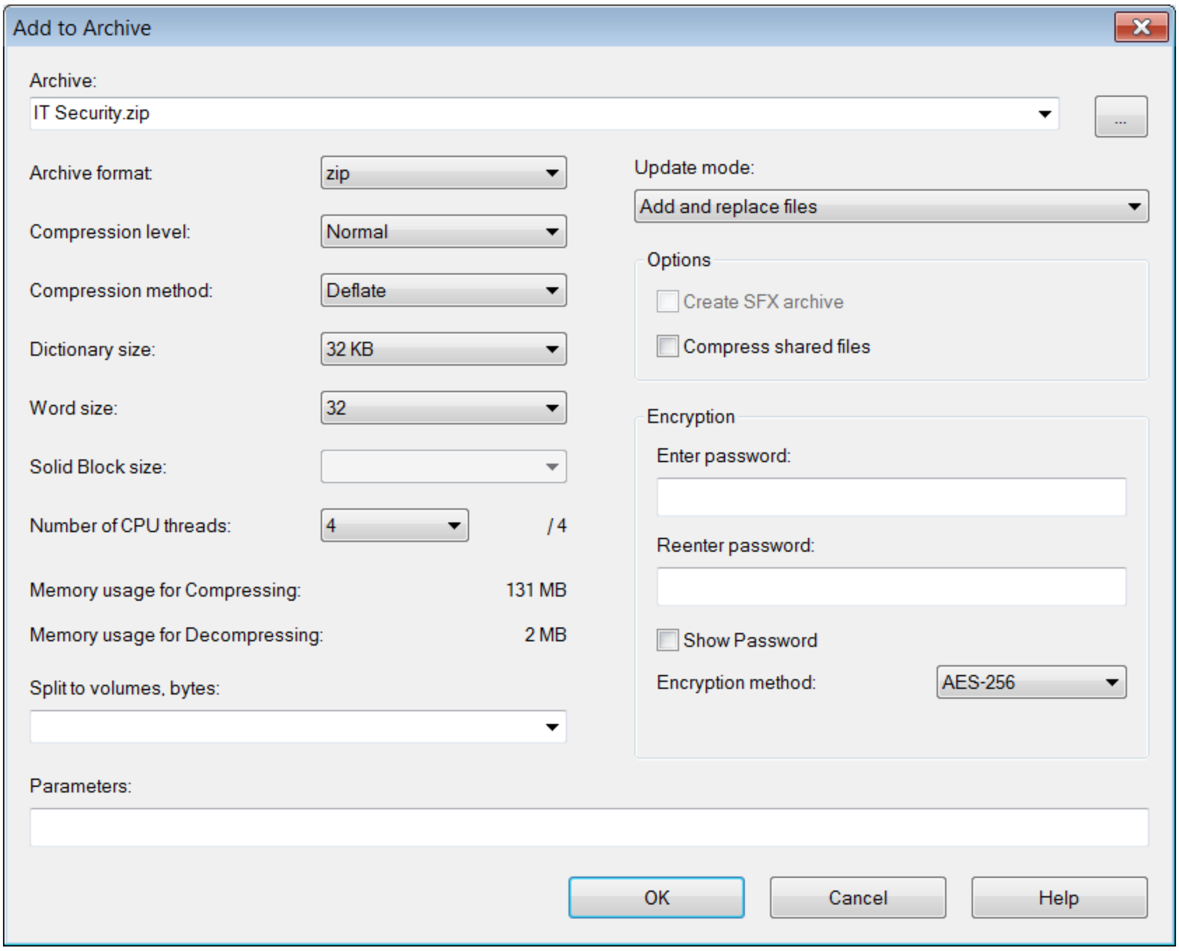
To set a password for a compressed file

MS Windows has a built-in file compression utility that can copy one or more files in an archive file (often referred to as an archive folder) that has a .zip extension. The size of the copied file/s will be smaller in the archive file.

To compress a file/s and add a password to the archive folder you will need to install another compression program such as 7-Zip which can be downloaded for free from www.7-zip.org.

1. Right-click the file you want to add to an archive folder.
2. Click **7-Zip**.
3. Click **Add to archive...** The Add to Archive dialog box will be displayed.
4. In the Archive: field, type in a name for the encrypted file you are creating.
5. Set Archive format: to zip.

6. Change Encryption method: to AES-256.
7. In the Enter password: field type in a password.
8. In the Reenter password: field type the same password as for step 7.
9. Click **OK** button.



Add to Archive

Archive: IT Security.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 4 / 4

Memory usage for Compressing: 131 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

When you try to extract the files from your archive, or to open them from within, you will be prompted to enter your password.

Advantages & Limitations of Encryption

As indicated in an earlier section encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. To read encrypted data, you must have access to a secret key or password that enables you to decrypt it.

The advantages of encryption include:

- Encrypted data cannot be read without the secret code or password. Therefore encrypted data is protected from unauthorised access.
- If a computer/laptop is stolen the encrypted data will remain secure and unreadable.

One limitation of encryption is the inability to access data if the secret code or password is lost.

MALWARE

Definition & Types of Malware

Malware is malicious software designed to install itself on a computer without the owner’s consent. It is a computer program that secretly enters and damages a computer system.

Malware includes:

- **Trojan** secretly places illegal, destructive instructions in the middle of a computer program. Once the program is run, the Trojan becomes active. Trojans can delete, block, modify or copy data. They can also disrupt the performance of a computer or a network. Trojans typically enter a computer system attached to a free game or other utility. Unlike viruses, Trojans do not replicate themselves.

- **Rootkit** is another type of malware that is activated each time a computer system boots (loads) up. Rootkits are difficult to detect because they are activated before the operating system (e.g. MS Windows) has completely booted up. A rootkit often allows the installation of hidden files, hidden processes and hidden user accounts in the operating system of a computer.

- **Back door** is a secret way to access a computer without passing security mechanisms. Back doors are built into a software by the original programmer, who can gain access to the computer by entering a code locally or remotely. Typically programmers install a back door so that they can access a program for troubleshooting purposes. However, hackers often use back doors that they detect or install themselves to enter a computer system.

Other types of infectious malware include:

- **Virus** attaches itself to a program or file and spreads from one computer to another, leaving infections as it travels. Almost all viruses are attached to an executable (.exe) file, which means that a virus may exist on a computer but it actually cannot infect a computer unless the user runs or opens the malicious program. A virus cannot be spread without human action. Viruses are usually spread by sharing infected files as email attachments or downloaded from websites.

- **Worm** is a type of malware that self-replicates and distributes copies of itself in a computer network. Worms spread from computer to computer, but unlike viruses, worms are able to infect computer systems without intervention from computer users. For example, a worm can send copies of itself to all contacts in an email address book. The worm replicates again and sends itself out to everyone listed in each of the receiver's address. Typically worms slow down computer systems and networks.

Other types of malware include:

- **Adware** is a software application that automatically displays advertising banners while the program is running. The programmers of these software applications include additional code that displays advertisements in pop-up windows or in a bar on the computer screen. These advertisements sponsor the development and free use of the software applications (freeware). The advertisements disappear when users stop running the freeware software. Some freeware applications may contain adware which tracks the Internet surfing habits of users and pass this on to third parties, without the user's authorization or knowledge. The users will then receive other advertisements that are targeted to their Internet browsing habits etc. When the adware becomes intrusive like this it is considered as spyware.

- **Spyware** is a program that secretly installs itself on computers and collects information about users without their knowledge. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited. They can also interfere with user control of the computer in other ways, such as installing additional software and redirecting web browser activity. Spyware changes the computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs.

- **Botnet** is a group of computers connected together for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers used to transmit malware or spam, or to launch attacks. Botnet attacks slow down a computer network or a website.

- **Keystroke logging** is a program that allows the user to monitor what another user types into a device. It involves recording consecutive key strokes on a keyboard. Sensitive information such as usernames and passwords that are keyed in the computer may be stolen through such programs.

- **Dialer** is a program that causes the computer to dial premium (high rate) telephone numbers without the user’s knowledge or consent. This will result in high telephone bills. This is possible only if users are using a dial-up modem.

Using Antivirus Software

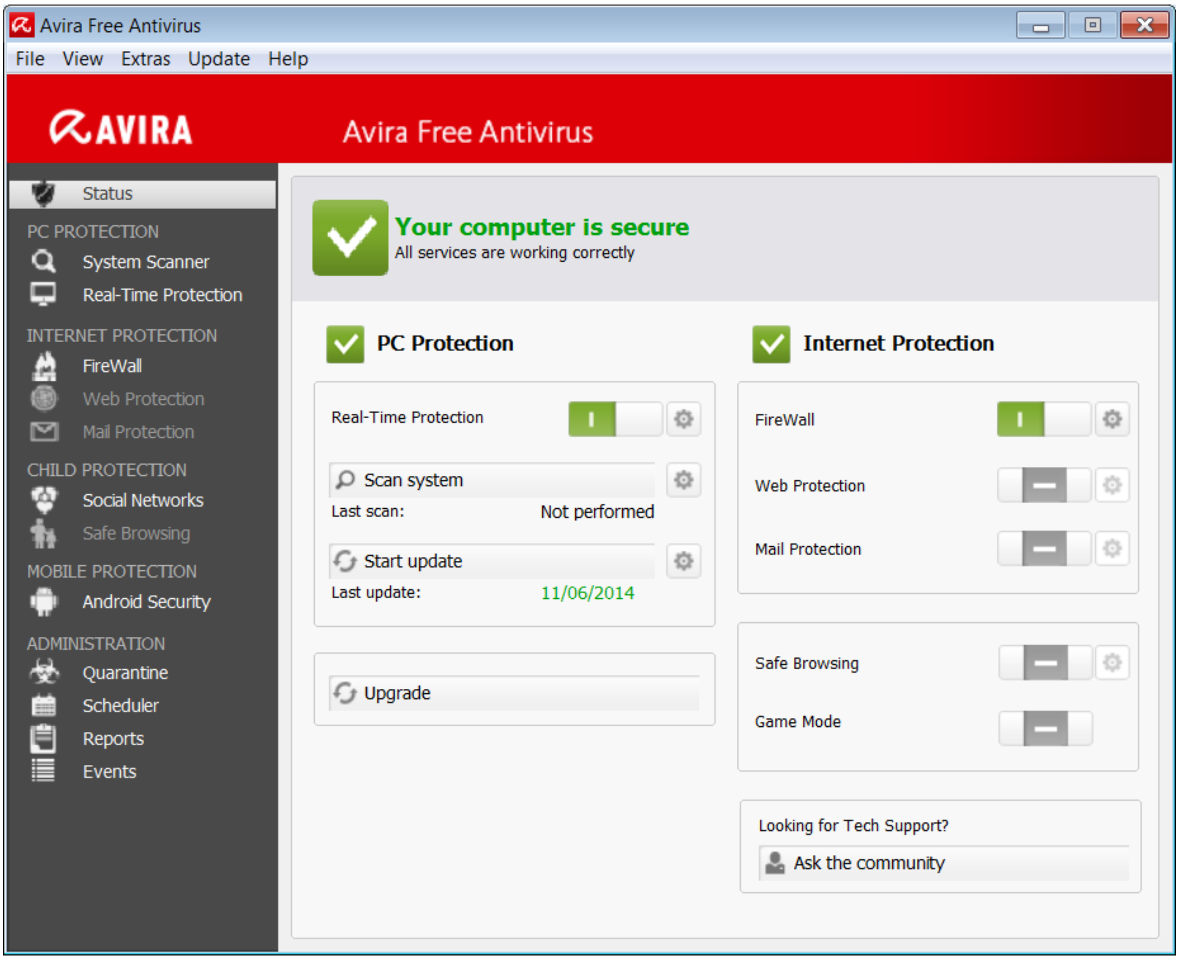
Anti-virus software is a program which protects the computer system against most viruses. Typically, such programs detect the presence of viruses in a computer and in most cases remove (or disinfect) any files infected by viruses.

Unfortunately, new viruses are being developed all the time. Thus, if the anti-virus program is not updated on a regular basis it will not be able to detect new virus types and variants. When you install an update, new entries are added to the software's virus definitions database so that suspect files can be recognised and dealt with. Most anti-virus programs are updated automatically when the computer connects to Internet.

Different users may have different anti-virus programs. Home users can download free antivirus programs e.g. Avira (www.avira.com). The following instructions assume that you have Avira anti-virus installed on your computer.

To scan specific drives, folders, and files for viruses using Avira antivirus:

1. Click **Start** button.
2. Highlight **All Programs**.
3. Click **Start Avira Free Antivirus**. The following window will be displayed.



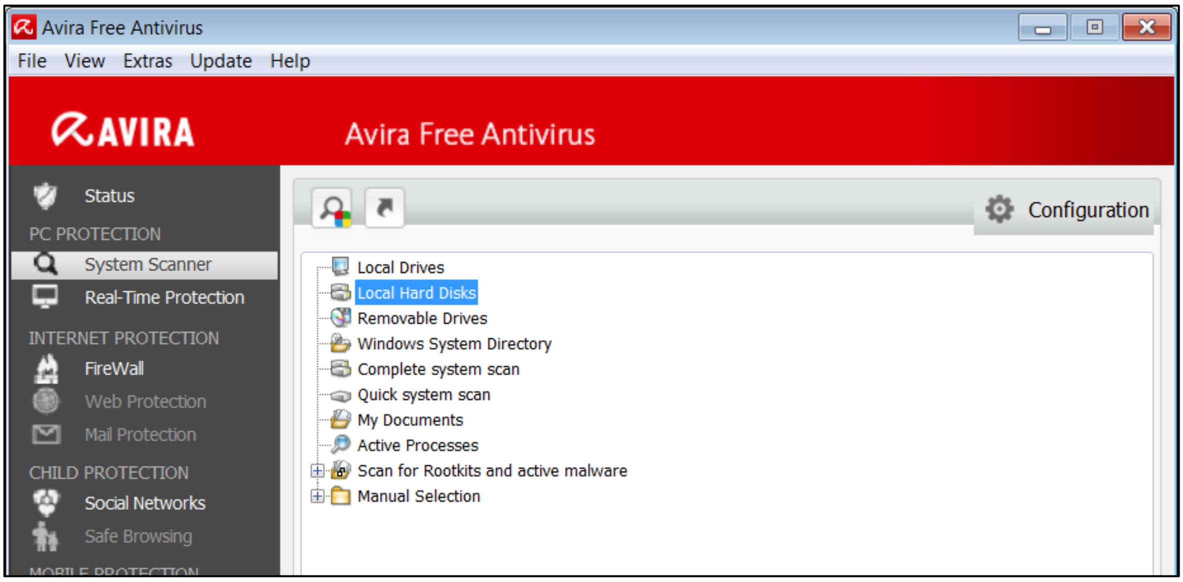
Your computer is secure
All services are working correctly

Last scan: Not performed

Last update: 11/06/2014

Looking for Tech Support?

4. Click **System Scanner** (top left). The following window will be displayed.



5. Select the appropriate scanning option e.g. **Local Hard Disks** or **Removable Drives** (for USB pen disks).
6. Click **Start scan** button.
7. Follow any other steps.

Quarantining Infected Files

A **quarantine** is the process of moving an infected file, such as a virus, into an area where it cannot cause harm. It is the process of isolating a file suspected of being infected with a virus to a specific area of a storage device in order to prevent it from contaminating other files. The file can still be restored from quarantine if required.

The quarantine process is used when the anti-virus software detects a problem and is unable to eliminate it or when it is unsure whether or not the file is a known virus. If the user suspects that a file is infected but the virus is not detected by the software, s/he can enable the quarantine manually.

■ NETWORK SECURITY

Definition & Types of Network

Millions of computers are connected together to form computer networks. These networks facilitate the communication of data between computers and sharing of resources.

A **network** consists of two or more computer systems and other peripherals (printers, scanners etc.) linked together.

The advantages of a computer network include:

1. **Sharing of peripheral devices** – Networking enables two or more users to share laser printers, scanners, modems etc. Typically, several computer users in the same office are served by a single printer. This is cost effective for organisations with many computer users.

2. **Sharing of programs** – Networking enables several computer users to share the same programs. In most organisations, people make use of the same software. Rather than purchasing individual software packages for each computer user, organisations purchase network versions of the program.

3. **Sharing of data** – Networking enables several computer users to share data. Thus individual users can work on the same data at the same time. Depending on the configuration of the network, users work on real time updated data.

4. **Efficient communication** – Networking enables efficient exchange of messages and documents between several computer users. Networking eliminates the typical delays encountered with standard inter-office mail delivery or telephone calls.

Common types of networks include:

1. **Local-Area Network (LAN)** is a computer network located in a single building or in nearby buildings e.g. a school, a department, or a number of offices. Typically the computers are connected by copper cables.

2. **Wide-Area Network (WAN)** is a network which serves computers located at far away distances - across towns and countries. Communication between the various computers is usually carried out via telephone lines, fibre-optic links, radio link, satellite etc.

3. **Virtual Private Network (VPN)** is a private network that is built over a public infrastructure typically the Internet. A VPN is similar to a WAN in that it enables users to connect to a private network that may be located at far away distances, however VPN uses the Internet for such connections. Several companies enable their employees to connect to the company’s private network (LAN) from their homes via VPN connections. Employees will be able to access data and other resources securely on the company’s network as if they are at the office.

The Network Administrator

A **network (or system) administrator** manages an organization's network. S/he keeps the computer network operational and monitors the functions and operations within the network. The network administrator is responsible for installing, maintaining and upgrading the software or hardware required to efficiently run a computer network.

Network administrators, particularly in large companies are not usually involved in direct user support like helpdesk duties. Instead, they engage in high-level technological support, such as maintaining network hardware and software equipment, and monitoring equipment to ensure overall network operations. Network addresses are often assigned through the network administrator. In addition, the network administrator configures the authorization and authentication of employees that require access to data and resources on the network. S/he provides employees with usernames and passwords to access the network. The network administrator ensures that network usage is in line with the ICT policy of the company.

Firewall

A **firewall** is a system designed to prevent unauthorized access to or from a private network (LAN). Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized users from accessing a LAN connected to the Internet. All messages entering or leaving the LAN pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

The limitations of firewalls include:

- Firewalls are ineffective if employees disclose their usernames and passwords to other people.
- Firewalls cannot stop internal users from accessing websites with malicious code.
- Firewalls can restrict employees from performing legitimate operations. These restrictions can slow down the work of employees.

Wired & Wireless Connections

Computers can be connected to a network using either wired or wireless technology.

- A **wired** network is when a computer is connected to a network using a physical cable also known as an Ethernet cable. Wired connections are reliable and faster in terms of data transmission compared to wireless connections. There is less risk of others being able to access your broadband connection. Wired technology is not suitable to connect tablets and smartphones.

- A **wireless** or **Wi-Fi** (wireless fidelity) network is when a computer is connected to a network without the need for cables. Wireless networks enable you to connect a variety of devices including laptops, tablets and smartphones. Data transmission tends to be slower compared to wired connections. Also thick walls and electrical interference affect wireless connections. Unsecure wireless connections enable others to access your broadband connection.

When connecting to a network keep in mind the following security implications:

- Computers connected to a network may be infected with malware.
- Connecting to a network may expose your computer to unauthorised data access.
- Connecting to a network may increase the challenge of maintaining privacy.

Wireless Security

Wireless networks can be protected/secure or open. A secure wireless connection requires users to enter a network security key. This ensures that only authorised users can access the network and data.

Whenever possible, you should connect to security-enabled (protected) wireless networks. If you do connect to an open network, be aware that someone with the right tools can see everything that you do, including the websites you visit, the documents you work on, and the user names and passwords that you use. Eavesdropping involves someone secretly monitoring the actions of another user on the computer.

Wireless networks can be secured by implementing encryption. This protects the data that is travelling over the network and prevents unauthorised access to data residing on the computer network. Several types of wireless network encryption are available:

- **Wired Equivalent Privacy (WEP)** is the oldest and least secure wireless network encryption. This is used for hardware (routers) that do not support Wi-Fi Protected Access.

- **Wi-Fi Protected Access (WPA/WPA2)** is a security standard to secure computers connected to a Wi-Fi network. WPA/WPA2 is more secure than the WEP.

Network encryption is set through the router’s/modem’s admin interface. This will generate a network encryption key that will be used by each computer to connect to the wireless network.

In addition to the network encryption key one can also implement MAC address filtering to restrict specific computers to connect to the network.

A **MAC (Media Access Control) address**, sometimes referred to as a hardware address or physical address, is an identifcation code that is assigned to any computer or device (including printers) that has built-in networking capability. The MAC address is "burned into" a given device from the factory having the following format: six pairs of hexadecimal digits separated by colons e.g. 01:1F:33:69:BC:14. Hexadecimal digits can include only the numbers 0-9 and letters A-F.

Connecting to a Protected/Unprotected Wireless Network

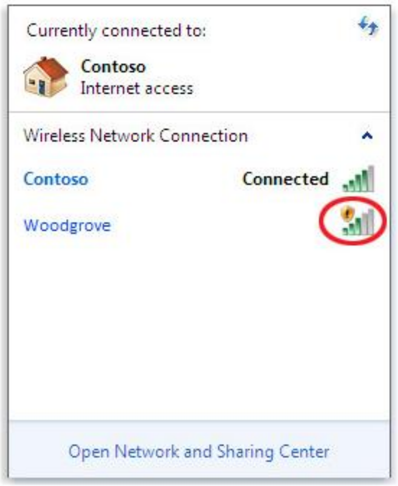
If you have a laptop, tablet or smartphone, you can see a list of available wireless networks, and then connect to one of those networks, no matter where you are.

To view the available wireless networks on a computer running MS Windows:

- Open **Connect to a Network** by clicking the network icon 📶 or 🖥 in the notification area. A pop up menu will display the list of available wireless networks.

Note that:

- Wireless networks appear only if your laptop has a wireless network adapter and driver installed and the adapter is enabled.



Currently connected to:

Contoso
Internet access

Wireless Network Connection

Contoso Connected

Woodgrove

Open Network and Sharing Center

Connect to a Network, showing the shield icon on an unsecured network

To connect to a wireless network:

1. Open **Connect to a Network** by clicking the network icon 📶 or 🖥 in the notification area.
2. In the list of available wireless networks, click a network.
3. Click **Connect** button**.**

Note that:

- The first time you connect to a protected wireless network, you will need to enter the network security key.

Accessing a Network

As indicated earlier, the network administrator provides employees with an individual account that will enable them to access the LAN of the company. Each account consists of a unique username and a password. The employees are required to change their password the first time they access the network. Network accounts ensure that only authorised users can access the computer network.

Users should ensure that they set strong passwords for their network account. A strong password should be at least 6 characters long. It should consist of a mix of upper- and lower-case letters, one or more numbers and one or more special characters e.g. T3!mz*2. Date of births, phone numbers or any word that can be found in a dictionary should be avoided. Passwords should be changed regularly.

Passwords should not be disclosed or shared with any other person including colleagues, family members etc. Users should change their password if they suspect that somebody knows it.

Biometric Security

Biometric security is a security mechanism that uses information about the physical characteristics of a person to verify the person’s identity and then provides access to a computer network. Biometric security relies on specific data about unique biological traits of people.

Biometric security systems store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition. The individual's body characteristics are pre-stored in a biometric security system. When individuals walk into a facility or try to gain access to a system, the biometric scanner evaluates their physical characteristics, which are matched with stored records. If a match is located, the individuals are granted access.

■ SECURE WEB USE

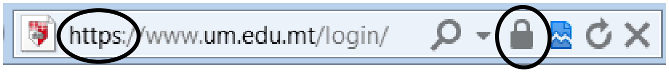
Secure Websites

Internet users are often concerned about online purchases. Normally payments for online purchases are made by a bank card. Before you submit your credit card you should be aware of the following:

- Information travelling between your computer and a server can be routed through many computer systems.
- Any one of these computer systems can capture and misuse your information. Each of these computers can eavesdrop and make copies of your information.
- An intermediary computer could even deceive you and exchange information with you by representing itself as your intended destination.

If you decide to shop or do banking on the Internet, protect yourself by dealing with secure sites. You must ensure that your credit card details are only entered in secure websites. Web browsers (e.g. MS Internet Explorer and Chrome) display security warnings when you are about to enter a secure site. You can tell when you have a secure connection by looking at the URL.

The URL of a secure website starts with "**https://**" not "http://". The browser will also show the **padlock** symbol:



When you try to access a secure website, the Internet browser prompts you to enter your username and a password. The website will be displayed if the correct username and password are entered.

A **secure (protected) website** is a site that can only display its content if the user types in a username and a password. Many organisations restrict access to sections of their websites.

Be cautious with email messages asking you to send your username and password. Reputable organisations will never ask for these details and other personal information (e.g. financial details) to be sent by email or phone.

It is important to sign out/log off and close all browser windows when you are done with your online shopping, e-banking etc.

Pharming

As indicated in an earlier section pharming involves stealing personal information from users. Phishing attempts to capture personal information by getting users to visit a fake website whilst pharming redirects users to false websites without them even knowing it. How does this happen?

We use domain names to access websites e.g. www.bov.com. A Domain Name Server (DNS) will automatically translate the domain name to an Internet Protocol (IP) address in this case to http://80.85.110.241. The Web browser then connects to the server at this IP address and loads the web page data. After a user visits a certain website, the DNS entry for that site is often stored on the user's computer in a DNS cache. This way, the computer does not have to keep accessing a DNS server whenever the user visits the website.

Pharming occurs when the victim opens an email virus that "poisons" the user's local DNS cache. It does this by modifying the DNS entries, or host files. For example, instead of having the IP address 80.85.110.241 direct to www.bov.com, it may direct to another website determined by the hacker. Pharmers can also poison entire DNS servers, which means any user that uses the affected DNS server will be redirected to the wrong website. Fortunately, most DNS servers have security features to protect them against such attacks.

Digital Certificates & One-Time Password

A **digital certificate** verifies the authenticity and legitimacy of a website. A web browser may display an unsafe digital certificate alert but still permit user entry. This warning signal indicates that the website is a threat and security risk.

A secure website has a digital certificate confirming that it is secure and genuine. It ensures that no other website can assume the identity of the original secure site. When you are sending personal information over the Internet, you should check the certificate of the website you are using to ensure that it will protect your personally identifiable information.

Digital certificates are issued by a certificate authority. When you visit a secure website, the site automatically sends you its digital certificate. Digital certificates are used, for example, by organisations involved in online monetary transactions. The certificates ensure that bank card details will not be intercepted as these travel from the buyer’s computer to the web server. Digital certificates can be viewed by double-clicking on the padlock icon in the web browser.

A **one-time password** is type of password that is valid for only one use. It is a secure way to provide access to an application or perform a transaction only one time. The password becomes invalid after it has been used and cannot be used again.

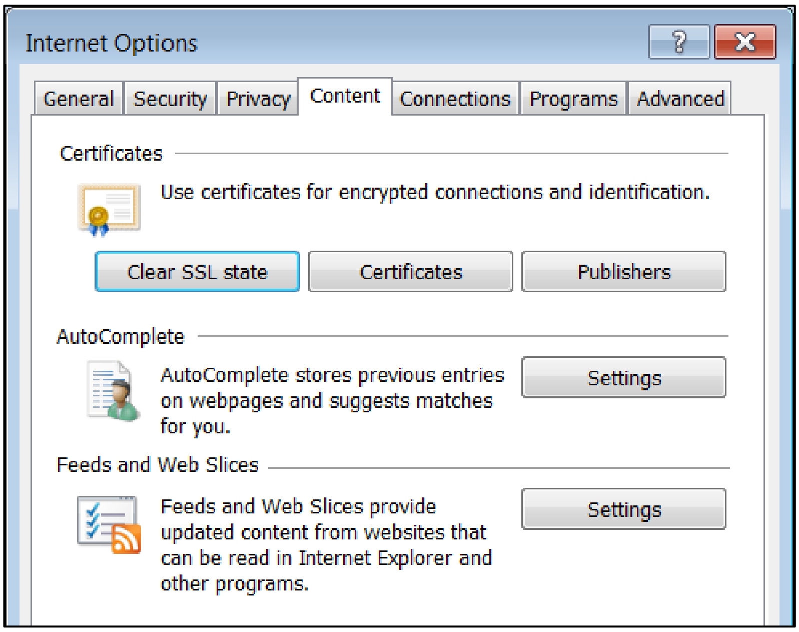
Enabling or Disabling AutoComplete

If you do tasks online that require entering personal information e.g. shipping and billing addresses on websites, the AutoComplete feature in MS Internet Explorer can save you time by filling out forms automatically. The next time you visit a website with a form and start entering your information, MS Internet Explorer will automatically fill out the form based on what you have previously entered.

AutoComplete saves you time by remembering information you enter into forms online. Since this information is securely stored on the computer you are using at the time, you should be careful about using AutoComplete on public or shared computers. When you are using a public or shared computer, make sure AutoComplete is turned off.

To enable/disable AutoComplete in MS Internet Explorer:

1. In MS Internet Explorer, click the **Tools** button on the right side of the Command bar. A menu will be displayed.
2. Click **Internet options**. The Internet Options dialog box is displayed.
3. Click the **Content** tab.

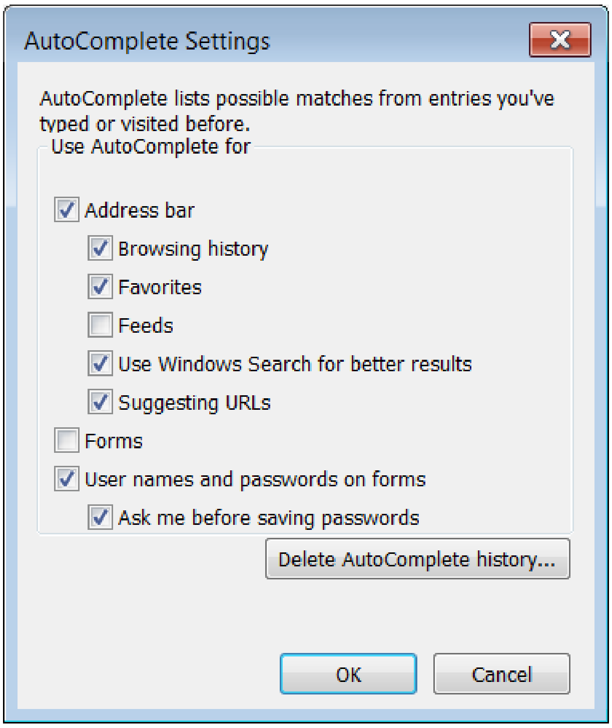


Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

4. Click **Settings** button in the AutoComplete section. The AutoComplete Settings dialog box is displayed.



AutoComplete lists possible matches from entries you've typed or visited before.

Use AutoComplete for

☑ Address bar
- ☑ Browsing history
- ☑ Favorites
- ☐ Feeds
- ☑ Use Windows Search for better results
- ☑ Suggesting URLs

☐ Forms

☑ User names and passwords on forms
- ☑ Ask me before saving passwords

5. To enable AutoComplete when filling forms tick the **Forms** checkbox. To disable automatic filling of forms untick the **Forms** checkbox.
6. Click **OK** button to close the AutoComplete Settings dialog box.
7. Click **OK** button to close the Internet Options dialog box.

Enabling or Disabling Autosaving

Autosaving saves you time by remembering username and passwords and other information you enter into forms online. This can be helpful if you enter your username and password regularly. However, this can also be a security risk if that computer is used or accessible by other users.

To enable/disable autosaving in Microsoft Internet Explorer:

1. Repeat steps 1 to 4 as for enabling/disabling AutoComplete.
2. In the AutoComplete Settings dialog box, tick the **User names and passwords on form** checkbox. To disable automatic saving of usernames and passwords untick the **User names and passwords on form** checkbox.
3. Click **OK** button to close the AutoComplete Settings dialog box.
4. Click **OK** button to close the Internet Options dialog box.

Cookies

Cookies are text files that save information regarding particular websites. They may save information, shopping cart contents, or user preferences.

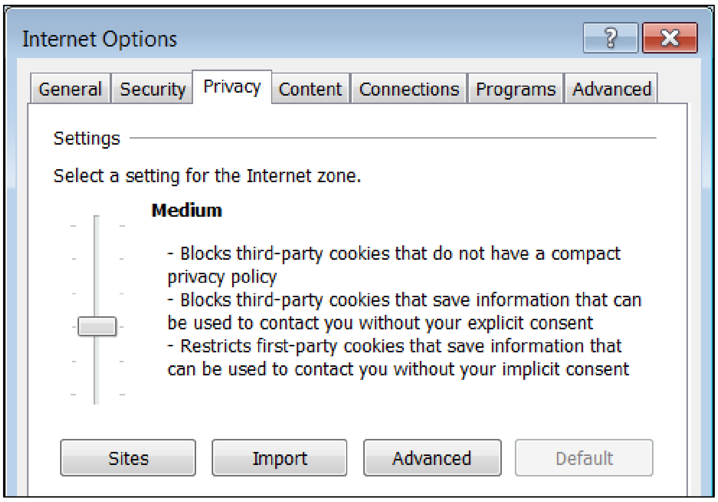
When a web browser requests a web page from a web server, the latter may store a piece of text on the user's computer. The text is sent back to the server each time the browser requests a page from that server.

The main purpose of cookies is to identify users and possibly prepare customised web pages for them. When you enter a website using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your browser which stores it for later use. The next time you go to the same website, your browser will send the cookie to the web server. The server can use this information to present you with custom web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it.

Many websites require that you enable cookies in order for the website to be properly viewed. To enable cookies:

1. In MS Internet Explorer, click the **Tools** button on the right side of the Command bar. A menu will be displayed.
2. Click **Internet options**. The Internet Options dialog box is displayed.
3. Click the **Privacy** tab.
4. Set the slider to **Medium**. This should be enough to enable cookies.

   If you want to enable cookies for a particular site, click **Sites** button. In Address of website: field type the URL. Click **Allow** button to enable cookies for that site.

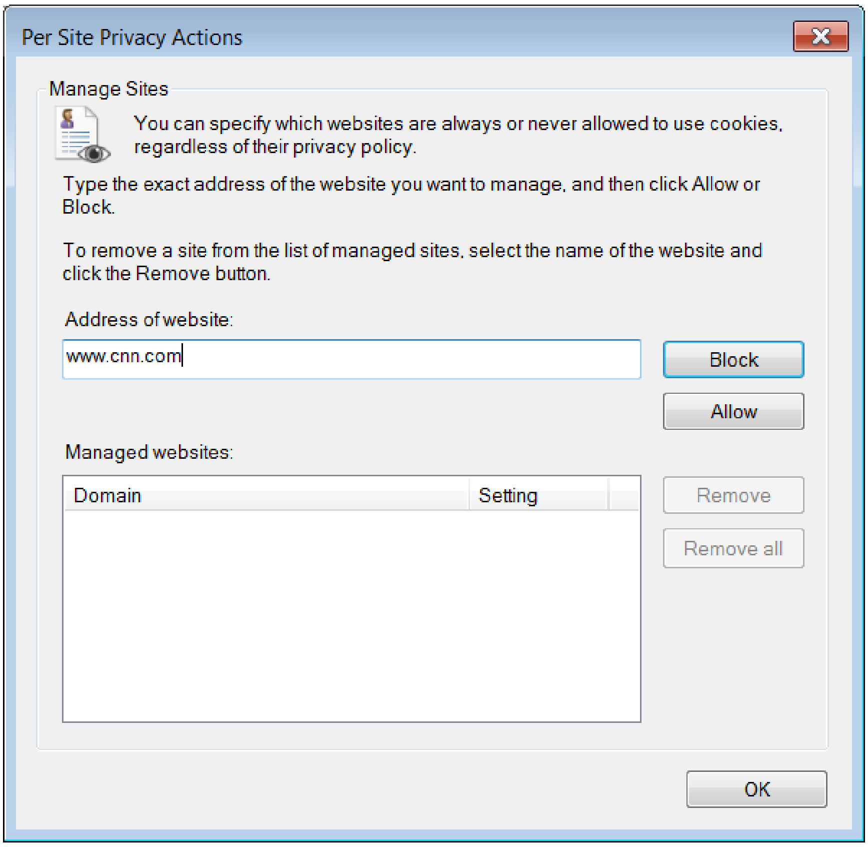


Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

5. Click **OK** button to close the Per Site Privacy Actions dialog box.
6. Click **OK** button to close the Internet Options dialog box.



You can specify which websites are always or never allowed to use cookies, regardless of their privacy policy.

Type the exact address of the website you want to manage, and then click Allow or Block.

To remove a site from the list of managed sites, select the name of the website and click the Remove button.

Address of website: www.cnn.com

Managed websites:

To block cookies for a site:

1. Repeat steps 1-4 as above.
2. If you want to block cookies for a particular site, click **Sites** button. In Address of website: field type the URL. Click **Block** button.
3. Repeat steps 5-6 as above.

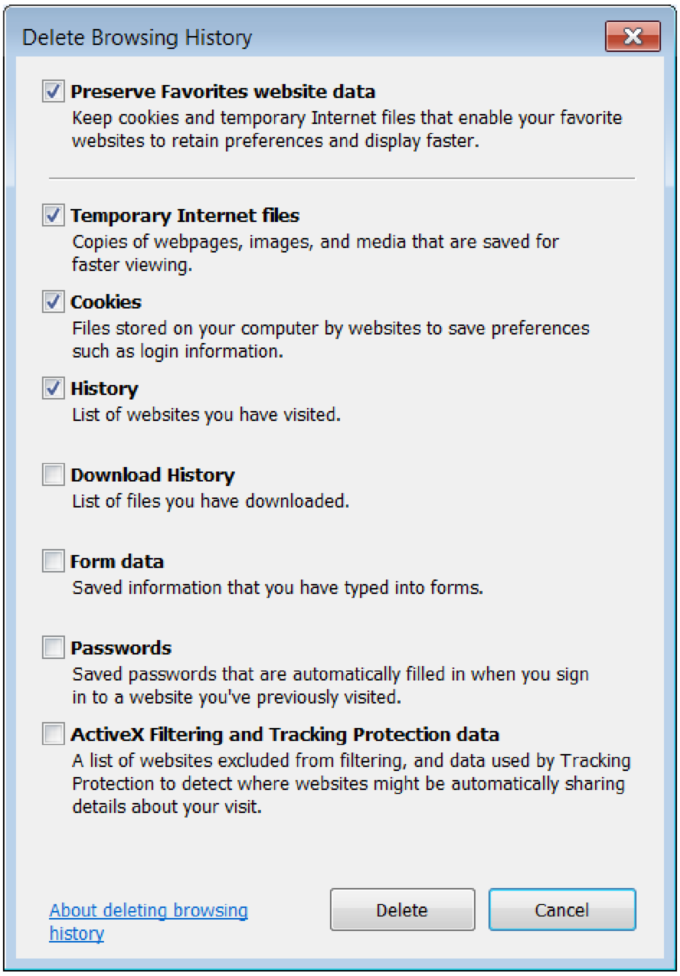
Deleting Private Data from a Browser

MS Internet Explorer automatically saves previously visited web pages, cached Internet files, passwords, cookies and autocomplete data.

Cache is a special folder on the hard disk that stores web pages accessed by your browser. The first time you visit a web page, your browser retrieves all content (text, images, audio etc.) and a copy of these will be stored on the hard disk. The next time you visit the same web page, your browser checks if the last modified dates of the files on the Internet are newer than the ones stored or cached. If the dates are the same, your browser uses the files on your hard disk instead of downloading these again from the web server. Thus the cache speeds up browsing of web pages. The files stored in the cache are known as **temporary Internet files**. The temporary Internet files are never deleted unless the cache is full.

To delete previously visited web pages, cached Internet files, passwords, cookies and autocomplete data:

1. In MS Internet Explorer, click the **Tools** button on the right side of the Command bar. A menu will be displayed.
2. Point to **Safety**.
3. Click **Delete browsing history…** The Delete Browsing History dialog box is displayed.



Delete Browsing History

☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

☑ **History**
List of websites you have visited.

□ **Download History**
List of files you have downloaded.

□ **Form data**
Saved information that you have typed into forms.

□ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

□ **ActiveX Filtering and Tracking Protection data**
A list of websites excluded from filtering, and data used by Tracking Protection to detect where websites might be automatically sharing details about your visit.

4. Tick the **Temporary Internet files**.
5. Tick the **Cookies** checkbox.

6. Tick the **History** check box.
7. Tick the **Form data** checkbox.
8. Tick the **Passwords** checkbox.
9. Click **Delete** button.

Note that:

- Deleting your browsing history does not delete your list of favourites or bookmarked web pages.

Content-Control Software

Content-control software is designed to restrict or control the content a person can access on the web. This software determines what content will be available or what content will be blocked.

Such restrictions can be applied at various levels. A government can attempt to apply content-control nationwide. An Internet Service Provider can apply restrictions to its clients. An employer can apply restrictions to its employees. The school administration can apply restrictions to its students. A parent can apply restrictions to a child's computer.

Content-control software is typically used to restrict content which is considered objectionable such as racial hatred, homophobic or pornographic sites. Some content-control software includes time control functions that empowers parents to set the amount of time that their children may spend accessing the Internet or playing games.

Content-control software is also referred to as Internet filter software. Content-control software used at homes is often referred to as parental control software.

Internet filter software and parental control software are used to control content, block objectionable websites and set up passwords to allow access to sites as needed. Powerful features such as email filtering, popup blocking and chat room monitoring are other tools available in these web filter programs.

Social Networking

Many individuals use **social networking websites** (e.g. Facebook) to keep in touch with their friends and seek ‘old’ friends. They set up an online profile, describing their interests, and add links to other profiles. Generally, users are able to post personal information, including photographs, videos etc. Some people join special interest groups on social networking sites.

Social networking provide ways to learn, talk and socialize, however some users abuse these systems.

- **Cyber bullying** is a practice where an individual or group uses the Internet to ridicule, embarrass, threaten, harass or harm another person. Cyberbullying can take many forms:
    - Making fun of another user in an Internet chat room.
    - Harassing a user over an instant messaging session.

  - Posting derogatory messages on a user's social networking page.
  - Circulating false rumours about someone on social networking websites.
  - Posting unflattering pictures of another user on the Web.
  - Spamming another user with unwanted email messages.
  - Sending threatening or provocative emails.
  - Repeatedly calling another person's cell phone.

  Cyberbullying can lead to low self-esteem and depression. It should not be tolerated. Victims should:

  - Avoid sharing personal details online.
  - Block cyberbullies on all social media sites.
  - Report cyberbullies to website administrators.
  - Report cyberbullies to the police.

- **Grooming** is the process where an adult establishes a friendly relationship with children or teenagers with the aim of getting them to behave inappropriately. The adult uses chat rooms or social networking sites to find and befriend youngsters. Initially the communication will be very friendly and the adult may also promise gifts to youngsters. Gradually the adult wins the trust of the youngsters and makes arrangements to meet in person. In due course the adult may get the youngsters to behave inappropriately such as being photographed nude or engaging in sexual encounters etc.

  These adults often pretend to be younger and may even change their gender. Many give a false physical description of themselves which may bear no resemblance to their real appearance. Some send pictures of other people, pretending that it is them.

  Children and teenagers should:

  - Understand that online, persons may lie about themselves.
  - Avoid giving personal information (e.g. name, email, phone number, home address, or school name) to people they don’t know.
  - Avoid meeting people who they have met online unless a parent or a trusted adult is present.
  - Avoid accepting emails, instant messages or opening files from people they don’t know.
  - Tell their parents or a trusted adult if someone or something makes them feel uncomfortable or worried.

- **Misleading/dangerous information** can be posted by users on social networking sites. Postings on social networking sites are not usually controlled by administrators. This means that users can post almost anything on these sites. Misleading/dangerous information include posting: rumours, false information about a product or service and messages that incite social hatred.

- **False identities** is the process of setting up and using fake profile accounts on a social networking site. It is very easy to set up a profile on social networking sites. People of all ages may set up fake profiles to pass themselves off as someone else. Some use the identities of genuine people, using information and photographs they find on the Internet. One should avoid accepting strangers as new friends.

- **Fraudulent links or messages** may be sent to elicit information from you. Phishing messages may also be sent via social networking sites.

Protecting Yourself Online

- Use appropriate privacy settings on social networking sites to limit access to your information, pictures etc. Double-check your privacy settings to ensure that these are working as you would expect. From time to time developers of social networking sites implement improvements to privacy settings. Adjust your privacy settings accordingly.

- Be careful how much information you divulge about yourself on social networking sites. You may have friends with whom you are uncomfortable sharing particular information. Avoid posting comments and pictures which embarrass you if seen by family members, colleagues, students, your present or future employer.

- Posting particular messages on walls of social networking sites may not always be appropriate. Avoid posting sensitive information including when you plan to be away from home, confidential data about your company etc. Use private messaging when appropriate.

■ COMMUNICATIONS

Encrypting & Decrypting Email

Email messages travel between servers on the Internet in plain text format making it easy for persons with the right tools to intercept and read email. Sending an email message is the electronic equivalent of sending a postcard. One should avoid sending confidential data via email unless this is encrypted.

As indicated in an earlier section encryption is the conversion of data to a form that cannot be easily understood by unauthorized people. Encrypting email messages and attachments involves converting these to a format which is unreadable by people who do not have the right key. Email encryption hides the email content from eavesdroppers. When you encrypt a message, you create the equivalent of a sealed envelope so that only you and the recipient can see the message.

Digital Signatures

Emails can be encrypted and decrypted by means of a digital signature that uses public and private keys. The public key is shared with everyone while the private key is kept private.

To be able to send digitally signed emails, one needs to apply for a digital certificate from a Certificate Authority (CA). The CA issues the digital certificate containing the applicant's public key and other identification information. The CA makes its own public key readily available on the Web.

The digital certificate is a pair of files on your computer containing the public key and the private key. Your computer programs understand how to share only the public portion of your keys so that others can see them, while still keeping your private keys secure.

When you send a digitally signed email this will also include the digital certificate (attached). The digital certificate is used to verify that the sender is who s/he claims to be, and to provide the recipient with the means to encode a reply.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

Creating & Adding a Digital Signature

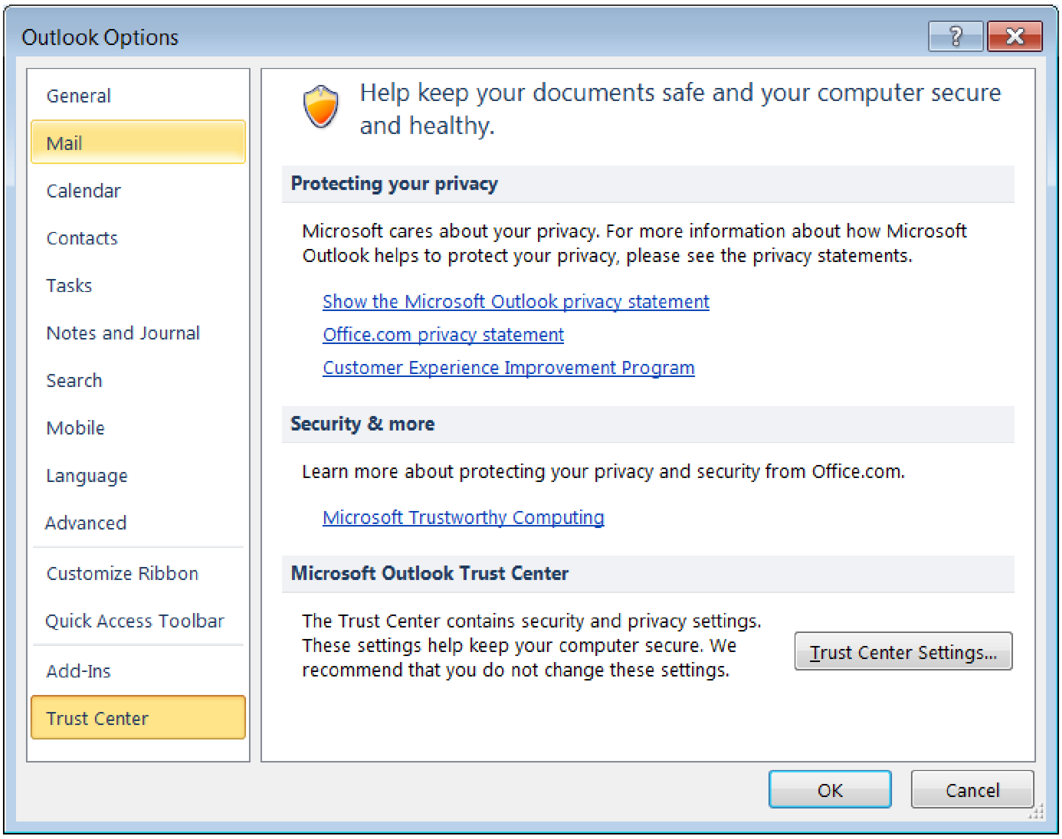
To start adding a digital signature to an email, you need to purchase a digital certificate from a Certificate Authority (CA). Some CAs provide free digital certificates e.g. Comodo (www.comodo.com).

To create a digital certificate, visit the website of the CA and enter your details including your email address. Make sure that you enter your personal details in a secure website (URL starts with https://).

The CA will send you an email after you enrol for a digital certificate. Typically the email contains a link that takes you to a website to 'collect' and install your digital certificate on your computer.

Once you have created a digital signature you can add this in you email program (e.g. MS Outlook 2010 and Thunderbird). To add a digital signature in MS Outlook 2010:

1. In MS Outlook 2010, click the **File** tab.
2. Click **Options**. The Outlook Options dialog box is displayed.
3. Click **Trust Center**.



Help keep your documents safe and your computer secure and healthy.

Protecting your privacy

Microsoft cares about your privacy. For more information about how Microsoft Outlook helps to protect your privacy, please see the privacy statements.

Show the Microsoft Outlook privacy statement

Office.com privacy statement

Customer Experience Improvement Program

Security & more

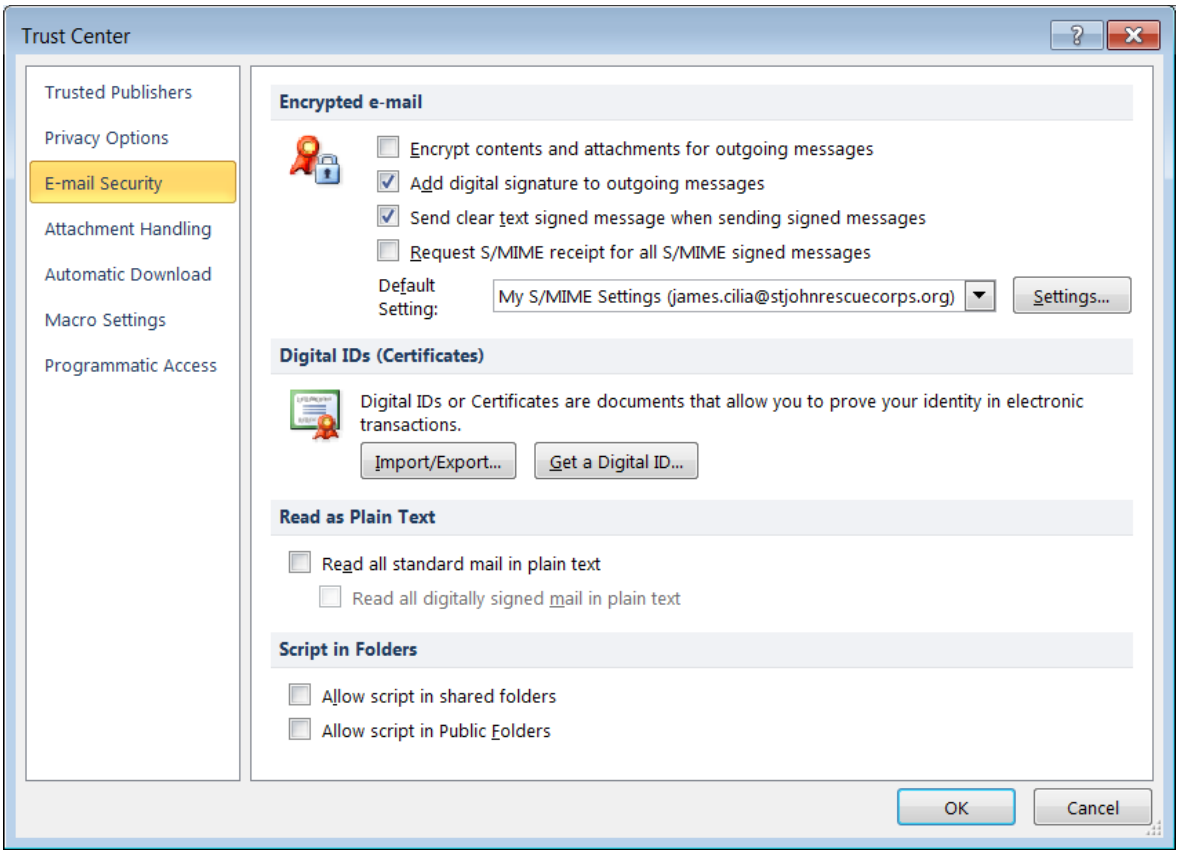
Learn more about protecting your privacy and security from Office.com.

Microsoft Trustworthy Computing

Microsoft Outlook Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

4. Click **Trust Center Settings…** button. The Trust Center dialog box is displayed.
5. Click **E-mail Security**.
6. Tick the **Add Digital Signature to Outgoing Messages** checkbox. This option includes your signing certificate on all outgoing messages.
7. Tick the **Send clear text signed messages when sending signed messages** checkbox. This ensures that all recipients can read your signed messages including those that use web-based or mobile mail client.
8. Click **OK** button to close the Trust Center dialog box.
9. Click **OK** button to close the Outlook Options dialog box.



Encrypted e-mail

- □ Encrypt contents and attachments for outgoing messages
- ☑ Add digital signature to outgoing messages
- ☑ Send clear text signed message when sending signed messages
- □ Request S/MIME receipt for all S/MIME signed messages

Default Setting: My S/MIME Settings (james.cilia@stjohnrescuecorps.org)

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

- □ Read all standard mail in plain text
- □ Read all digitally signed mail in plain text

Script in Folders

- □ Allow script in shared folders
- □ Allow script in Public Folders

In order to exchange digitally signed e-mail messages with another user, you must have each other's public keys. You provide access to your public key through your digital certificate.

You can provide your digital certificate to another person by sending a digitally signed email message. Similarly other persons can provide you with their digital certificates by sending you a digitally signed email message.

To add a digital certificate to your contacts' list:

1. Open a message that is digitally signed. A signed message is indicated in the message list by a Signature icon.
2. In the From box, right-click the recipient's name.
3. Click **Add to Outlook Contacts**.

The certificate is now stored with your contact entry for this recipient. You can now send encrypted messages to this person.

Note that:

- If you already have an entry for this person, in the Duplicate Contact Detected dialog box, select **Update information of selected Contact**. A backup copy is saved in Deleted Items Folder.
- To view the certificate for a contact, double-click the person's name, and then click the **Certificates** tab.

Unsolicited Email

We should be careful about unsolicited (unexpected) emails that we receive. Some of these emails may contain a virus or malware, or may be trying to gain sensitive information and should not be opened.

One should be very careful before opening an email attachments even if these are received from people that they know. Email attachments may contain macros or executable files that harm your computer.

As indicated earlier, one should also be careful about phishing email designed to steal personal data or information such as bank card numbers, passwords, and account data. Typically phishing email appears to be sent from legitimate organisations or reputable people. The email usually contains a link to a fake web page that seems legitimate. The fake web page may be very similar, if not identical to the web page of the organisation. In such cases, the only difference would be that the address of the fake web page does not contain https://. Therefore it is important that before you enter personal data in any web page you ensure that the address field in the web browser starts with an https://.

Instant Messaging

Instant Messaging (IM) is real-time text based communication between two or more people over a network usually the Internet. The communication is real time – similar to a telephone conversation but using text instead of voice.

IM may involve the installation of a program, referred to as instant messenger, on the users’ computers or devices. It may involve the use of an online interface in online collaboration tools (e.g. Google Apps or MS Office 365) or social networking sites (e.g. Facebook).

Typically, the instant messaging system alerts you whenever somebody on your contacts’ or friends’ list is online. You can then start a chat session with that particular individual. You can also send files such as documents and pictures.

Some IM systems permit messages to be sent when the recipient is not online. In these cases, IM behaves like email and sends a message to the recipient's email address. IM systems may also include live voice or video communication.

Instant Messaging Security Threats

As indicated earlier, IM systems allow transfer of text messages and files. Consequently, IM systems can transfer worms and other malware. Instant messengers can also provide an access point for backdoor trojan horses. Furthermore, finding victims involves a simple process of selecting these from a directory of contacts’ lists.

In addition to file transfers made by users, IM systems support peer-to-peer file sharing where one can share a folder or drive. This means that all the files on a computer can be shared using the IM system, leading to the spread of files that are infected with a virus or other malware. This characteristic makes information being communicated along IM vulnerable to unauthorized viewing.

To ensure confidentiality while using IM:

- Avoid using the IM system to communicate sensitive information.
- If you plan to send files containing sensitive data, ensure that these are encrypted before sending.
- Avoid enabling peer-to-peer file sharing.

■ SECURE DATA MANAGEMENT

Physical Security of Devices

Physical security describes measures designed to ensure the physical protection of IT equipment and data from damage and unauthorized physical access. IT equipment must be protected from physical threats including theft, vandalism, fire and natural disasters.

- **Log equipment** - It is important to keep an inventory of all IT equipment, their location and details of persons using the equipment.
- **Use cable locks** - To minimise theft of computers and laptops, one can use cable locks to lock these to a desk.
- **Control access** - The server room is the heart of any computer network. Someone with physical access to the servers, switches, routers, cables and other devices in that room can do enormous damage. It is therefore important that access to the server room is restricted to authorised people only. The server room must be locked at all times.

  Access to the server room should be controlled via an authentication system integrated in the locking devices. For example a smart card, token, or biometric scan is required to unlock the doors. Moreover a record is made of the identity of each person entering the server room. In addition to authentication systems integrated to locking devices of the server room, a video surveillance camera can be installed to monitor persons entering and leaving the server room

Data Back-up

Backing up data is the copying of data files to a secondary storage medium (USB flash disk, CD/DVD, external hard disk or magnetic tape streamer) as a precaution in case the first medium fails.

Backups of data are important in case:

- the computer fails;
- the computer is stolen or vandalised;
- the computer is damaged because of a fire or flooding and
- a virus damages/deletes data from the computer.

All companies implement data backup procedures to maintain business continuity.

Most users store data (e.g. important documents, financial records, web bookmarks/history, photos) on the hard disk without backing this on other storage media. It is of utmost importance to back up your data regularly.

It is suggested that you make at least two backups of all your data files. To be especially safe, you should keep one backup in a different location from the other – off-site storage. The latter protects data against theft and fire hazards.

You can back up files using operating system commands, or you can buy a dedicated backup utility (program). Backup programs often compress the data so that backups require fewer disks.

Back up procedures feature the following:

- **Regularity/Frequency** – Data should be backed up at regular intervals that reflect the frequency of change in data. If critical data changes on a daily basis, then one should back up this data every day. In case of home users, data may be backed up on a weekly or monthly intervals.

- **Schedule –** The network or system administrator in a company configures the backup programs to perform backups according to a schedule.

- **Storage location** – Data can be backed up on secondary storage devices. In case of companies data is typically backed up on magnetic tape streamers and external hard disks. Home users back up their data on DVDs, USB pen drives, external hard disks and online storage. It is important to store one copy in a location away from the computer.

Secure Destruction

File deletion involves the removal of a file from a computer's file system. The reasons for deleting files are to:

- free the disk space.
- remove duplicate or unnecessary data to avoid confusion.
- make sensitive information unavailable to others.

All operating systems include commands for deleting files. Files may be deleted one-by-one or in batches.

By default, when you delete a file in MS Windows, the file will be moved to the Recycle Bin. However, even when you empty the Recycle Bin, the file will not be permanently deleted. To permanently delete files from a hard drive, you need to overwrite the data contained in the files. Unless the software you are using replaces the "deleted" file's data with new data, the file would not be permanently deleted. The file is not permanently deleted until the data of the file is overwritten with new data and the old data rendered unrecoverable. Hard drive erasure software is used to permanently delete files from the computer.

Data can be permanently destroyed using these methods:

- **Shredding** – CDs, DVDs and papers containing sensitive data should not be thrown away in garbage bins. Instead shredding machines should be used to destroy these, making it impossible for people to recover data.

- **Drive/media destruction** – Holes can be drilled in a hard drives to make the data unreadable.

- **Degaussing** - This is a process that uses a magnetic field on a hard disk or a magnetic tape to scramble electronic data and make it unreadable. The data on degaussed hard disks or tapes cannot be recovered. Several companies offer degaussing services.

- **Data Destruction Utility** – This is a software program designed to overwrite data in a hard disk in a way that will make it impossible to recover data after the process. This software is also referred to as hard drive eraser software or disk wipe software. Following this process a hard-disk can be reused to store new data.