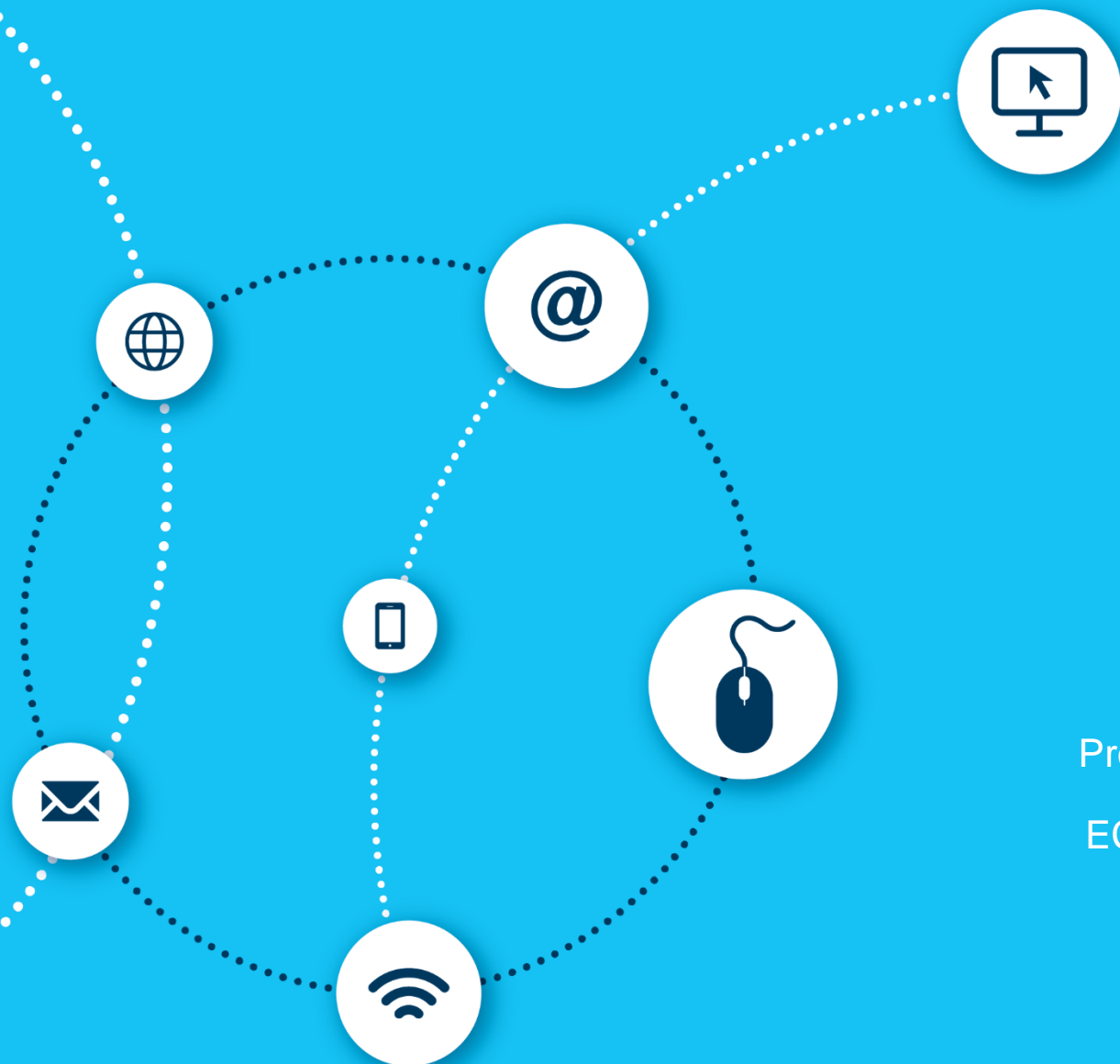


ECDL IT SECURITY

Syllabus 2.0
Learning Material



Provided by:
ECDL Malta

European Computer Driving Licence, ECDL, International Computer Driving Licence, ICDL, e-Citizen and related logos are all registered Trade Marks of The European Computer Driving Licence Foundation Limited ("ICDL Foundation").

This courseware may be used to assist candidates to prepare for the ICDL Foundation Certification Programme as titled on the courseware. ICDL Foundation does not warrant that the use of this courseware publication will ensure passing of the tests for that ICDL Foundation Certification Programme.

The material contained in this courseware does not guarantee that candidates will pass the test for the ICDL Foundation Certification Programme. Any and all assessment items and / or performance-based exercises contained in this courseware relate solely to this publication and do not constitute or imply certification by ICDL Foundation in respect of the ECDL Foundation Certification Programme or any other ICDL Foundation test. This material does not constitute certification and does not lead to certification through any other process than official ICDL Foundation certification testing.

Candidates using this courseware must be registered with ECDL Malta before undertaking a test for an ICDL Foundation Certification Programme. Without a valid registration, the test(s) cannot be undertaken and no certificate, nor any other form of recognition, can be given to a candidate. Registration should be undertaken at an Approved Test Centre.

Screen shots used with permission from Microsoft. Tool and application-specific details are correct as of May 2016. Online tools and applications are subject to frequent update and change.

ECDL IT SECURITY

Maintaining IT security on a day-to-day basis is a vital online skill to ensure professional, personal, and financial security. Knowing best practices with regards to managing data, who you disclose personal information to, and browsing securely will help you stay safe online. This ECDL IT Security module will help you understand the primary concepts underlying the IT Security in daily life, and to use relevant techniques and applications to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately.

On completion of this module you will be able to:

- Understand the key concepts relating to the importance of secure information and data, physical security, privacy and identity theft.
- Protect a computer, device, or network from malware and unauthorised access.
- Understand the types of networks, connection types, and network specific issues, including firewalls.
- Browse the World Wide, Web; communicate on the Internet securely.
- Understand security issues related to communications, including e-mail and instant messaging.
- Back-up and restore data appropriately and safely; securely dispose of data and devices.

What are the benefits of this module?

This module highlights skills and knowledge relating to the importance of secure information and data, physical security, privacy and identity theft. At the end of this module you will be able to demonstrate competency in these areas, and carry out your online activities in a safe manner. Once you have developed the skills and knowledge set out in this book, you will be in a position to become certified in an international standard in this area – ECDL IT Security.

For details of the specific areas of the ECDL IT Security syllabus covered in each section of this book, refer to the ECDL IT Security syllabus map at the end of the book.

ECDL IT SECURITY

| | |
|---|-----------|
| LESSON 1 – SECURITY CONCEPTS | 1 |
| 1.1 Data Threats | 2 |
| 1.2 Value of Information | 4 |
| 1.3 Personal Security | 7 |
| 1.4 File Security | 9 |
| 1.5 Review Exercise..... | 17 |
| LESSON 2 - MALWARE | 18 |
| 2.1 Types of Malware | 19 |
| 2.2 Protection..... | 21 |
| 2.3 Review Exercise..... | 26 |
| LESSON 3 – NETWORK SECURITY..... | 28 |
| 3.1 Networks and Connections..... | 29 |
| 3.2 Wireless Security..... | 36 |
| 3.3 Review Exercise..... | 47 |
| LESSON 4 – ACCESS CONTROLS | 48 |
| 4.1 Methods | 49 |
| 4.2 Password Management..... | 52 |
| 4.3 Review Exercise..... | 55 |
| LESSON 5 – SECURE WEB USE..... | 56 |
| 5.1 Browser Settings | 57 |
| 5.2 Secure Browsing | 59 |
| 5.3 Review Exercise..... | 63 |
| LESSON 6 – COMMUNICATIONS..... | 64 |
| 6.1 E-Mail..... | 65 |
| 6.2 Social Networking..... | 74 |
| 6.3 VoIP and Instant Messaging..... | 79 |
| 6.4 Mobile | 80 |
| 6.5 Review Exercise..... | 85 |
| LESSON 7 – SECURE DATA MANAGEMENT..... | 86 |
| 7.1 Secure and Back up Data..... | 87 |

| | | |
|---------------------------|---------------------------------------|-----------|
| 7.2 | Secure Deletion and Destruction | 95 |
| 7.3 | Review Exercise..... | 97 |
| ECDL SYLLABUS..... | | 98 |

LESSON 1 – SECURITY CONCEPTS

In this section, you will learn about:

- Data threats
- Value of information
- Personal security
- File security

1.1 DATA THREATS

Maintaining data security is a vital for individuals, small businesses and large corporations. Ensuring that data is kept secure is essential in avoiding disaster, both personally and professionally, but unfortunately it can be a difficult task due to malicious or unintentional behaviour.

The following are some of the common terms related to data threats:

- **Data**
A collection of facts, figures and statistics related to an object. Data can be processed to create useful information. Data is raw and unorganised facts and figures.
- **Information**
Information is data that is organised and processed to give it more meaning and context. While data is like pieces of a puzzle, information is like a completed puzzle that shows a final picture to the user.
- **Cybercrime**
An offence that involves using the Internet or a computer to carry out illegal activities, often for financial or personal gain. Examples include identity theft and social engineering.
- **Hacking**
Hacking involves using computer expertise to gain access to a computer system without authorisation. The hacker may wish to tamper with programs and data on the computer, use the computer's resources, or just prove they can access the computer.

Key threats to data security:

- System crashes and hard disk crashes – a system or hard disk crash may cause physical damage to the storage media.
- Computer viruses which may delete or corrupt files.
- Faulty disks and disk drives – physical damage to disks such as bad sectors.
- Data lost by accidentally deleting or overwriting files.
- Deletion by unauthorised users or hackers.
- Destroyed by natural disasters, such as floods, fire or earthquakes.
- Acts of terrorism, or war.
- Accidental or malicious deletion by employees.

Cloud Computing

Cloud computing is a type of internet based, on-demand computing service that lets users share resources and data with other devices anytime and anywhere. In a cloud computing environment, services, applications, storage and servers are usually managed by third party data centres. This allows for easy access to services and applications with minimal management effort.

Cloud Computing Vulnerabilities

Cloud computing has its advantages and disadvantages. When deciding to migrate to the cloud, you need to consider some of the possible cloud service vulnerabilities:

1. **Session Hijacking** – when an attacker intercepts or steals a user's cookie in order to use the application. The stolen cookie allows the attacker to impersonate the user, and log in using the user's authenticated credentials.
2. **Service Reliability** – as with on premise services and private clouds, you can expect the occasional downtime and unavailability of services. Cloud Service Providers have uninterrupted power supplies, but they may sometimes fail. So, 100% uptime should not be expected.
3. **Reliance on the Internet** – the availability of cloud services is highly dependent upon Internet connectivity. If the Internet connection fails or is temporarily unavailable, users will not be able to use the required cloud services. This may cause loss of revenue for the company. This would also greatly affect services that need to run 24/7 such as in a hospital, where lives are at stake.

Cloud Computing Threats

- **Data Control** – a big concern of companies moving to the cloud is Data Control. Putting a company's sensitive and confidential data on a cloud service provider's servers is a risk some companies are not willing to take. There is concern about the security of their data and whether it could fall into the wrong hands.
- **Denial of Service** - Due to a fairly simple and sometimes anonymous registration process for some cloud services, cloud services may be used for malicious purposes such as spamming, botnets, Distributed Denial of Service (DDoS) or for distribution of malicious software.
- **Potential Loss of Privacy** – since cloud services are accessible from anywhere on the Internet, there is a concern about privacy of data. When data is transferred from the clients to the cloud, an attacker may be able to intercept the communication.
- **Malicious Insiders** – employees working for the cloud service provided could access your data and steal confidential information.

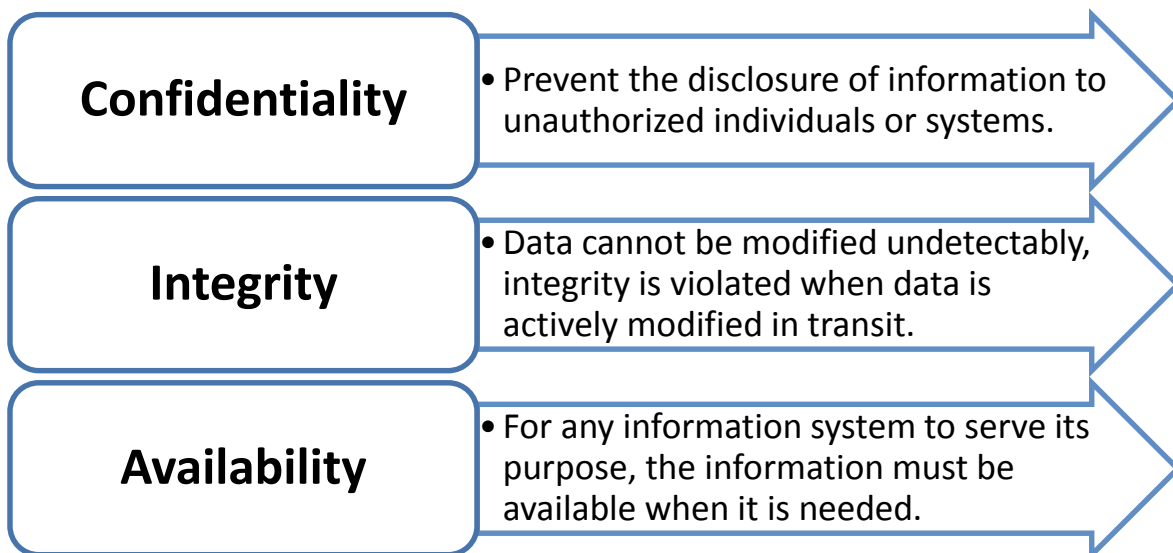
- **Loss of Data** – this could occur if the Cloud Service Provider’s hard drive fails proper data backup was not implemented. A CSP could also accidentally delete your data.

1.2 VALUE OF INFORMATION

Basic Characteristics of Information Security

Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The goals are protecting the confidentiality, integrity and availability of information.



Reasons for Protecting Personal Information

Nowadays, more and more people are using the Internet and mobile devices for online shopping, banking, business, communication and other activities. Some companies rely on various cloud services and other web based services to run their day to day business.

Making information easier to access through the Internet also exposes businesses to some security issues. Hackers are able to take advantage of vulnerabilities in the transmission of data online to gain unauthorised access to systems and networks. There have been many reports of data breaches and identity theft in the past few years. Cybercriminals often steal personal information such as banking records, credit card details, usernames and passwords for financial gain.

Personal Information is most often used by companies to identify and authorise users who transact business on their websites. For example, an online shopping site may have a record of a user's name, address, credit card details, etc. Hackers may steal this information in order to impersonate a user and then conduct fraudulent and unauthorised transactions and other fraudulent activities. Without adequate security and protection of personal information, users are exposed to Internet based crimes such as identity theft and fraud and loss of privacy. Companies which do not protect their user's personal information may lose customers' trust - and their business.

Reasons for Protecting Commercially Sensitive Information

Commercially sensitive information is any information owned by a company that could cause harm if it is lost, misused, stolen or altered in any way.

The following are examples of information that may be classified as being commercially sensitive:

- Financial statements such as balance sheets, cash flow, income statements or equity statements.
- Information such as lists of current and past clients.
- Trade secrets such as designs, formulas, production processes etc.
- Information about new products, marketing strategies or patent information.

Commercially sensitive information must be protected to prevent:

- Theft of private and confidential company information – company information could be stolen by corporate spies, social engineering or hacking. The data may be passed on to the company's competitors to the disadvantage of the owner of the information.
- Accidental loss of data – users may mistakenly delete or alter sensitive data. Storage media or mobile devices containing sensitive information could be misplaced.
- Fraudulent use of company data – such as client information and credit details.
- Corporate sabotage – some competitors may use information to sabotage your business.

Data Privacy or Protection Control

With the widespread use of the Internet to perform various types of business and personal transactions, there is a need for measures to ensure that the privacy and security of the data being used by organisations. Laws and guidelines have been crafted to ensure data and information is not abused and used for any unlawful practices.

Data protection legislation usually provides for the protection of individuals against the unlawful use of a person's personal data and violation of their privacy. Data protection legislation is, however, likely to vary between countries.

In general, persons in possession of personal data must ensure that:

- Personal data is processed in a fair and lawful manner.
- Good practice is always used to process personal data.
- The collection of personal data can only be for legitimate and explicitly stated purposes.
- Personal data shall not be processed if it is not compatible with the purpose for which the information is collected. This is referred to as proportionality.
- Processed personal data is both adequate and relevant.
- There will be no unnecessary processing of personal data.
- Personal data that is processed is accurate and up to date.
- Personal data is not kept for a period longer than is necessary.

Data Subjects and Data Controllers

A **Data Subject** is someone who is the subject of personal data, while a **Data Controller** is an individual (or a collection of people) who control and use that personal data. Within this relationship, there are guidelines and policies that must be followed in the interest of protection and fairness. The Data Controller will be responsible for obtaining and processing the data fairly, keeping it secure, ensuring that it is adequate and relevant, and will provide a copy of a Data Subject's personal data on request.

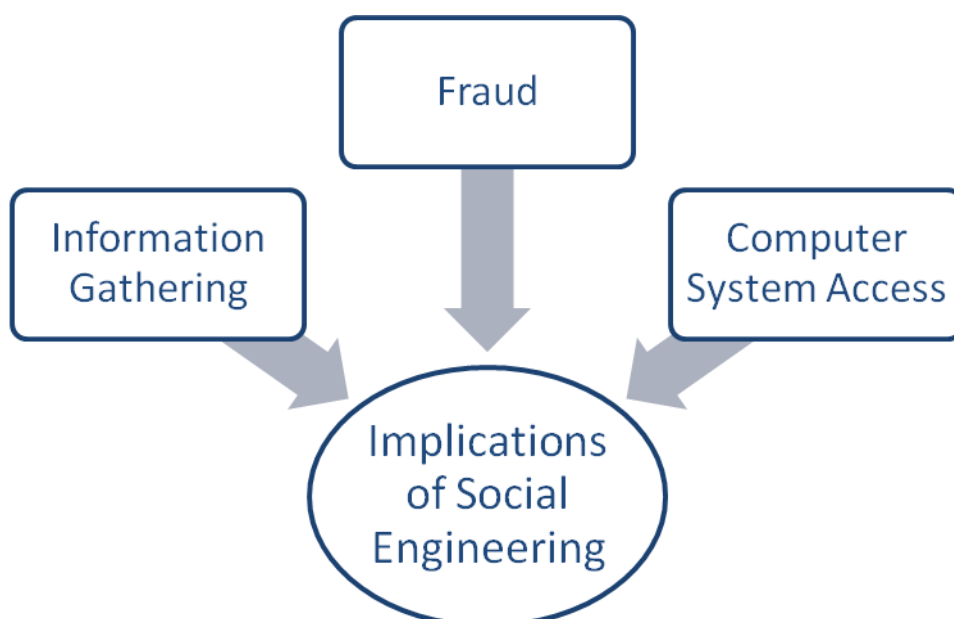
ICT Policies

ICT policies are usually implemented in a workplace to ensure safe and appropriate use of Internet services and connections. A company may issue a document to be signed by employees to comply with their regulations. Businesses that you may not work for but which you use, for example universities, restaurants and public transport that have a shared Wi-Fi network, may also have ICT policies that requires you to comply with before connecting to the network.

1.3 PERSONAL SECURITY

Social Engineering

Social engineering is a way to manipulate or influence people with the goal to illegally obtain sensitive data (for example, passwords or credit card information). Social engineers research and learn about the personal environment of their target and fake their identity to obtain confidential information from the victim. In most cases, they infiltrate third-party computer systems to spy on sensitive data.



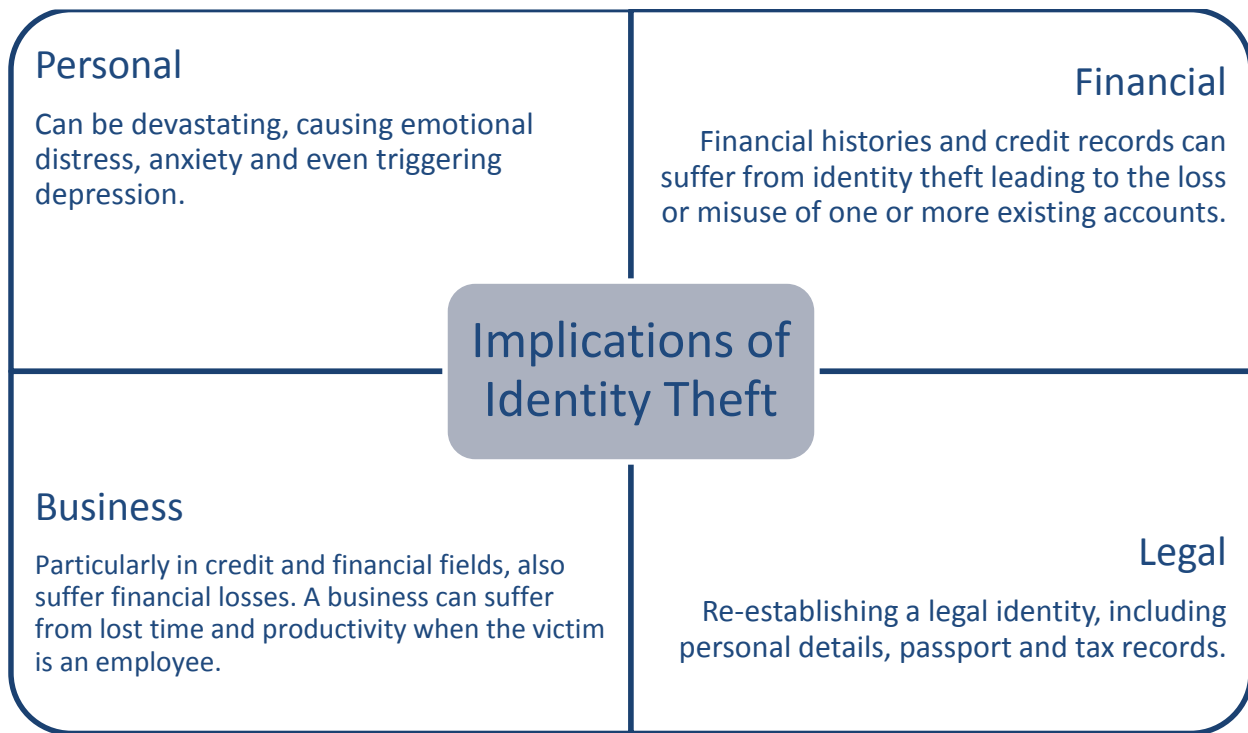
Methods of Social Engineering

- **Phone calls**
One of the most common methods social engineers use in their attacks is conducted via the phone. The attacker may impersonate a person of authority, a person representing a person of authority or a service provider to extract information from an unsuspecting user. For example, a person claiming to be the CEO of the company calls someone on the helpdesk, requesting for his password, which he claims to have forgotten.
- **Phishing**
A type of social engineering attack wherein the perpetrator sends an e-mail that appears to come from a legitimate source (for example, a banks). The e-mail usually requests for verification of information, sometimes warning of dire consequences if the recipient fails to comply. A phishing e-mail usually includes links to fraudulent web pages which are made to look very similar to legitimate web pages, including logos and content.
- **Shoulder Surfing**
This includes direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, ATM PINs and security codes.

Identify Theft and Its Implications

Identity theft is when someone deliberately impersonates and uses another person's identity. This is usually done for financial gain or to obtain credit and/or other benefits using someone else's name: for example, when someone uses another person's identity to obtain a driver's license. This type of fraud could have a devastating effect on the person whose identity has been assumed.

An initial implication of identity theft is the amount of time and money needed to re-establish your identity and credit history and to clear your name.



Methods of Identity Theft

- Information Diving**

Also known as Dumpster Diving, it is a method of obtaining personal or private information by digging through a dumpster or trash bin for discarded documents or material such as utility bills or credit card statements.
- Skimming**

Identity thieves use skimming as a method of capturing a victim's personal data by using a small electronic device. A skimmer is a device that is usually attached to an ATM machine's card slot. A victim may unwittingly slide his card into the skimmer, which then reads and stores all the information from the card's magnetic strip.
- Pretexting**

This involves creating and using an invented scenario (the pretext) to engage a targeted victim. The pretext increases the chance the victim will reveal information or perform actions that would be unlikely in ordinary circumstances – for example, someone pretending to be from a company that provides you with a service might persuade you to share your bank account details with them.

1.4 FILE SECURITY

Often, some of the most important information you have is stored on files such as documents and spreadsheets. There are a range of security considerations associated with these files that you should be aware of.

Enabling/Disabling Macro Security Settings

Macros are used to automate repetitive or frequently-used tasks in Microsoft Office applications. A macro can be created by using the Macro recorder feature or written by software developers using VBA (Visual Basic for Applications). A person with malicious intent could potentially create destructive macros, which can spread viruses. Therefore, macros are a potential security threat.

Users can disable macros automatically and enable them only when they trust that source of the file. The macro security settings can be found in the Trust Center. In some organisations, these settings are disabled by default and cannot be changed without authorisation from system administrators.

Example: To set macro security settings in Microsoft Excel 2013

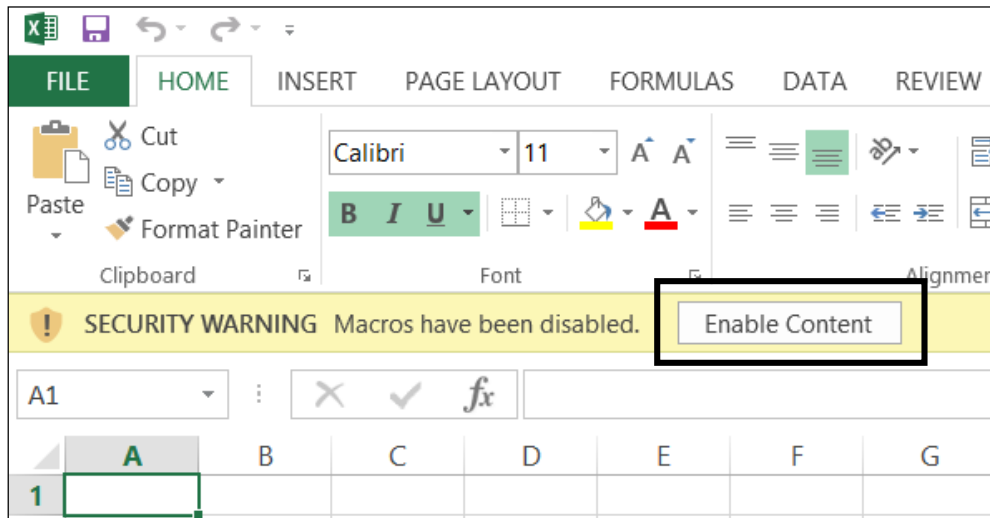
1. Click the **FILE** tab.
2. Click **Options**.
3. Click **Trust Center**, click **Trust Center Settings** and then click **Macro Settings**.

Macro Settings

For macros in documents not in a trusted location:

- Disable all macros without notification
- Disable all macros with notification
- Disable all macros except digitally signed macros
- Enable all macros (not recommended; potentially dangerous code can run)

4. Click on one of the options below:
 - a. **Disable all macros without notification**
Select this setting if you do not want to allow macros to run, unless they are in a trusted location. Users will not receive any notifications when they open Excel macro enabled files.
 - b. **Disable all macros with notification**
When a macro-enabled file is opened, a security warning is displayed, letting the user choose to enable macros. This setting is the default.



- c. **Disable all macros except digitally signed macros**
With this setting, only macros that are digitally signed by a trusted publisher are allowed to run. If the macro is signed by a publisher you haven't trusted, a notification will appear to let you trust the publisher, thereby enabling the macros.
- d. **Enable all macros (not recommended; potentially dangerous code can run)**
Allow all macros to run with no notifications or security warnings. This setting leaves your machine vulnerable to macro viruses and is not recommended.

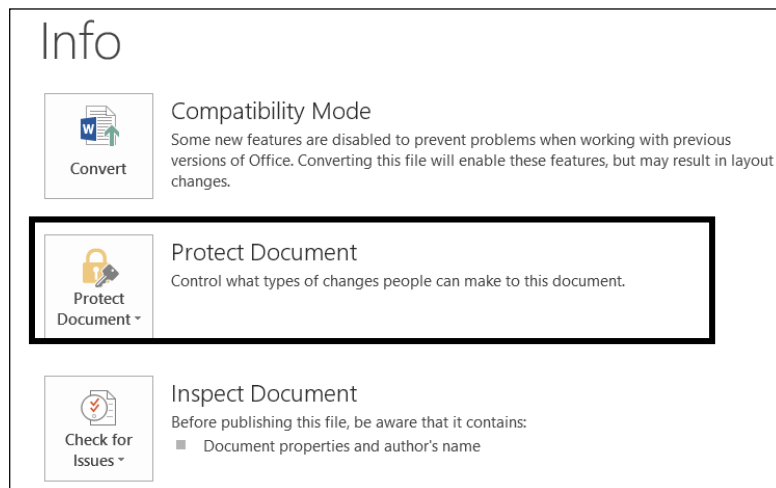
5. Click **OK**.

Setting File Passwords

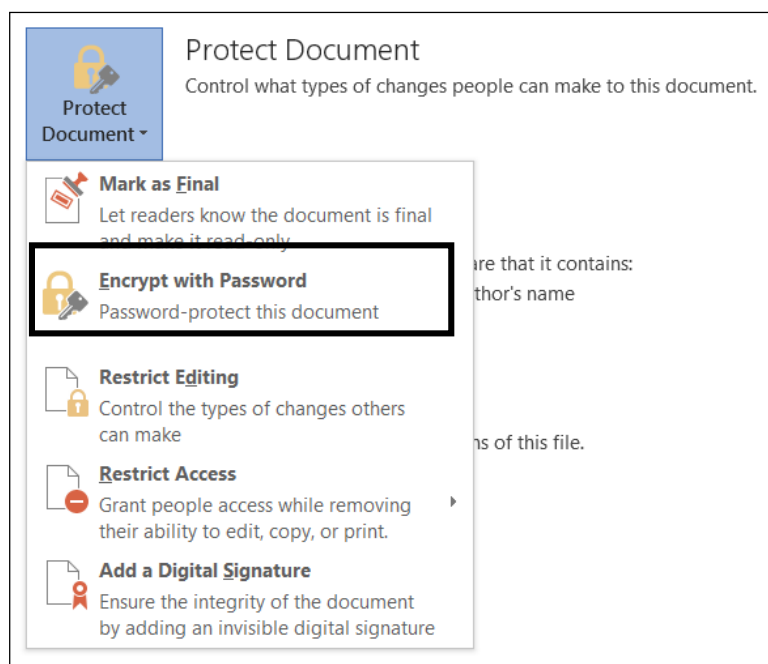
In the Microsoft Office system, you can use passwords to help prevent other people from opening and modifying your documents, workbooks, and presentations.

To set file password for a **Microsoft Word** document:

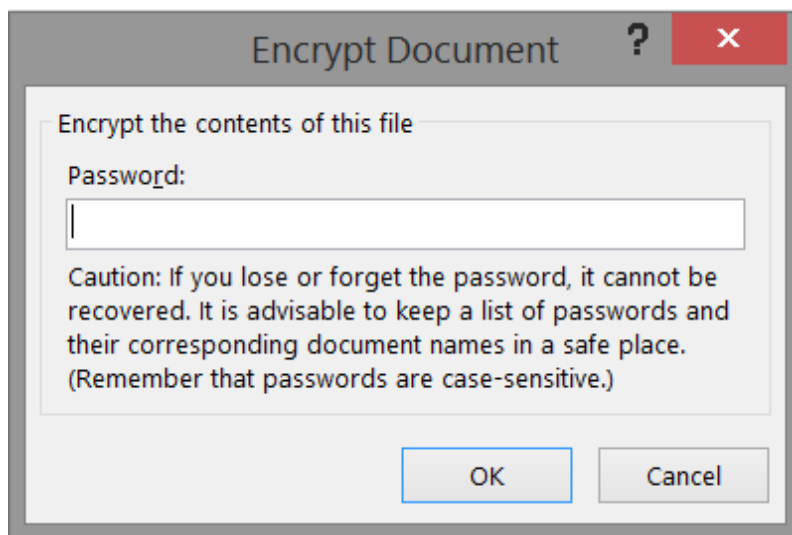
1. Click the **FILE** tab.
2. Click **Info**.
3. Click **Protect Document**.



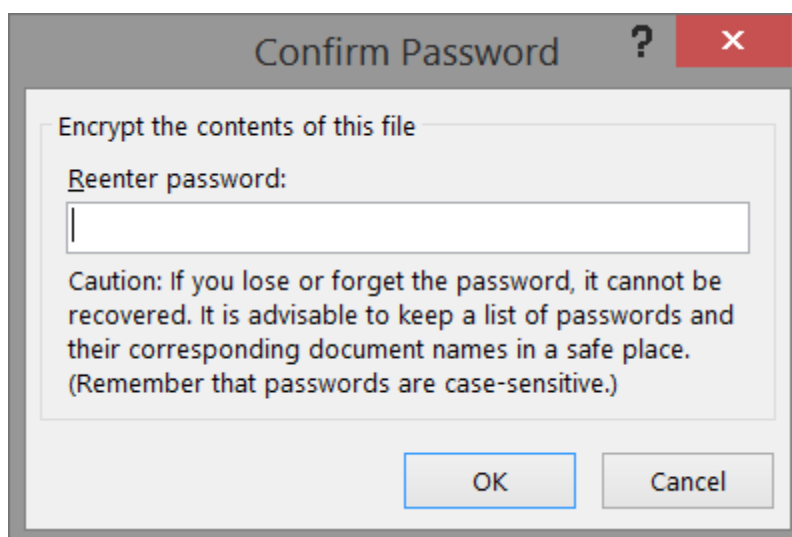
4. Click **Encrypt with Password**.



5. In the **Encrypt Document** dialog box, type a password in the **Password** box.



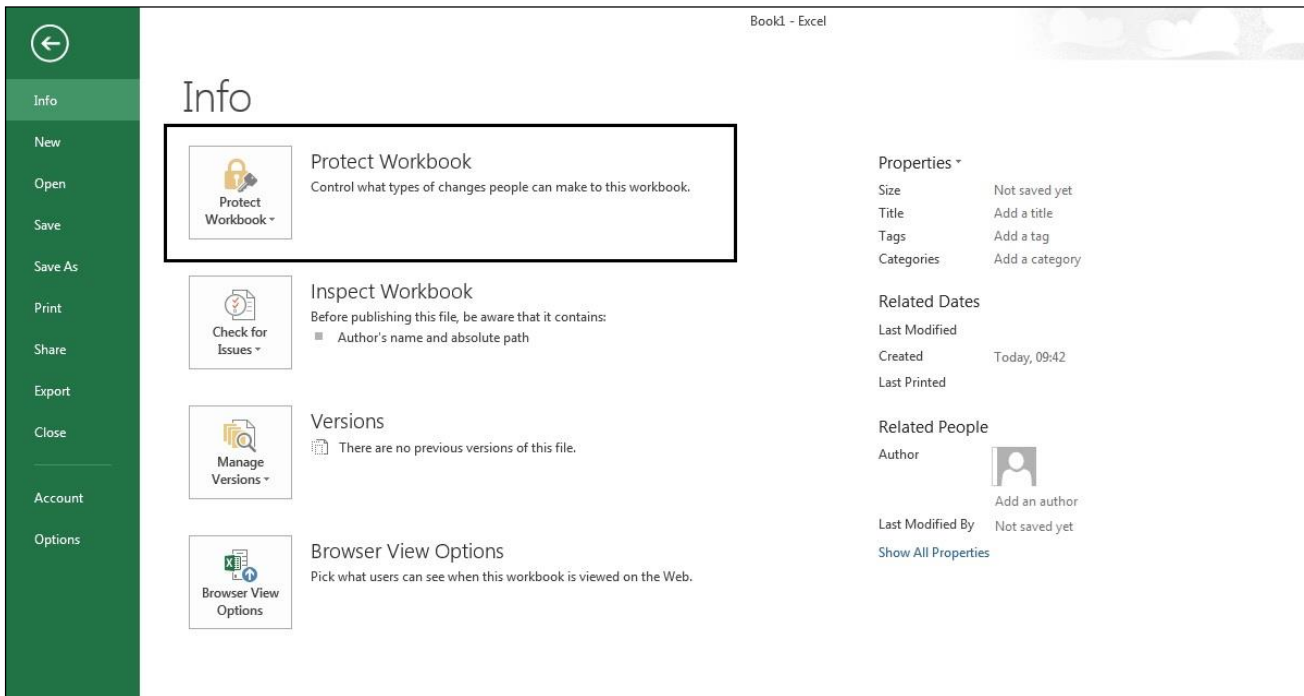
6. Click **OK**.
7. In the **Confirm Password** dialog box, type the password again in the **Reenter password** box, and then click **OK**.



8. Save the file.

To set password for a **Microsoft Excel** spreadsheet:

1. Click the **FILE** tab.
2. Click **Info**.
3. Click **Protect Workbook**.



4. Click **Encrypt with Password**.

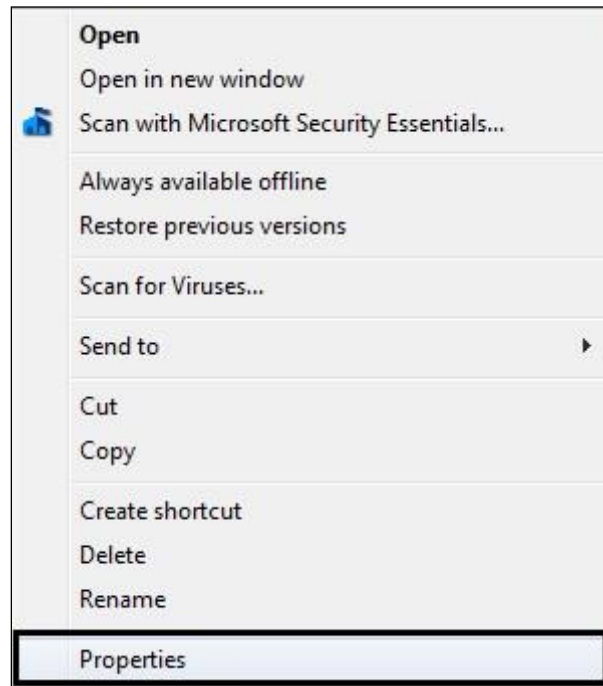


5. In the **Encrypt Document** dialog box, type a password in the **Password** box.
6. Click **OK**.
7. In the **Confirm Password** dialog box, type the password again in the **Reenter password** box, and then click **OK**.
8. Save the file.

Encrypt a Folder or Drive

To encrypt a folder:

1. Right click the folder you wish to encrypt.
2. Click on **Properties**.



3. Under the **General** tab, click **Advanced**.
4. Tick the box beside **Encrypt contents to secure data**.



5. Select **OK**.

Advantages and Limitations of Encryption

The single most important reason for using encryption is to preserve confidentiality.

Advantages:

- Ensures that private and confidential data can only be viewed by the intended recipient. This ensures that only those authorised to see the information will be able to view it.
- Encryption of data while in transit prevents anyone who is not the intended recipient of the data from opening and reading the data, even if the data is intercepted.
- Ensures data integrity and prevents any unauthorised alteration of your data.
- Encryption allows you to verify if the author of the document is or isn't who they say they are.

Limitations:

- If you forget your password then you may not be able to recover your data.
- Some forms of encryption only offer nominal protection and can be broken easily with the right program, for example an older ZIP archive or Word Document.
- The very existence of encrypted files attracts suspicion as to what it is you are trying to protect whereas a non-encrypted file would not attract the same level of interest.
- Cannot prevent deletion of data.

1.5 REVIEW EXERCISE

1. The process of intentionally accessing a computer without authorisation or exceeding authorised access is known as:
 - a. Shoulder Surfing
 - b. Phishing
 - c. Hacking
 - d. Pretexting

2. Which of the following is not a basic characteristic of information security?
 - a. Confidentiality
 - b. Locality
 - c. Integrity
 - d. Availability

3. Which of the following is an advantage of encryption?
 - a. Prevents deletion of data
 - b. Ensures data integrity
 - c. Doesn't require a password
 - d. Keeps the file author anonymous

4. Which one of the following terms describe the process of someone monitoring you keying in your ATM pin with malicious intent?
 - a. Shoulder surfing
 - b. Phishing
 - c. Cyber bullying
 - d. Hacking

LESSON 2 - MALWARE

In this section, you will learn about:

- Types of malware
- Protection against malware
- Resolving and removing malware

2.1 TYPES OF MALWARE

Definition of Malware

Malware is malicious software that is designed to install itself on a computer or device without the owner's consent. It is used as an umbrella term to describe the following types of malicious software.

Types of Infectious Malware

| | |
|----------------------|---|
| Viruses | Malware that can replicate when triggered by a human action and cause damage to a computer. |
| Worms | Self-replicating malware that uses a computer network to send copies of itself to other computers. |
| Trojan horses | A non-self-replicating malware that pretends to be a harmless application. |
| Rootkits | Malware that enables continued access to computers or devices while hiding their presence. |
| Backdoor | A backdoor is a method of bypassing normal authentication in an attempt to remain undetected. This is usually done in an attempt to secure remote access to the computer. |

Types of Data Thefts

Data theft is the illegal access (reading, editing, or copying) of data without the data owner's authorisation. Data can be stolen in many ways.

Attackers generally use malware for monetary gain. They can use infected computers to generate income in many ways. One of the simplest is through advertising. Just as many of the websites generate income by displaying ads, malware can display ads that result in payments to the cybercriminal.

In some cases, hackers use a group of zombie computers known as a 'botnet' to send a large amount of requests and traffic to a server or website. This can result in the network being inaccessible to normal users. This type of attack is known as a Distributed Denial of Service (DDoS) attack. The attackers then extort money from the owner in exchange for stopping the attack.

Some hackers may also use a type of malware called **Ransomware** that encrypts a user's data and demand payment for them to decrypt the data. Basically, the

user's data is held for ransom. The user is forced to pay the attacker to release the data.

Hackers may use banking Trojans for the purpose of gaining unauthorised access to bank accounts. A banking Trojan is a sophisticated type of malware that allows the attacker to take control of the victim's machine and steal a user's credentials, thereby allowing the hacker to use the victim's identity to perform banking transactions.

Below are a few examples of the way data theft and extortion can happen using malware:

| | |
|------------------|---|
| Adware | A type of software that automatically downloads and displays unwanted ads. It is used by authors to generate revenue and collect data without the victim's knowledge or consent. Some adware may trick users into downloading malware or visiting malicious websites. |
| Spyware | Hackers use spyware to monitor all your activities. Spyware can capture your keystrokes, take screenshots, view your webcam, monitor sites that you visit, and view programs and files that you run on your computer. Spyware could be unintentionally installed when a user clicks on adware or installs seemingly harmless files. |
| Botnet | The term bot is short for robot. Criminals distribute malware that can turn your computer into a bot. When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet. |
| Keylogger | A Keylogger is a hardware or software based tool used to keep track of, or record the keys struck on a keyboard. This is usually done covertly, so as not to alert the user that their keystrokes are being recorded. This allows a hacker to secretly gather confidential data such as passwords and credit card information without the victim's knowledge. |
| Dialler | A dialler is a program that tries to establish a phone connection with a premium-rate number. It infects computers that uses a modem to connect to the Internet, as it modifies the phone and modem configuration, changing the number provided by the ISP (Internet Service provider), which is normally charged at local rates, for an |

expensive premium-rate telephone numbers, often located in small countries far from the host computer. Alternatively, it can dial a hacker's machine to transmit stolen data.

2.2 PROTECTION

Understanding Anti-Virus Software and Its Limitations

Anti-virus software identifies and eliminates various malware by scanning files in your computer system. It is important to have anti-virus software installed on your computer to reduce the threat of malicious and damaging threats to your information and work.

Typically, anti-virus software uses two different techniques to accomplish this:

1. By scanning and examining files on the computer system and comparing them to known malware based on certain virus signatures.
2. By checking programs for various types of bad behaviour which may indicate a new type of virus. This technique is known as "heuristic checking."

Most well-known anti-virus software in the market use both techniques when performing a scan.

Anti-virus software needs an updated list of the newest viruses and other malware in order to be effective in protecting your system. Without this, the software may be unable to detect some viruses. The capabilities of different anti-virus software varies depending on how updated the software is. It is also essential to keep web browsers, plug-ins, applications and operating systems up-to-date as most updates contain bug fixes and measures that will help keep developed viruses and malware from your computer.

Limitations:

- **Anti-virus software features**
Various anti-virus software has different features. The most basic anti-virus software, especially free programs, can be limited because they can only protect computers for certain virus variants but will not protect computers for the more sophisticated ones.
- **Zero-day exploits**
A zero-day exploit is a type of attack on a computer system which has an unknown or undisclosed vulnerability. This type of attack takes advantage

of the fact that there is no known patch for the vulnerability at the time of the attack.

- **Vulnerabilities**

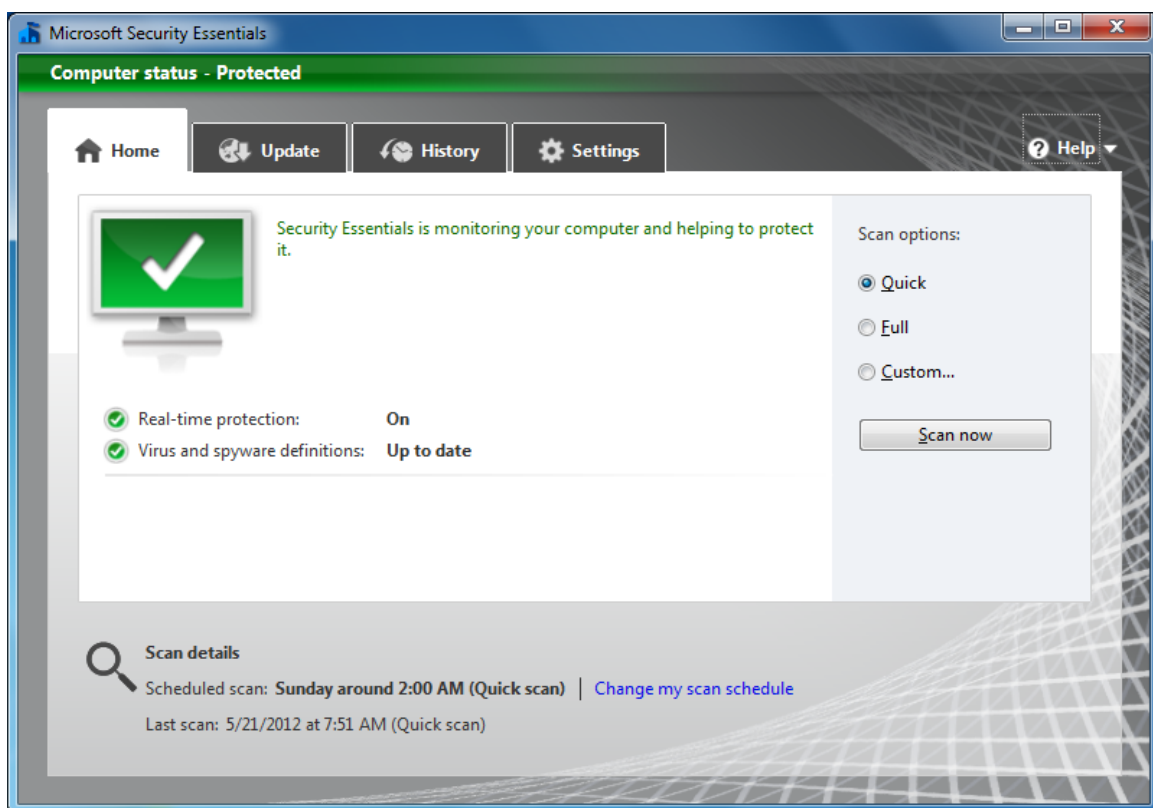
Anti-virus software is also limited because it cannot stop exploits, which attack vulnerabilities or security flaws inherent in the operating systems.

Using an Anti-Virus Software

Software: Microsoft Security Essentials

Scanning

1. Open **Microsoft Security Essentials**.
2. In the **Home** tab, select a **Quick scan** or a **Full scan**.



3. Click **Scan now**.

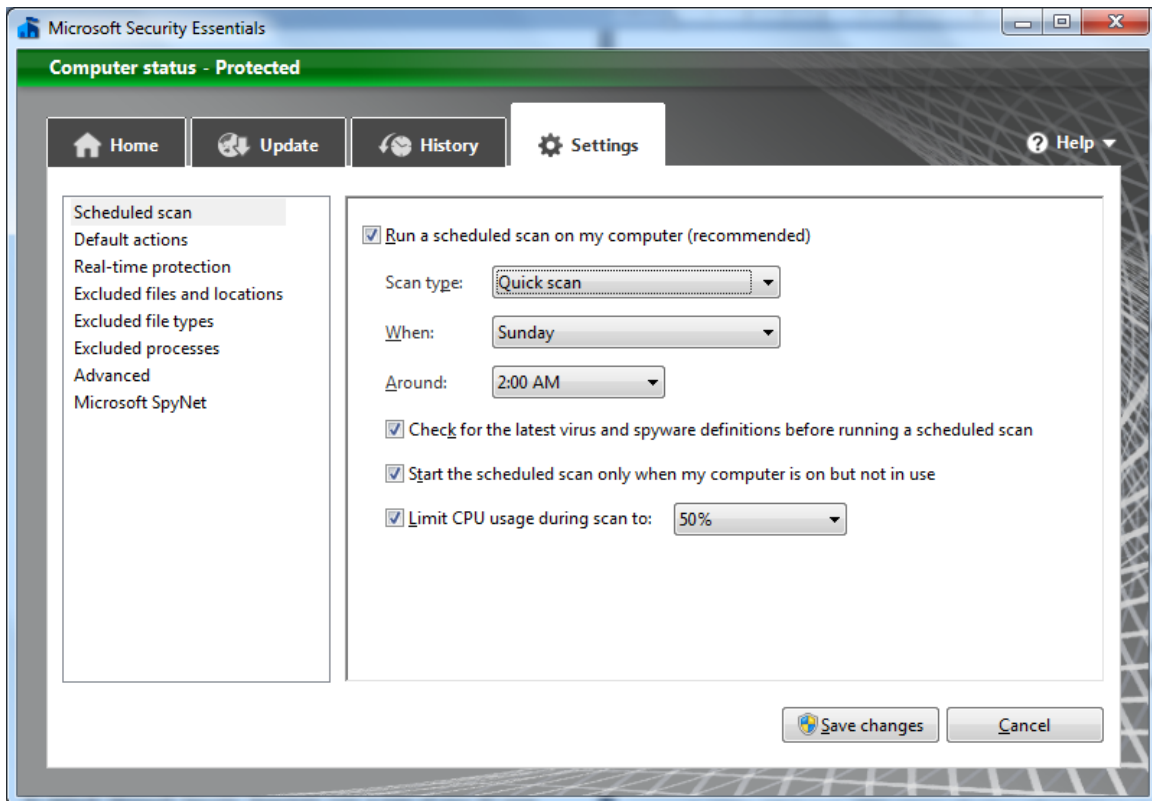
Scanning Specific Drives

1. In the **Home** tab, select **Custom**.
2. Click **Scan now**.
3. Check the required drive and folders.
4. Click **OK**.

Scheduling Scans

By default, Microsoft Security Essentials runs a scan of your computer once a week (2:00 am on Sunday).

1. Click the **Settings** tab.
2. Under **Scheduled scan**, set the type of scan, day and time using the drop down list provided.



3. Click **Save Changes**.

Quarantine Files

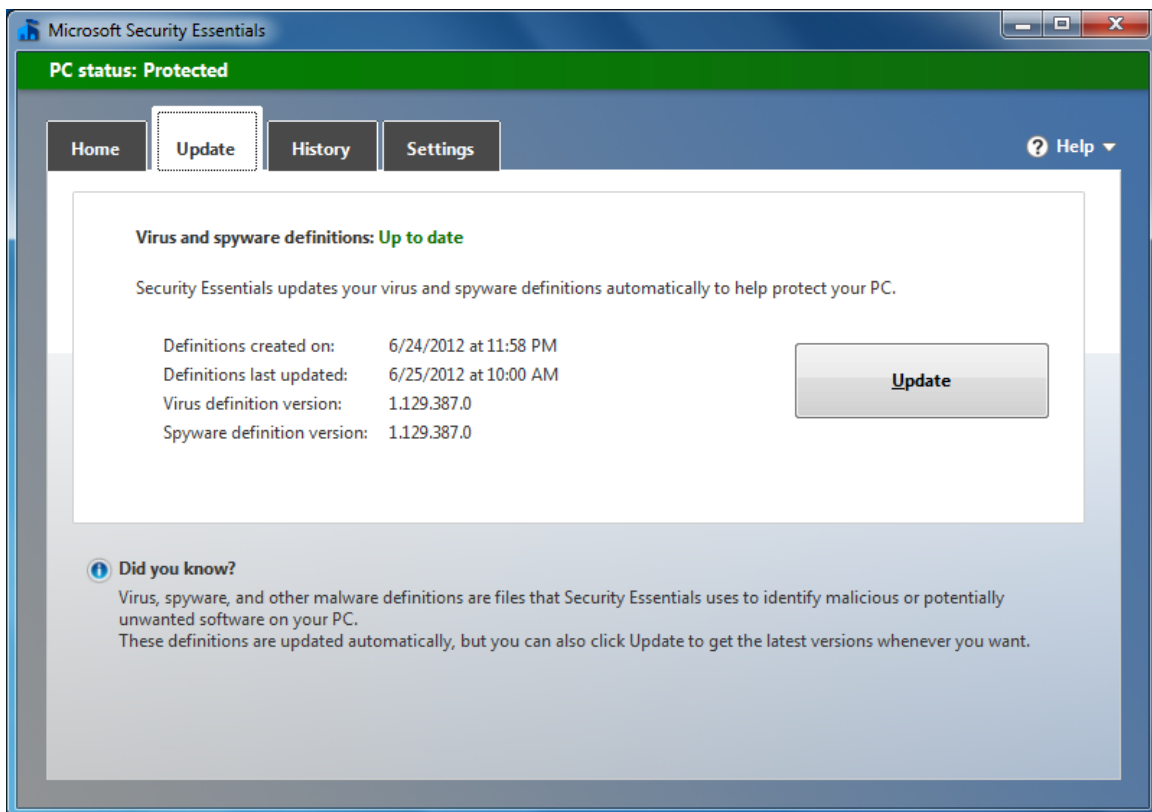
When anti-virus software encounters an infected file, there are generally three options available: clean, quarantine, or remove. Quarantine attempts to move the file to a safe location that is managed by the anti-virus software.

Updating Anti-Virus Software

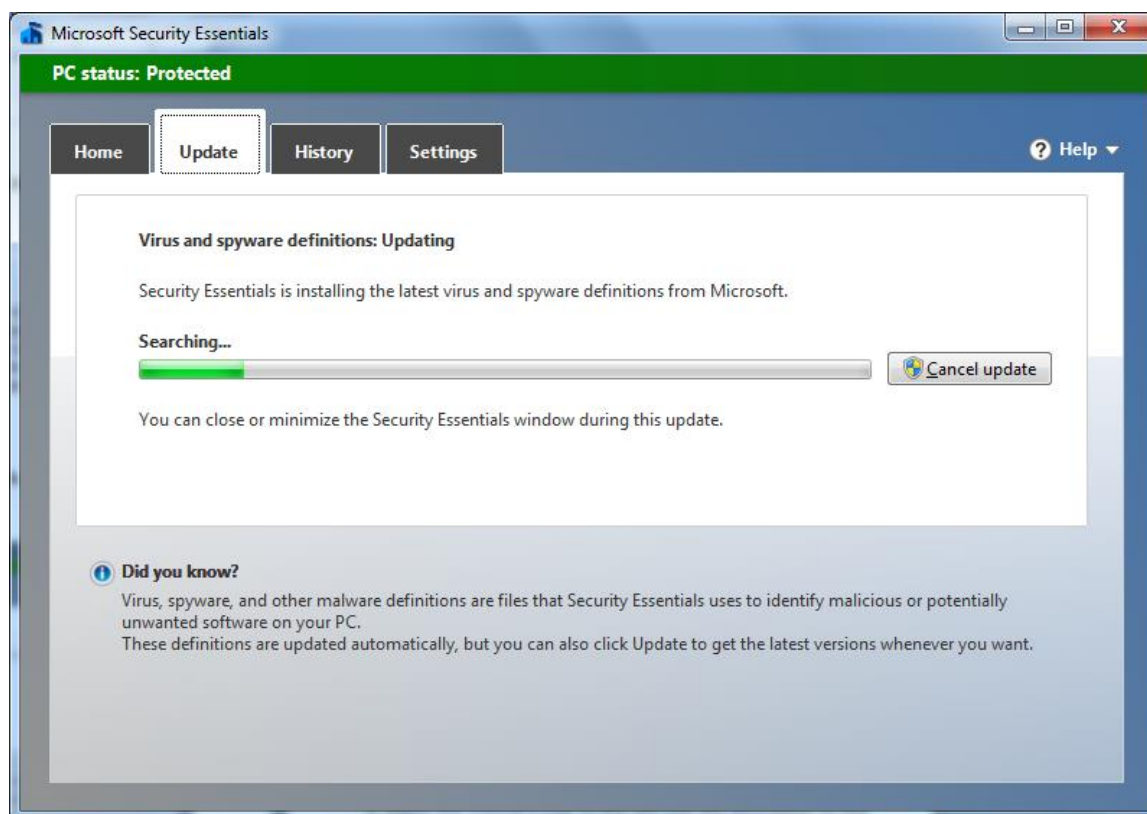
Virus definition file refers to the database of viruses that the anti-virus software uses to identify threats. Updating anti-virus software's virus definition file is important because it will enable the program to detect newer and more complex viruses. Most anti-virus programs may be configured to update automatically, provided there is Internet access.

Updating Virus Definition

1. Open **Microsoft Security Essentials**.
2. In the **Update** tab, click **Update**.



The latest virus and spyware definitions from Microsoft will be installed.



The definitions are by default done automatically.

2.3 REVIEW EXERCISE

1. _____ is created and distributed for malicious purposes.
 - a. Malware
 - b. Firewall
 - c. Anti-virus software
 - d. Database management

2. Which of the following is not a characteristic of spyware?
 - a. Monitor keystrokes
 - b. Obtain information using cookies
 - c. Reconfigure Internet browser settings
 - d. Call numbers without consent

3. A network of infected computers used to distribute malware is known as:
 - a. Robot
 - b. Botnet
 - c. Internet
 - d. Intranet

4. Which one of the following options is not a common option when anti-virus software detects an infected file?
 - a. Quarantine
 - b. Delete
 - c. Open
 - d. Clean

5. Match the malware type on the left with the description on the right.

TROJAN

This virus is so called because it is disguised as a file that a user would be particularly tempted to open e.g. a game or a graphics file

SPYWARE

This is a type of virus that replicates itself within a system so many times that it simply clogs up the system resources.

WORMS

This keeps track of web pages that you look at and then sends the data to a third party.

6. Go to the following web page to use the free Microsoft Safety Scanner tool to scan and remove malicious programs from your computer's security profile:

<http://www.microsoft.com/security/scanner/en-us/default.aspx>

LESSON 3 – NETWORK SECURITY

In this section, you will learn about:

- Networks and connections
- Wireless security

3.1 NETWORKS AND CONNECTIONS

A computer network is a group of two or more computer systems linked together by communication channels to allow for sharing of resources and information.

The devices on a network are called nodes. Nodes can be connected using any of various types of connecting media, including twisted pair copper wire cable, optical fibre cable, coaxial cable and radio waves.

Common Network Types

- **LAN** (Local Area Network)

A local area network is the smallest type of network, usually extending over a small area within a building. When users connect their computers to the LAN, they can access shared resources such as Internet connection, network drives, printers as well as other user's computers.

When logging-on to a LAN, user's need to input their user name and password. Once authenticated, they are able to access the services on the network depending on the type of permissions assigned to their account. This ensures that users are only able to access files, folders and services that they are given rights to access.

- **WAN** (Wide Area Network)

Wide area networks (WANs) can extend over a large geographic area and are connected via the telephone network or radio waves. Many modern companies have offices, shops or factories in various locations around the country, and for large corporations, across the world. Even though the staffs work in different places, they often need to be able to access the same information no matter where they are. By linking LANs together, the network is no longer local to one building; it is now spread over a wide area. It is known as a WAN.

So basically a WAN is where individual computers or LANs which are a long distance apart from each other are connected together. They generally will not share hardware or software, unlike a LAN. The largest WAN in existence is the Internet.

- **WLAN** (Wireless Local Area Network)

A wireless local area network or WLAN allows mobile users to connect to a local area network via a wireless (radio) connection. It provides a link between two or more devices within a limited area such as an office, home, school or office building.

- **VPN** (Virtual Private Network)

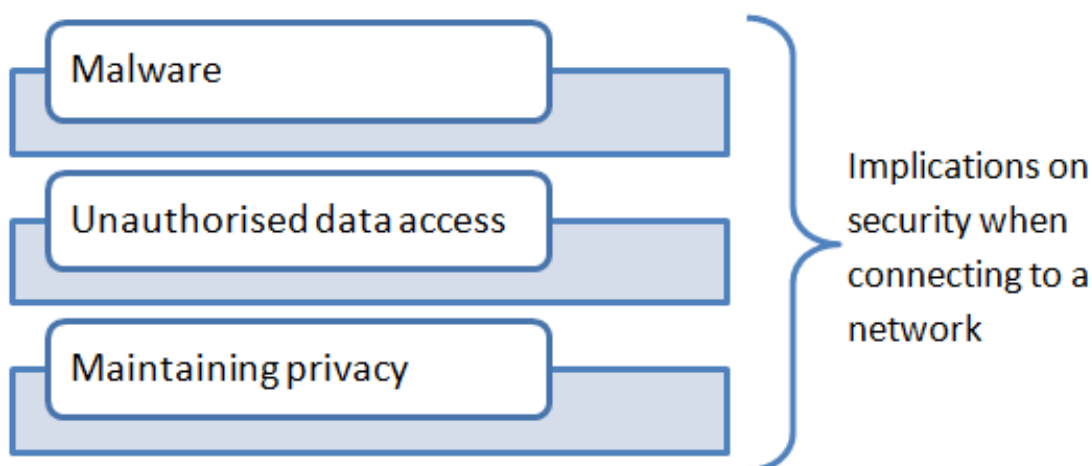
A virtual private network (VPN) allows users to access their private network over the internet. Users can access their shared network resources, printers, intranet sites, databases and other services in their organisation remotely through an encrypted connection. This allows the users to send and receive data as if they were directly connected to the private network. A VPN typically uses encrypted traffic and tunnelling protocols to establish a virtual point-to-point connection between the user and the private network.

Security Implications of Connecting to a Network

Devices can connect to a network through:

- Network cable connections
- Wireless Access Points.

Anyone can connect an unsecured device to an unsecured network and can gain access to the resources and data. This compromises the devices that are on the network, including servers.



- **Malware**

The interconnectivity of devices on networks allows for malware and viruses on an unprotected device to spread to other devices easily through an unsecured network.

- **Unauthorised data access**

An intruder or hacker can gain access to the network and may read its unprotected data. As a result, confidential or sensitive data can easily be compromised, exposing, for example, intellectual property of the organisation's members to the public.

- **Privacy**

Connecting your device to a network may open up the possibility our information held on your device being accessed by other network users.

Proper network security implementation will reduce or eliminate these threats.

Role of the Network Administrator

A network administrator is a person responsible for the maintenance of computer hardware and software that comprises a computer network. This normally includes deploying, configuring, maintaining and monitoring active network equipment. An important component of the role of network administrator relates to security.

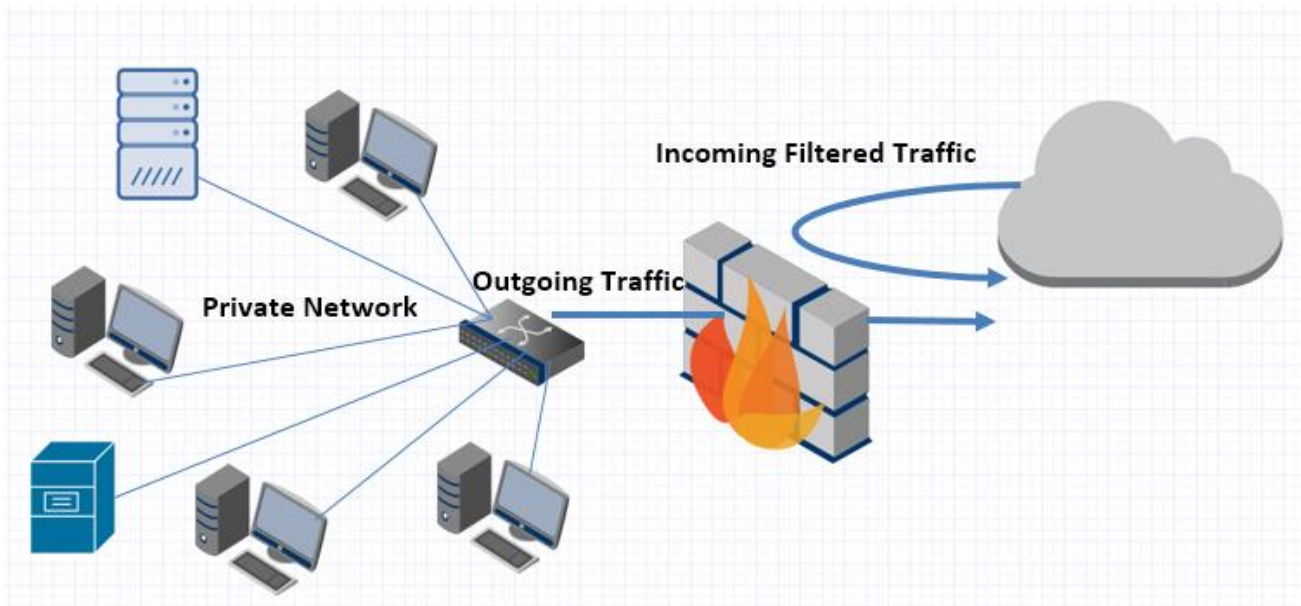
Security-related activities include:

- Managing authentication and authorisation of user accounts on the network.
- Maintaining staff access to required data on the network and ensuring network usage is in line with ICT policies.
- Monitoring and installing relevant security patches and updates, monitoring network traffic, and dealing with malware found on the network.

Function and Limitations of a Firewall

A firewall is a program or a hardware device that can be used to help protect a network from hackers who might try to break in and gain access to your data. The firewall filters the information coming through the Internet connection into your personal computer or into a company's network.

Firewalls serve as a barrier between the internal network and an external network such as the Internet. When any traffic from outside the network tries to access the internal network, the firewall checks against a set of rules. Any data coming from an unauthorised source is blocked by the firewall.



It is essential that anyone who has access to the Internet makes sure that they have a firewall installed. However, despite its necessity there are some limitations to a firewall:

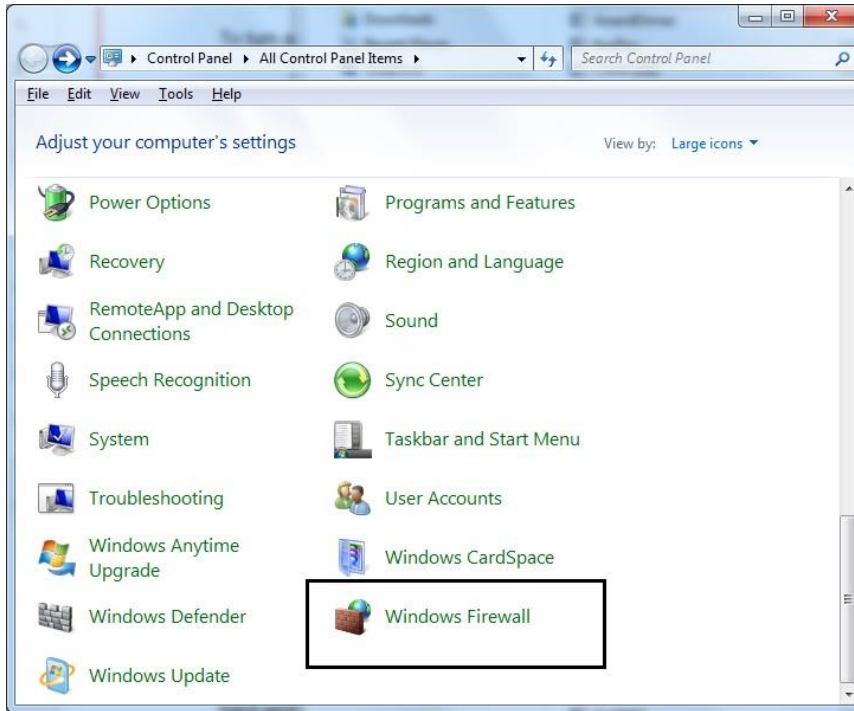
- **Viruses**
Not all firewalls offer full protection against computer viruses as there are many ways to encode files and transfer them over the Internet.
- **Attacks**
Firewalls cannot protect against attacks that do not go through the firewall. For example, firewall may restrict access from the Internet, but may not protect equipment from dial-in access to the computer systems, or user connecting their infected laptops and other mobile devices to the company's network.
- **Monitoring**
Some firewalls can notify if a perceived threat occurs, but may not notify if someone has hacked into the network. Many organisations find they need additional hardware, software and network monitoring tools.

It is possible to turn a personal firewall on or off, although turning it off is not recommended. You can also block an application, service or feature from getting access through a firewall.

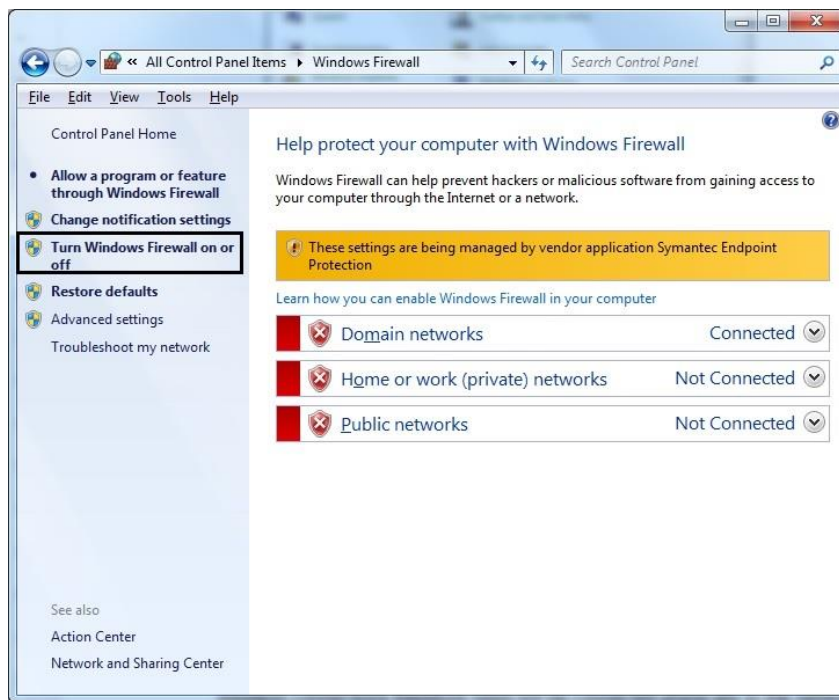
To turn a personal firewall on/off:

1. Click the **Start** button.
2. Click **Control Panel**.

3. Click the **Windows Firewall** button.



4. In the left panel, click **Turn Windows Firewall on or off**.

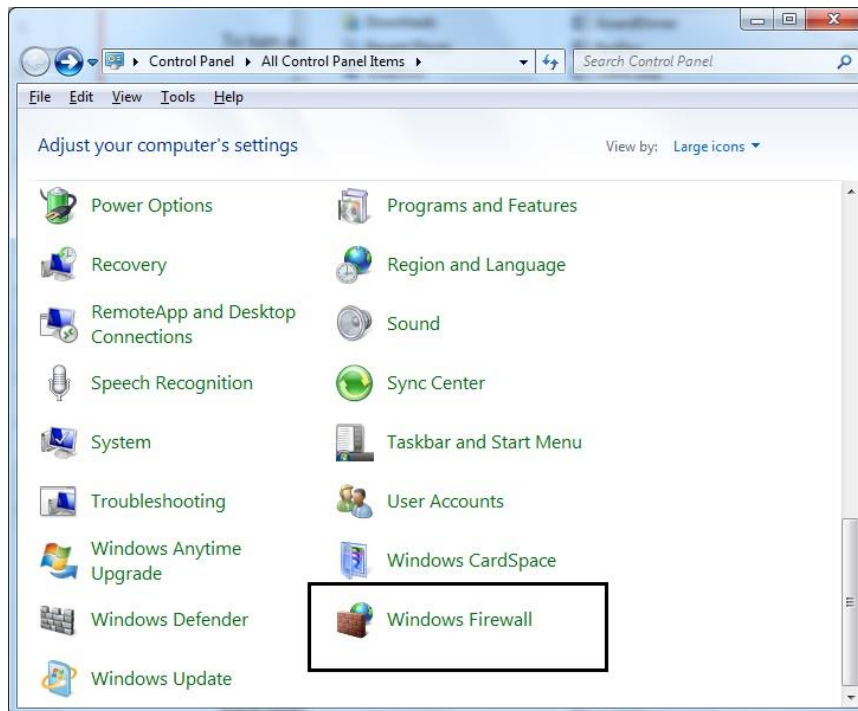


5. Click the appropriate option.

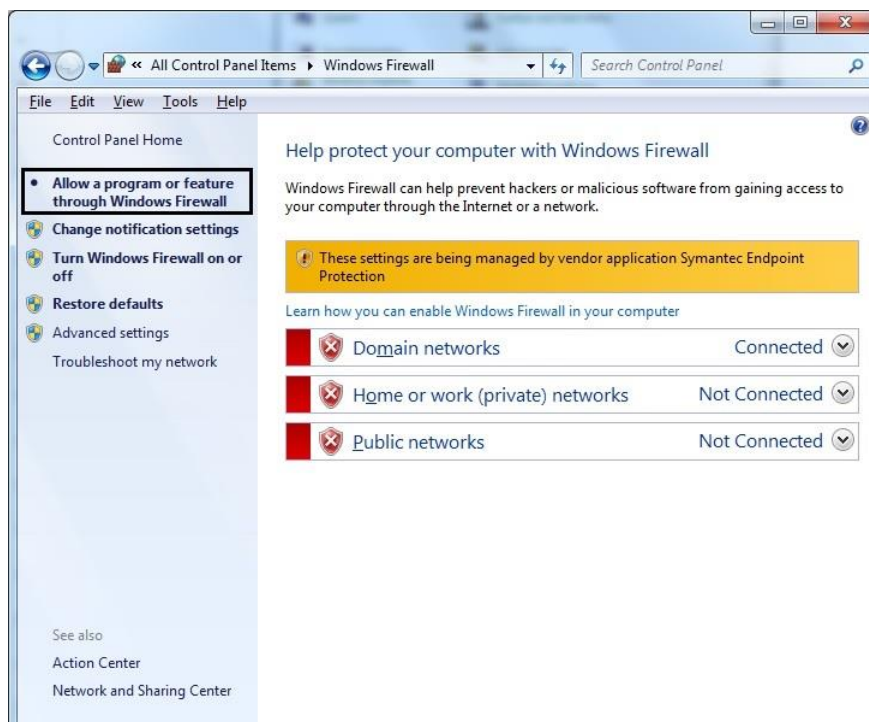
6. Click **OK**.

Allow an application, service/feature access through a personal firewall:

1. Click the **Start** button.
2. Click **Control Panel**.
3. Click the **Windows Firewall** button.



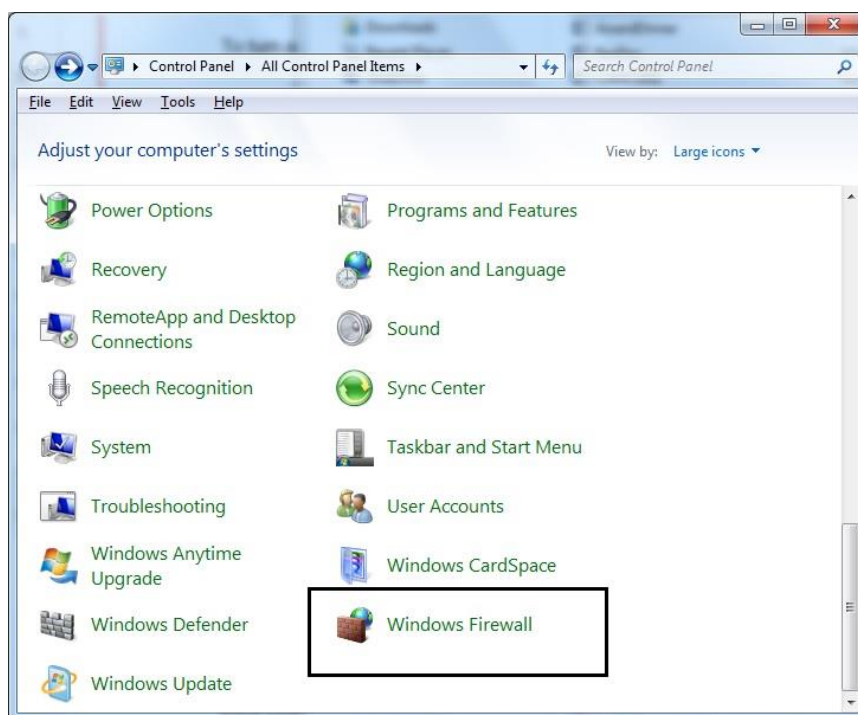
4. In the left panel, click **Allow a program or feature through Windows Firewall**.



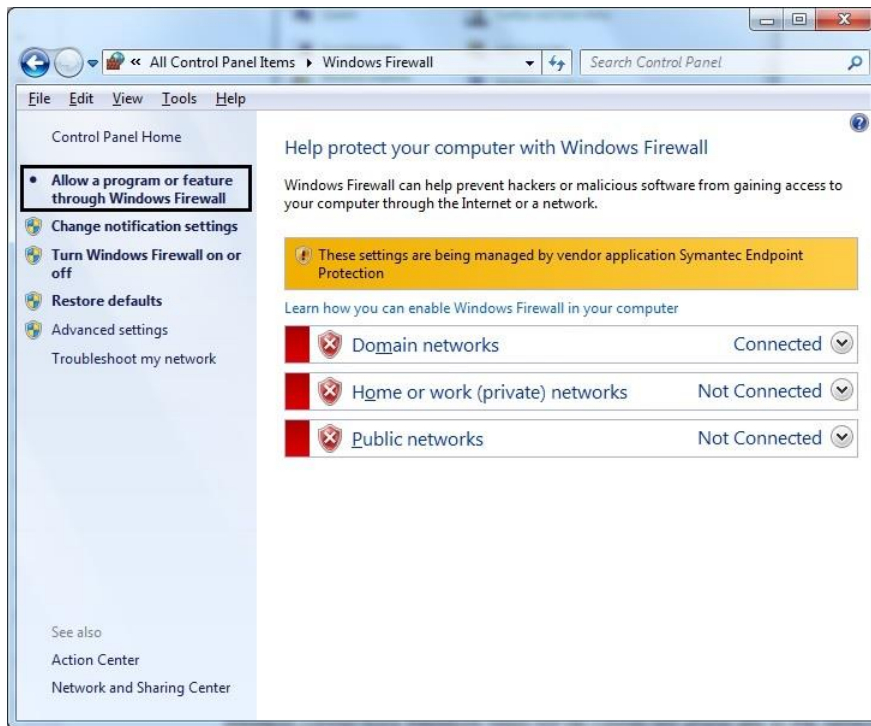
5. Click **Change Settings**.
6. Check the check box next to the program or feature you want to allow.
7. Check the check box of the network locations you want to allow communication on.
8. Click **OK**.

Block an application, service/feature access through a personal firewall:

1. Click the **Start** button.
2. Click **Control Panel**.
3. Click the **Windows Firewall** button.



4. In the left panel, click **Allow a program or feature through Windows Firewall**.



5. Click **Change Settings**.
6. Uncheck the check box next to the program or feature you want to block.
7. Uncheck the check box of the network locations you want to block communication on.
8. Click **OK**.

3.2 WIRELESS SECURITY

Wireless networks can be a convenient way to connect to the Internet, especially with mobile devices like laptop computers or tablets. When searching for available wireless networks, some connections are unsecured and others are secured networks. Unsecured networks do not require any form of authentication to connect any device to the wireless network, which can enable unrestricted access to other devices' data and resources. Wireless connections have the same security issues as hard-wired connections. Wireless connections however, do not have the same physical restrictions like hard-wired connections, which requires two devices to be physically connected.

Due to this there are potential risks associated with using an unprotected wireless network, such as:

- **Eavesdroppers** – Other people accessing and reading your data to find sensitive or confidential information.

- **Network hijacking** – Other people taking control of network communications.
- **Man in the middle** – Other people observing communications and collecting data that is transmitted.

Secured networks are those that have been set up with security passwords and encryption by the network administrator. The password of a secured network is required before logging on.

Types of Wireless Security

Implementing wireless security prevents unauthorised access to a wireless network and connected devices.

Common types of wireless security options include:

- **Wired Equivalent Privacy (WEP)**
WEP is a type of security standard used by wireless networks. It is still used to support older devices, but its use is no longer recommended. WEP uses a network key to encrypt information sent from one computer to another across a network. The encrypted information sent using this standard is relatively easy to crack.
- **Wi-Fi Protected Access (WPA)**
WPA encrypts information that is exchanged between two connected devices and it also ensures that the network security key is not easily obtained. WPA also authenticates users and only authorises these authenticated users to connect to the wireless networks and exchange data with other devices on that network.

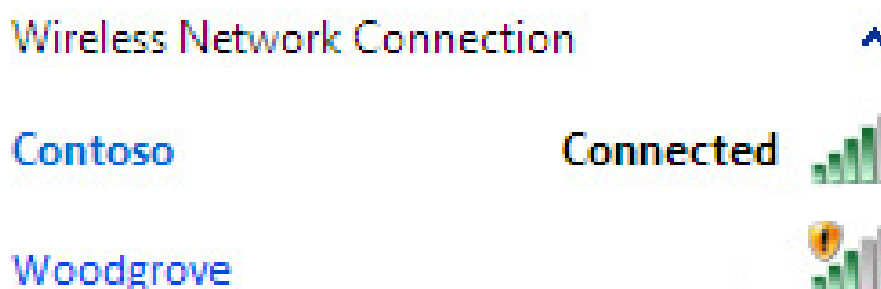
There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters. WPA2 is more secure than WPA, but it might not work with older routers or access points and some older network adapters.

- **Media Access Control (MAC) Address Filtering**
Each network interface controller (network adapter) has a unique 48 bit hardware identifier (MAC address). This value can be set into the allowed filter list of the wireless point's security setting, thus only connection from these devices is allowed. However, a hacker could set a valid address on his device to connect and gain access to the network. Also, it may be difficult to maintain a list of permitted MAC addresses.
- **Service Set Identifier (SSID) hiding**
Each wireless access point has a Service Set Identifier (SSID) which is broadcasted without restrictions to allow wireless devices to search and identify the wireless networks that are available. Wireless devices use this SSID to create a connection through the access point to the wireless network. Hiding the SSID makes this access point invisible to every device. Without knowing the SSID, a person will not be able to connect to

the network; only a person who knows the hidden SSID can set up a connection to the wireless network. However, software utilities can be used to reveal hidden SSIDs.

Public wireless network that allows access to the Internet or the network are convenient, but connecting to one might be risky if they are not properly secured. Whenever possible, only connect to wireless networks that require using a network security key or have some form of security, such as a digital certificate for authentication, before one is allowed to connect to the network. These requirements prevent unknown users from connecting and compromising the network and devices connected to that network.

In the list of available wireless networks, each unsecured network wireless access (or connection) point is labelled; this means that the SSID is not hidden. If you do connect to a network that is not secure, be aware that someone with the right tools can see everything that you do, including the websites you visit, the files you send and receive, and the user names and passwords you use.



Using Personal Hotspots

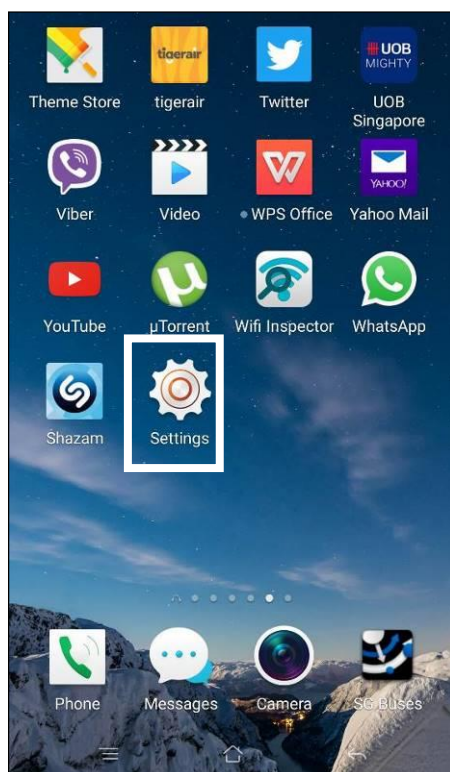
A personal hotspot provides a way for users to share an Internet connection using a smartphone or tablet. Most current mobile devices have this feature available. Enabling this feature on a mobile device turns the device into a wireless access point, similar to a Wi-Fi access point. Devices with Wi-Fi radio will be able to access the personal hotspot as long as it is within range.

A personal hotspot has some limitations and constraints compared to a Wi-Fi access point. For instance, the number of simultaneous connections to a personal hotspot is limited. Also, data transferred on the personal hotspot from the Internet may count against the smartphone's data plan.

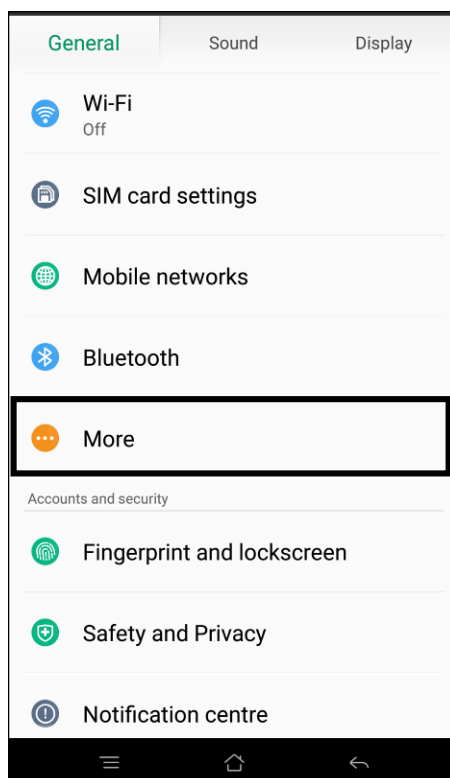
Enabling/Disabling a Personal Hotspot (Smartphone)

Enabling Personal Hotspot (Android):

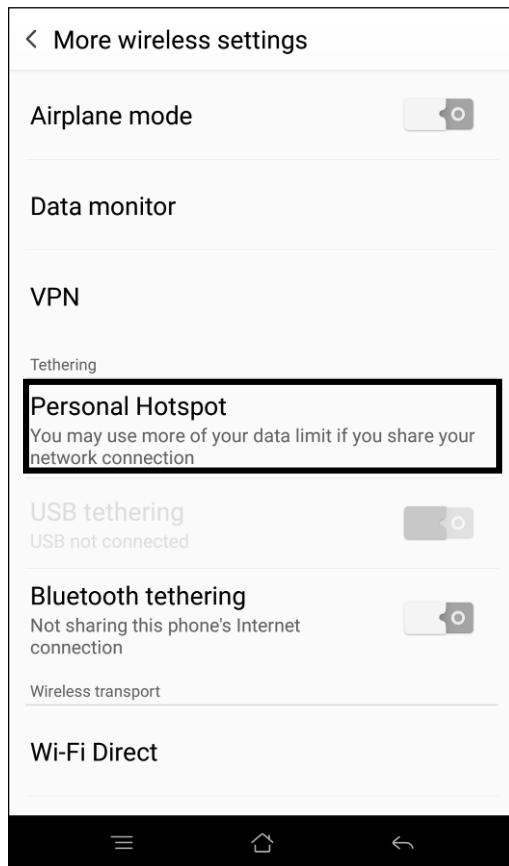
1. Select the **Settings** icon.



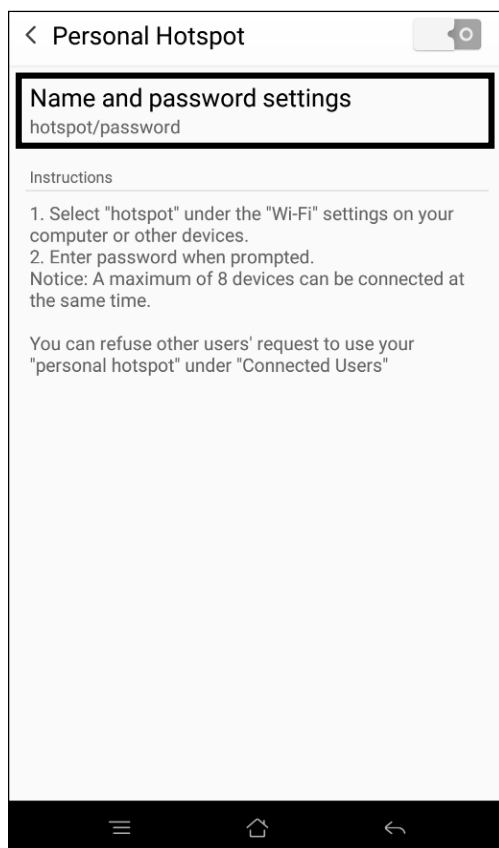
2. Select **More**.



3. Select **Personal Hotspot**.



4. Select Name and password settings.



5. Enter a name and password for the hotspot.

Name and password settings

Name (SSID)

Encryption
 WPA2 PSK

Password

The password must have at least 8 characters.

Show password

Save Cancel

6. Press **Save**.

7. Press the **on/off switch**.

< Personal Hotspot

Name and password settings
 Red Knight/password

Instructions

1. Select "Red Knight" under the "Wi-Fi" settings on your computer or other devices.
2. Enter password when prompted.

Notice: A maximum of 8 devices can be connected at the same time.

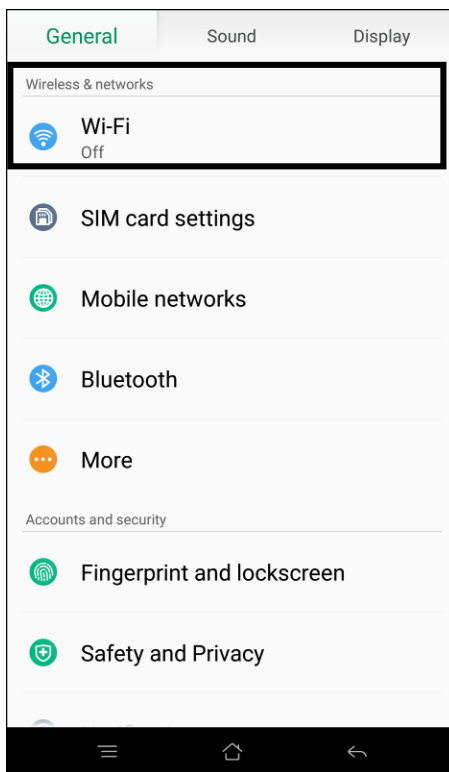
You can refuse other users' request to use your "personal hotspot" under "Connected Users"

Connecting to a Personal Hotspot:

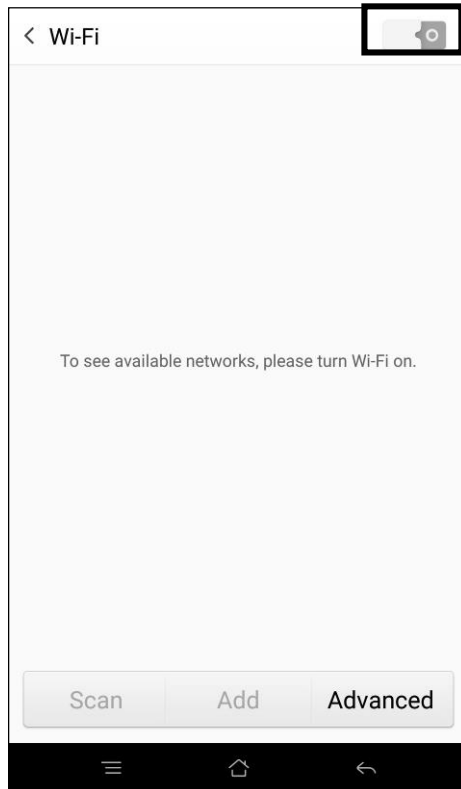
1. Select the **Settings** icon.



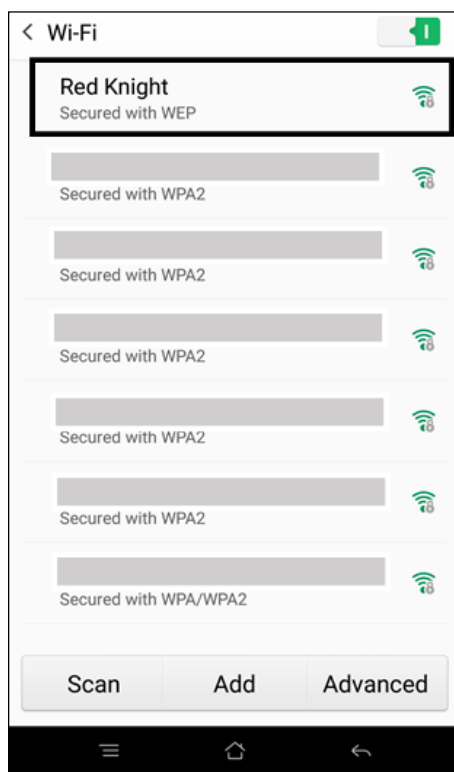
2. Select **Wi-Fi**.



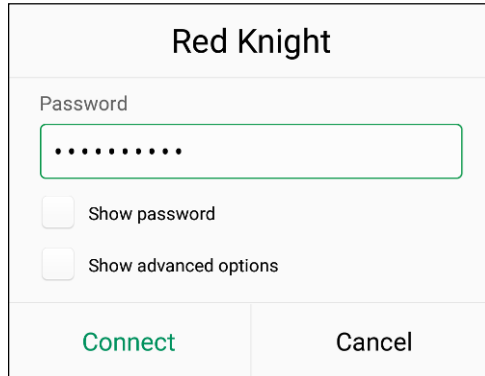
- 3. Press the on/off switch.



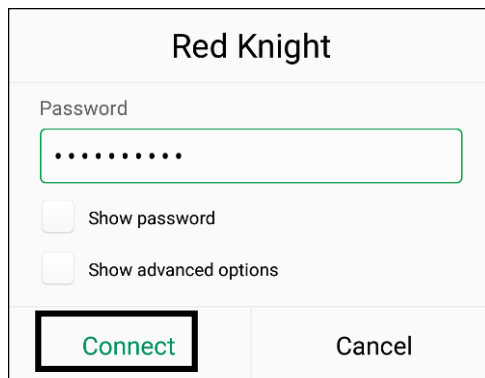
- 4. Select the name of the hotspot.



5. Enter the password.



6. Press **Connect**.

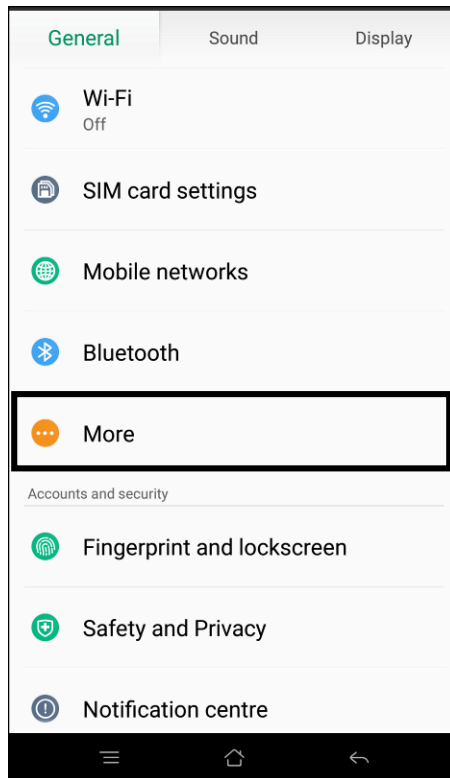


Disabling a Personal Hotspot

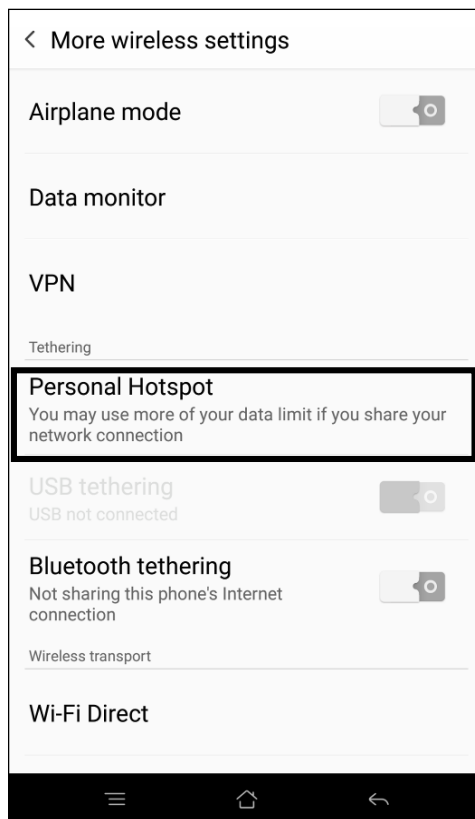
1. Select the **Settings** icon.

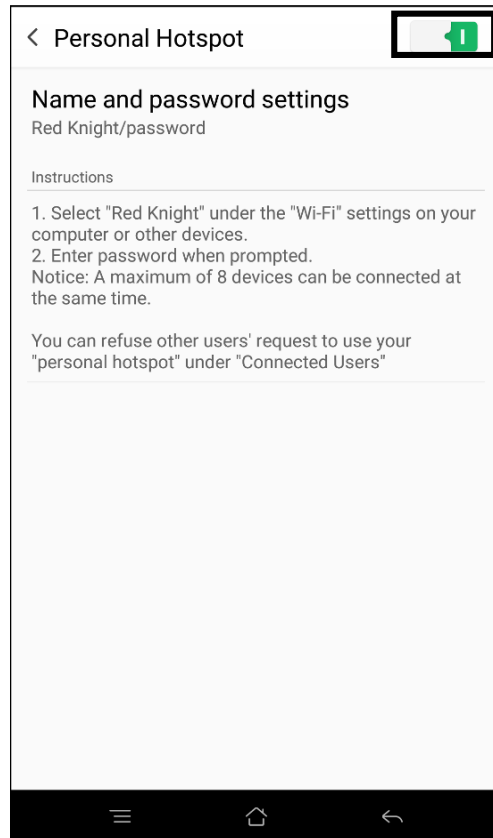


2. Select **More**.



3. Select **Personal Hotspot**.



4. Press the **on/off switch**.

It is possible to enable a secure hotspot using an iOS device by following similar steps to those listed above. This is done by going to **Settings > Personal Hotspot >** and turning the Personal Hotspot slider **On** or **Off**. Devices can connect to the hotspot through Wi-Fi, Bluetooth, or USB.

3.3 REVIEW EXERCISE

1. Which of the following is not a type of network?
 - a. WAN
 - b. WAP
 - c. LAN
 - d. VPN

2. Which of the following is not a feature of a firewall?
 - a. Reduces potential for malware intrusion
 - b. Blocks data from unauthorised source
 - c. Encrypts information
 - d. Filters incoming information

3. List 2 security implications of connecting to a network.

4. In wireless security, WPA is:
 - a. Work Protocol Access
 - b. Wireless Protected Access
 - c. Wi-Fi Protocol Access
 - d. Wi-Fi Protected Access

LESSON 4 – ACCESS CONTROLS

In this section, you will learn about:

- Access control methods
- Password management

4.1 METHODS

Preventing Unauthorised Data Access

Hackers are constantly looking for ways to steal private and confidential information, and to attack networks and computer systems for personal gain. There are many ways to ensure that users are protected from various malware attacks or theft of private information. Below are some of the ways you can prevent unauthorised access to your computer systems.

Passwords

Passwords need to be set for all of the network's computer systems. This helps ensure that only authorised users are able to access the computer system and network.

Password policies must be strictly enforced in order to prevent password cracking and theft of login credentials.

PIN (Personal Identification Number)

A PIN is a type of numeric password that is used by user to login to a system. It usually used in association with debit cards or ATM cards.

This type of password is also used for other purposes such as unlocking doors or mobile devices like smartphones and tablets.

Encryption

Encryption is a process that encodes data or information so that only authorised users can read the information. In the event that the data is intercepted by an unauthorised user, the interceptor will need to decrypt the data first before he is able to read it.

In the encryption process, the plain-text data is encrypted using an algorithm to generate cipher text which can only be read if decrypted. A key is provided by the originator of the data to the authorised recipient. The authorised user can then use the key to decrypt the data and read the information.

Multi-factor authentication

With Multi-Factor Authentication, users are only granted access to a system when they successfully present two or more forms of authentication methods.

Typically, at least two of the following types of authentication are required:

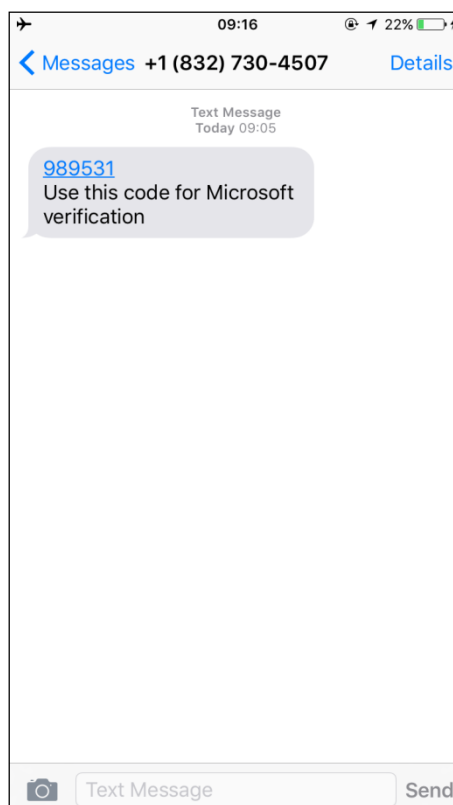
- Something they know – use of passwords, PIN, pattern.
- Something they have – use of Tokens, ID cards, Scan cards.
- Something they are – uses biometric security techniques such as face recognition, fingerprint scanners, voice recognition and iris scanners.

One-Time Password

A one-time password (OTP) is a type of password that is valid for only one transaction or log-in session. This type of password can only be used once within a limited period of time, usually lasting a few minutes. Unlike traditional static passwords, even if a hacker is able to record the one-time password, it cannot be reused since it will no longer be valid once the authorised user logs into the system.

One-time passwords are commonly required for online banking transactions.

For example, an SMS notification may be used to log into an online banking service.



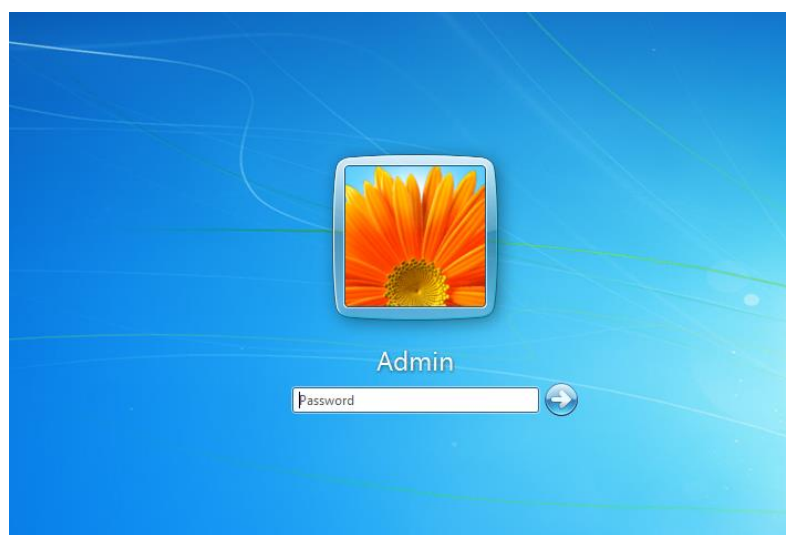
Another way of generating an OTP is using a security device, such as that shown below, which generates a random PIN that acts as a second level of authentication.



Network Accounts

A network account is needed for a user to access the network. A user is assigned rights and permissions along with the network account. This determines what the user can do on the network.

If your network account is part of the Administrators group, you will be allowed to add users to your computer as well as add users to a group in Windows. It is recommended that you log off from a network account when you are not using it to prevent any accidental or intentional damage being done to data.



Windows log in screen

Biometric Security Techniques

Biometric authentication is a security method used to protect physical and digital data. Fingerprints, irises, retinas, speech, facial features and other aspects of behaviour and physiology are all used in biometric authentication to administer

access to a computer system or physical space. Fingerprint scanning, facial recognition, and voice recognition are three biometric authentication techniques that individuals, corporations, and military facilities frequently use.

- **Fingerprint Scanning**

Fingerprint scanners are sometimes used on laptop and desktop computers and flash drives. Fingerprint authentication is the most popular and least expensive method to authenticate using biometrics.

Fingerprint readers or scanners record the unique series of lines, whorls, and arches that make up your fingerprint, allowing only prints with a statistically significant match to log on to a system or network.

- **Hand Geometry**

Hand geometry identifies a user by measuring their hand along many dimensions and comparing these with stored measurements. It has been used since the 1980s, meaning it was the first biometric in widespread use.

Although it is still a popular option, other biometric methods such as fingerprint scanning have overtaken it.

- **Facial Recognition**

Facial recognition authentication is a security technique that records and measures your facial features such as the distance between your eyes, the height of your cheekbones, and additional characteristics. Facial recognition systems can offer a heightened level of security only if the template image is effectively captured. For this reason, if you use facial recognition security software, be sure the template images are created using proper lighting and focus.

- **Voice Recognition**

This security technique works by matching the pattern of a person's voice to a template recording. Voice recognition is not the same as speech recognition, in that the words being said are not as important as the way in which they are said.

One problem with voice recognition security software is that it does not account for voice changes due to emotional states, sickness or other reasons.

4.2 PASSWORD MANAGEMENT

Good Password Policies

In order to protect computer systems from unauthorised usage and data theft, a good password policy must be put in place and continuously practiced by all users. A good password policy should include the following guidelines:

- Always use complex passwords of at least 8-12 character length, which include upper and lowercase, numbers, and special characters.
- Avoid words found in the dictionary.
- Change passwords on a relatively regular basis.
- Avoid using passwords that include your personal information, such as your name, birthdate, or spouse name.
- Never keep default user names and passwords such as “admin”, “root” or “password.”
- Consider using a password manager software instead of, for example, writing down passwords on sticky notes.
- Do not use the same password for different services.
- Do not divulge or share your password with anyone.

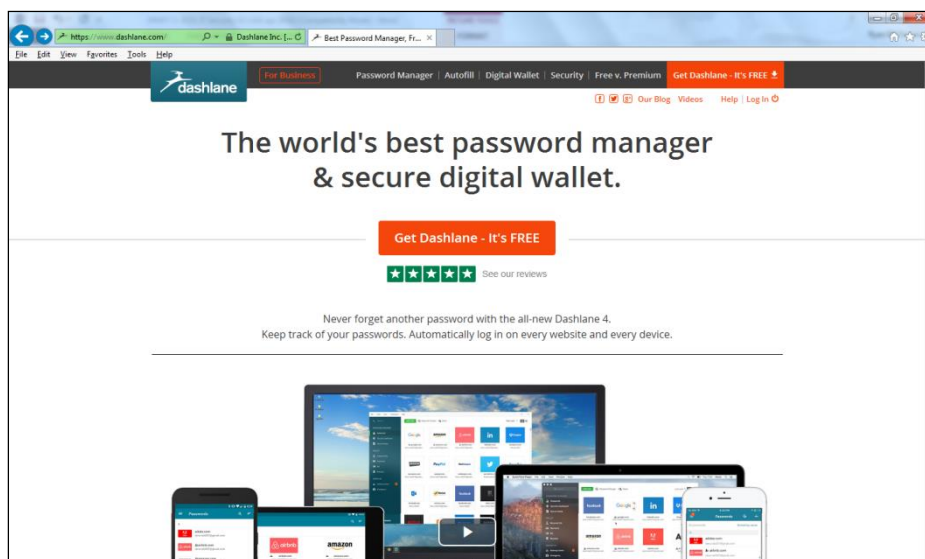
Password Management Software

A password manager helps you store login information to various sites and helps you login to those sites automatically. Some password managers may also allow you to generate complex passwords.

Despite their convenience, password managers have been criticised. If the password used to access the password manager is compromised, access will be given to all of a user’s passwords. To many they are a useful tool, but be aware that they are not infallible.

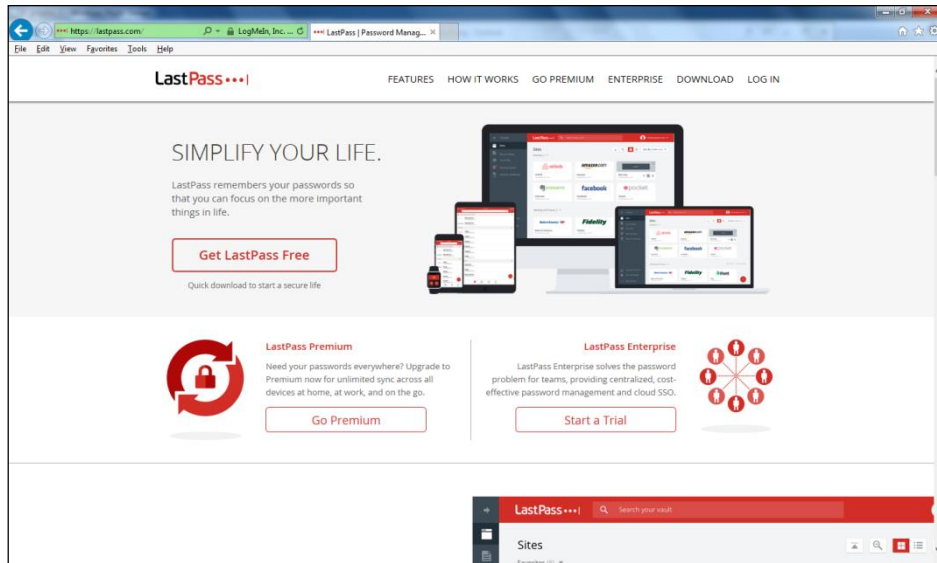
Different Password Managers include:

Dashlane



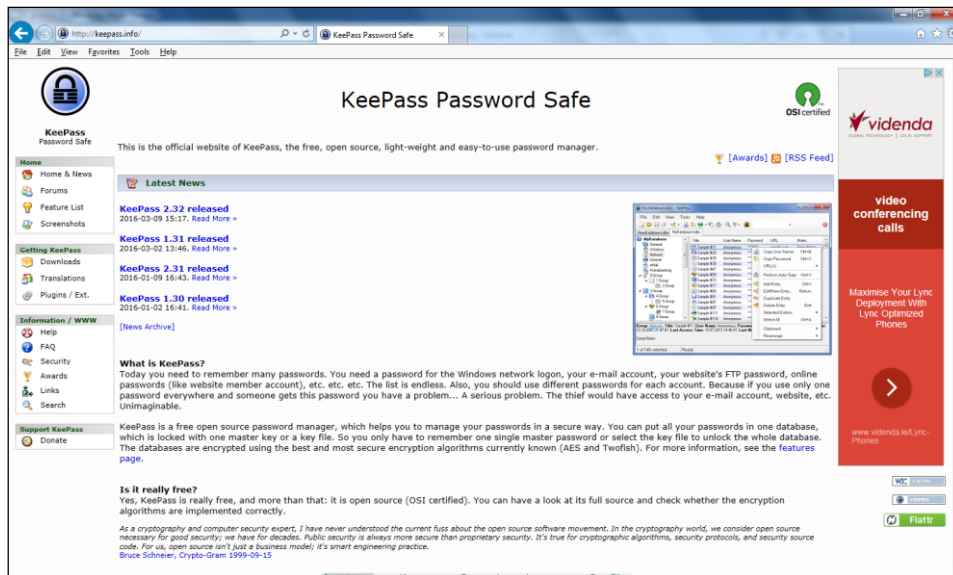
<http://www.dashlane.com>

LastPass



<http://www.lastpass.com>

KeepPass



<http://www.Keepass.info>

4.3 REVIEW EXERCISE

1. Which of the following is not a type of authentication?
 - a. Something I know
 - b. Something I have
 - c. Something I am
 - d. Something I believe

2. When data has been encrypted, what does the recipient need to read the data?
 - a. A password
 - b. A key
 - c. A confirmation e-mail
 - d. None of these

3. Which of the following is not a biometric security method?
 - a. Fingerprint scanning
 - b. Facial recognition
 - c. One time password
 - d. Voice recognition

4. Go to the following web page to test how secure your password is:

<http://howsecureismypassword.net/>

Example: Tested with the password “password”.

HOW SECURE IS MY PASSWORD?

Common Password: In The Top 10 Most Used Passwords
Your password is very commonly used. It would be cracked almost instantly.

Possibly A Word
Your password looks like it could be a dictionary word or a name. If it's a name with personal significance it might be easy to guess. If it's a dictionary word it could be cracked very quickly.

Character Variety: Just Letters
Your password only contains letters. Adding numbers and symbols can make your password more secure.

LESSON 5 – SECURE WEB USE

In this section, you will learn about:

- Browser settings
- Secure browsing

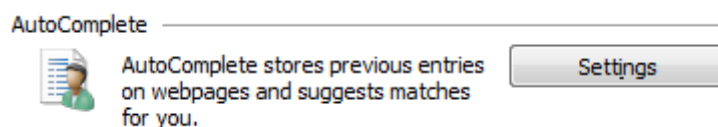
5.1 BROWSER SETTINGS

Setting AutoComplete Options

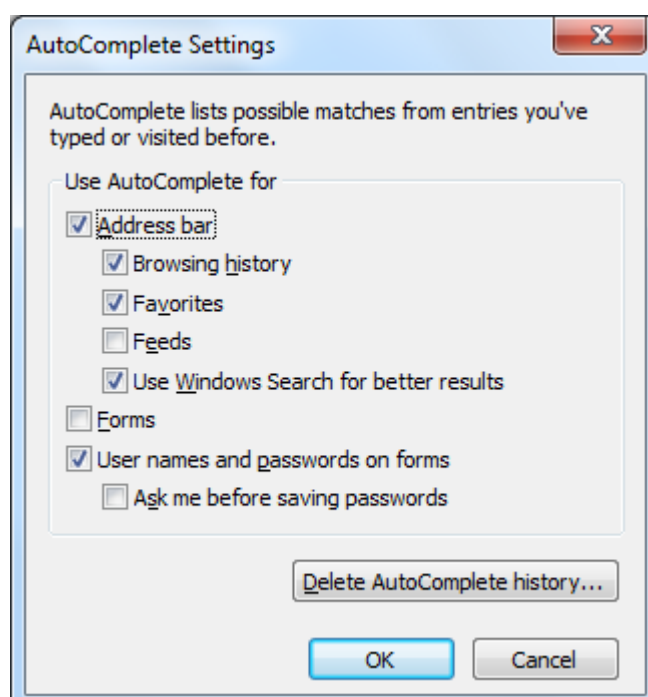
Most browsers have an AutoFill or AutoComplete feature which allows you to save usernames, passwords and other information, which you can then use to automatically fill-in online forms. For example, when logging-in to a frequently used web site, your username and password is automatically filled in for you when the web page is loaded. This is a time-saving feature when used on personal computers.

However, when using a shared or public computer, you do not want this information to be saved for anyone to use. In this situation, you will want to disable certain AutoComplete features.

1. In **Internet Explorer**, click on **Tools** menu.
2. Click on **Internet Options**.
3. Select the **Contents** tab.
4. Click on the **Settings** buttons in the **AutoComplete** section.



5. Check or uncheck the appropriate options.



6. Click **OK** to close the **AutoComplete Settings** dialog box.
7. Click **OK**.

Clearing Private Data from Browser

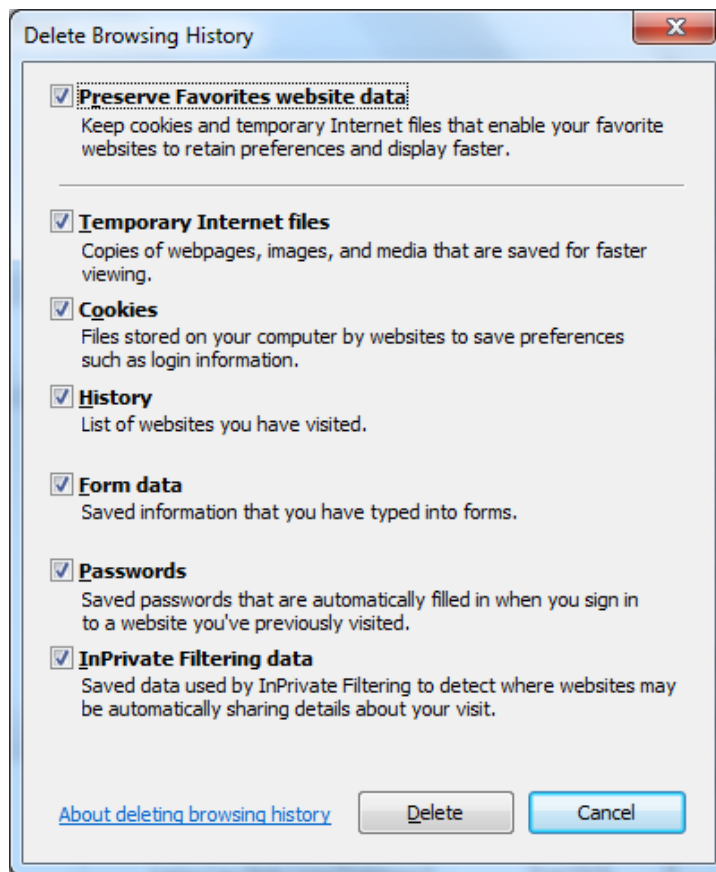
Internet Explorer stores information about the websites you visit, as well as information that websites frequently ask you to provide (such as your name and address).

Internet Explorer stores the following types of information:

- Temporary Internet files.
- Cookies.
- A history of the websites you've visited.
- Information that you have entered into websites or the Address bar.
- Saved web passwords.

If you are using a public computer and do not want any of our personal details to be left behind, you need to delete that information.

1. In Internet Explorer, click on **Tools** menu.
2. Click on **Delete Browsing History**.

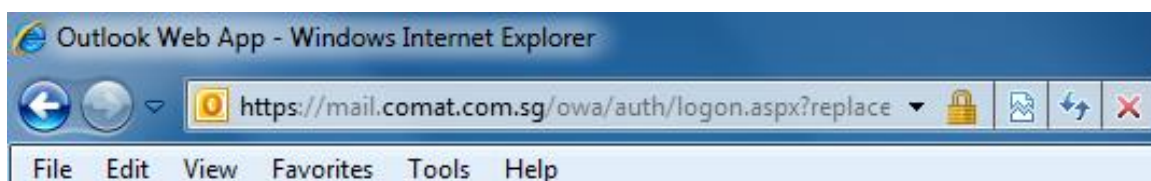


3. Select the required options to clear.
4. Click **Delete**.

5.2 SECURE BROWSING

Anytime a web page prompts you for sensitive information, you need to be able to identify if the page is secure or not. The ability to recognise a secure web connection is extremely important as online fraud cases have increased substantially from year to year.

Online activities such as online shopping or financial transactions should only be undertaken on secure web pages.



You can use the following measures to review a website’s safety:

- **Content Quality and Currency**
The quality of the content is often a good indicator as to whether a website is legitimate or not. This can include grammar and whether written material is error-free, as well as the currency of the material. If a website hasn't been updated in a significant period of time, it may not be safe to use its services if they involve sensitive data.
- **Valid URL**
If a company is selling an item through a host website such as eBay or Amazon, it can be worth checking whether their URL links to a genuine website or not.
- **Company or Owner Information**
If a business has little or no information about the company or any of its employees then it may not be operating in a legitimate manner. While there are businesses who may not provide information about themselves but have good intentions, you are still advised to remain alert if you come across a site such as this. You should also see what form of contact information is provided, if any.
- **Check for Security Certificate and Validate Domain Owner**
It is possible to check a website's security certificate in Internet Explorer by clicking the lock icon in the address bar and then clicking **View Certificates**. The domain owner can also be verified by using websites such as www.mywot.com, the "Web of Trust" website.

Pharming

In a pharming scam, a victim's computer or server is infected with malicious code that re-directs them to bogus websites. It is similar to Phishing in that it uses fake or spoofed websites to collect confidential data. However, in Pharming, the victim is re-directed to a bogus site even if they have entered the correct web address.

One way a pharming attack is done is by using DNS poisoning. In a DNS poisoning attack, the domain name system table in a server is modified so that users are automatically redirected to fraudulent sites.

The diagram below shows how a typical pharming attack is carried out.



1. The attacker targets a DNS service, for example one hosted by an ISP. The attacker changes the IP address of a website to the IP address of a web server that contains a fake version of the website.
2. A user wants to go the website, and types the address in the web browser.
3. The user's computer queries the DNS server for the IP address of the website.
4. Because the DNS server has already been 'poisoned' by the attacker, it returns the IP address of the fake website to the user's computer.
5. The user's computer now interprets the poisoned reply to be the correct IP address of the website. The user has now been tricked into visiting the fake website controlled by the attacker instead of the original website.

Content-Control Software

Content-control software is designed and optimised for controlling what content a user is allowed to access when browsing the Web. It is also known as censorware or web filtering software.

Types of filtering include:

- **Client-side filters**
This is a filter that is installed as software on a personal computer or laptop and can be customised. The filter can be disabled only by someone with the password. These applications are often used by parents to control children's access to inappropriate content on the Internet.
- **Browser-based filters**
Browser-based content filtering is typically carried out by plug-ins that can be added to a browser.
- **Content-limited (or filtered) ISPs**
Some internet service providers (ISPs) offer access to only a set portion of Web content. The decision on what content can be accessed is made by the ISP, and not the user.
- **Search-engine filters**
Many search engines offer users the option of turning on a safety filter that filters out the inappropriate links from all of the search results.

5.3 REVIEW EXERCISE

1. How do you identify a secure web site?

2. Open your browser and delete all temporary internet files.
3. Go to the Web of Trust website at <http://www.mywot.com/> and check the reputation of the following websites:
 - a. www.amazon.com
 - b. goldenpalace.com
 - c. whitehouse.com

LESSON 6 – COMMUNICATIONS

In this section, you will learn about:

- E-mail
- Social Networking
- VoIP
- Mobile

6.1 E-MAIL

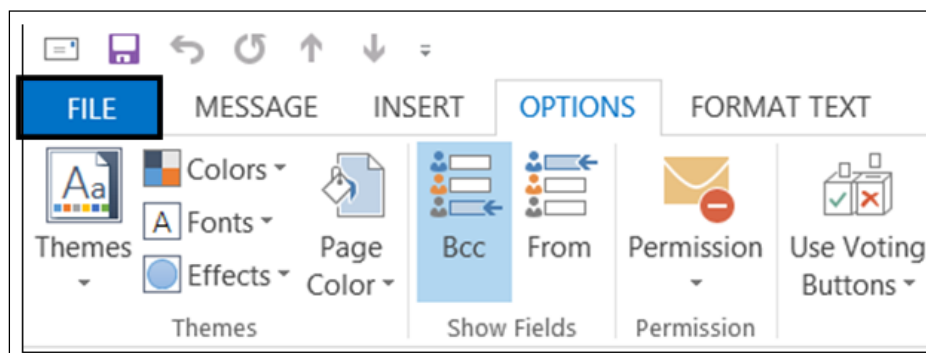
E-mail is a crucial tool for many individuals as well as organisations. There are important security considerations associated with using e-mail, however. You can take steps to ensure that your e-mail content is secure and to verify the identity of the sender of an e-mail. You also need to be aware of potential dangers associated with e-mail, such as fraud, spam, phishing, and malware.

Encrypting and Decrypting E-Mail

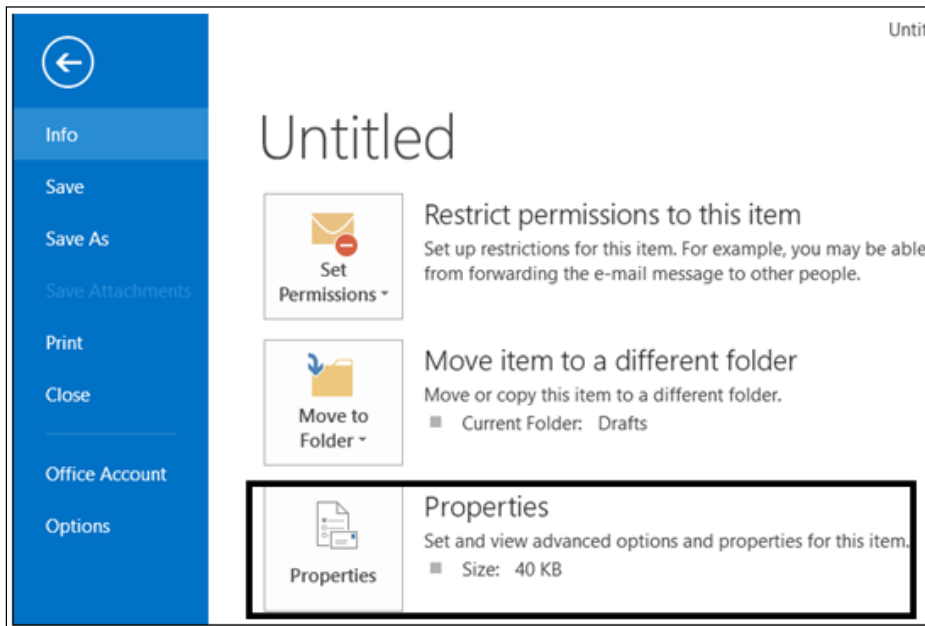
Encrypting an e-mail protects the content from being read by unintended recipients. It converts the text from readable plain text into scrambled cipher text, protecting the privacy of the message. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Any recipient without the corresponding private key would see only garbled text.

To encrypt a single message in Microsoft Outlook 2013:

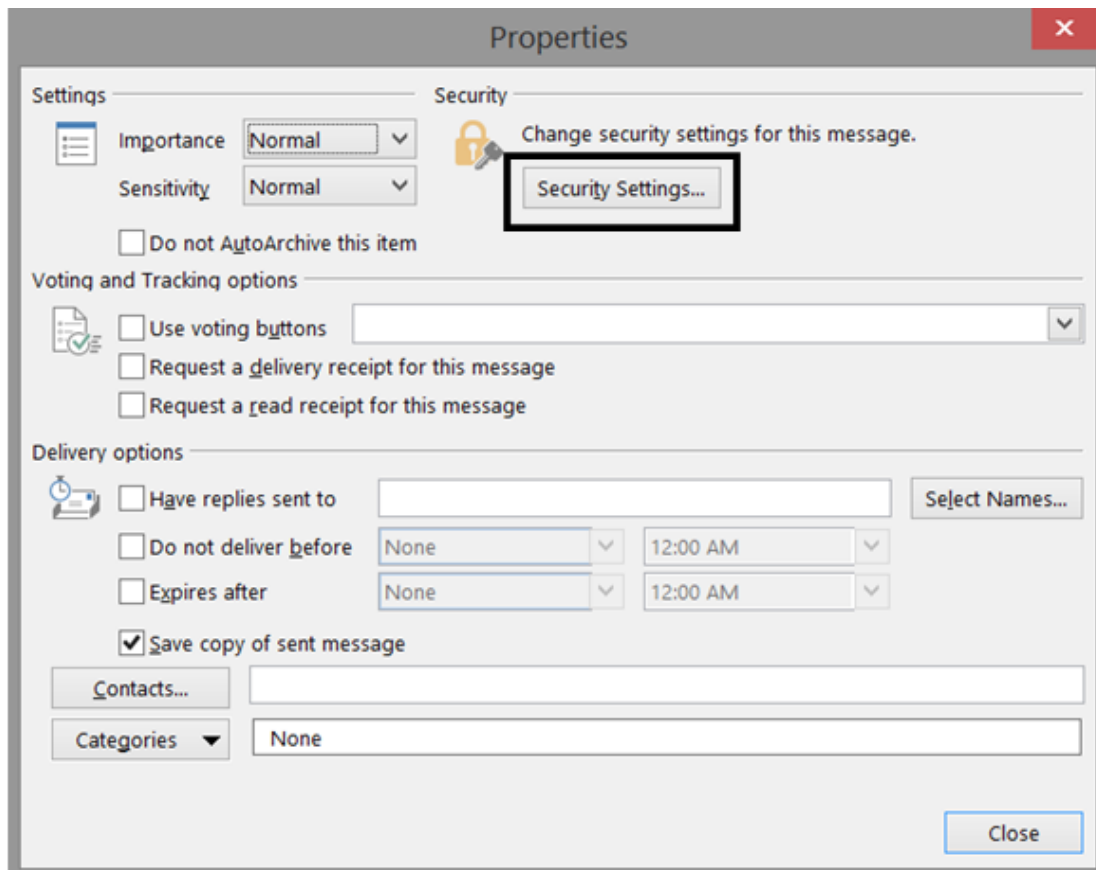
1. Compose a new message.
2. Click the **FILE** tab.



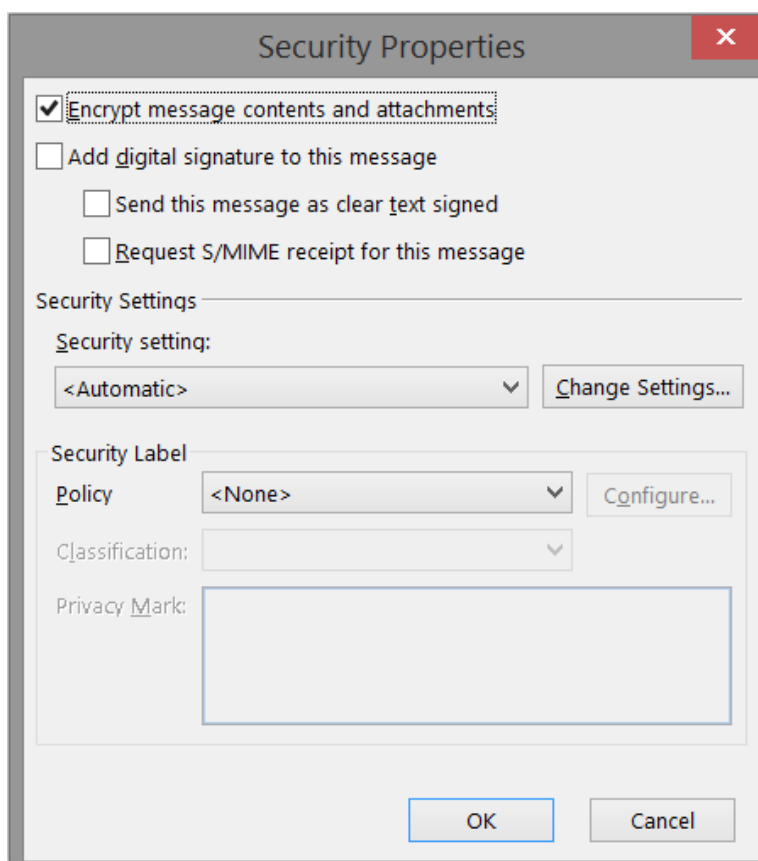
3. Click **Properties**.



4. Click **Security Settings**.



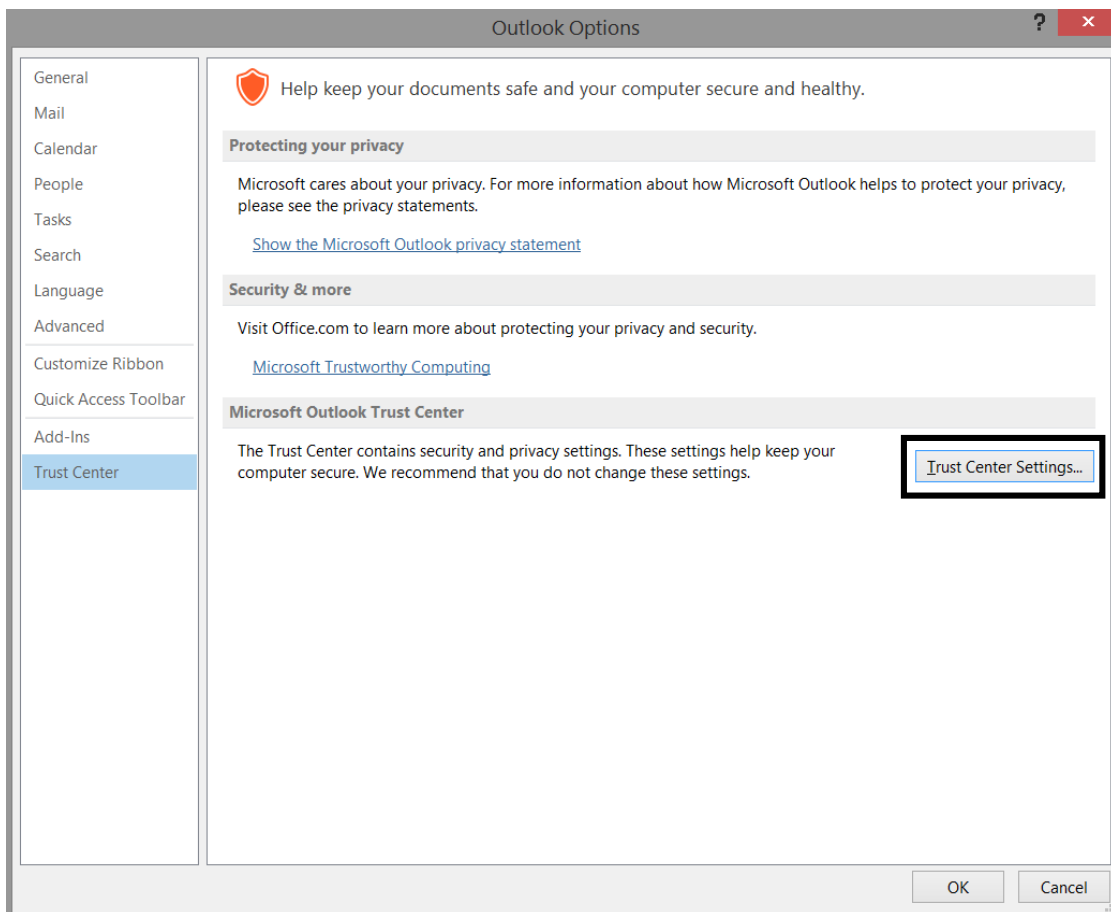
5. Click **Encrypt message contents and attachments**.



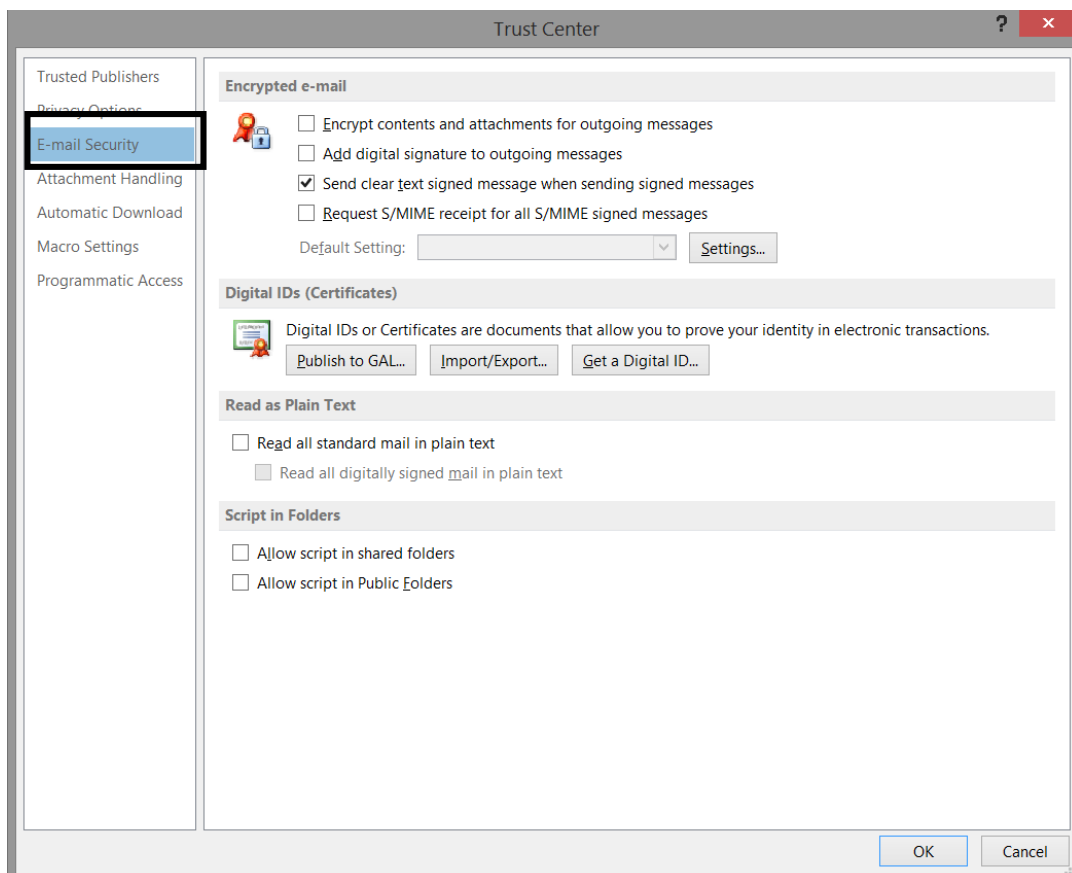
6. Click **OK**.
7. Click **Close**.

To encrypt all outgoing messages in Microsoft Outlook 2013:

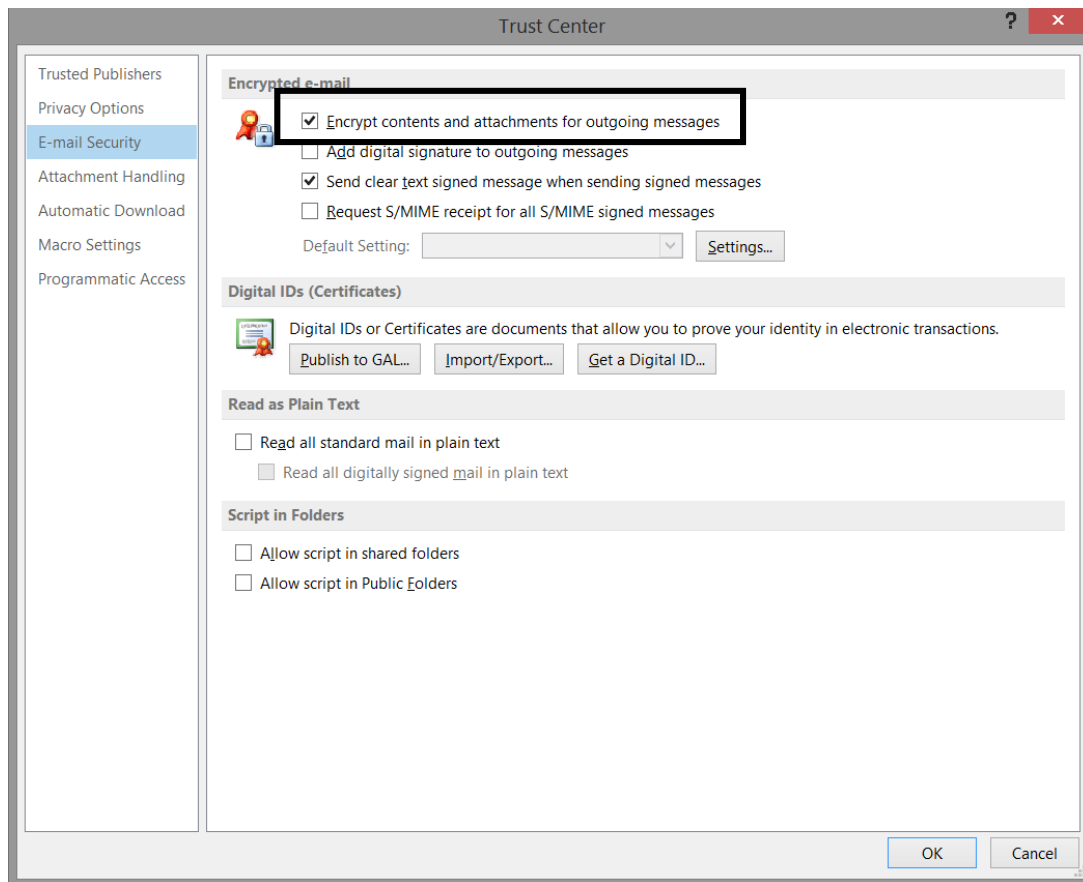
1. Click the **FILE** tab.
2. Click **Options**.
3. Click **Trust Center**.
4. Click **Trust Center Settings**.



5. Click **E-mail Security**.



- Under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.

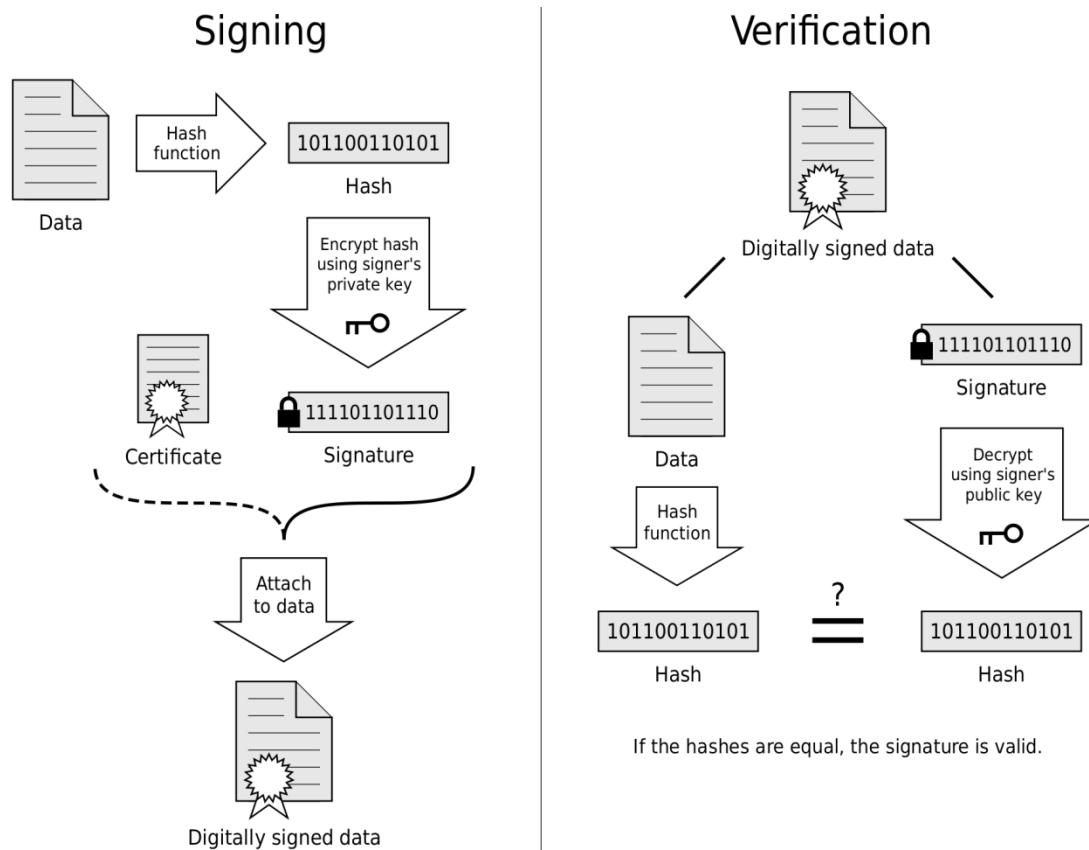


- Click **OK**.

Digital Signature

A digital signature is a unique digital mark applied to the message. The digital signature includes your certificate and public key. This information proves to the recipient that you signed the contents of the message and are not an imposter, and that the contents have not been altered in transit.

The diagram below shows how a simple digital signature is applied and then verified:

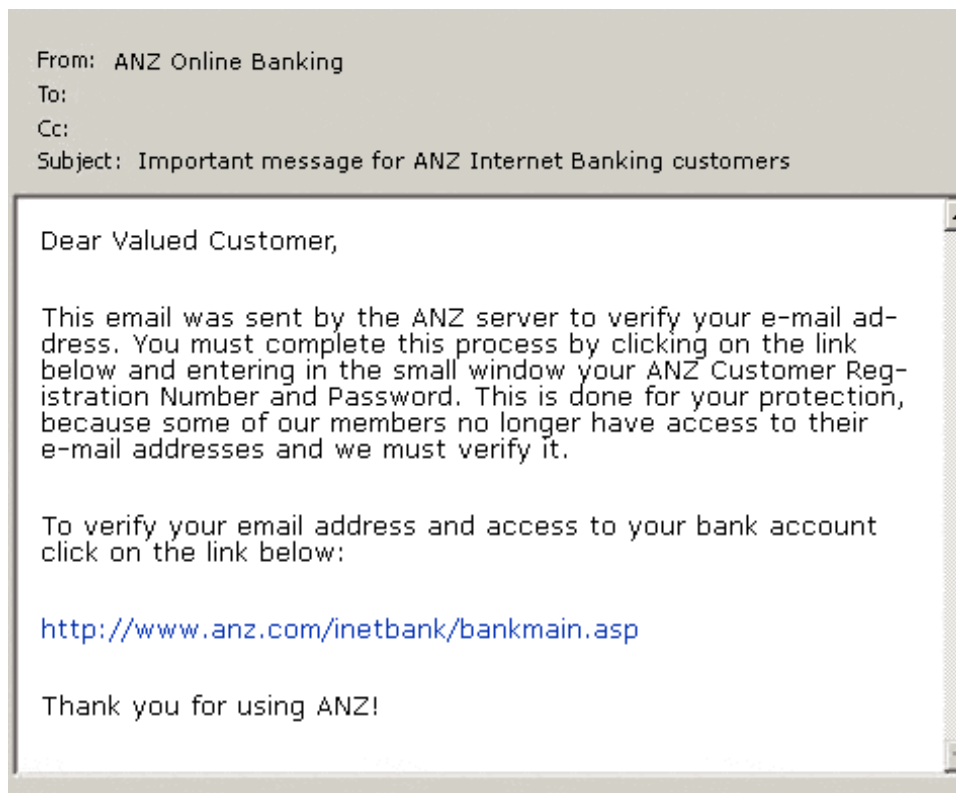


If you work in a large organisation, your employer may have obtained a digital ID for you. If you want to get a digital ID for your own use, you can get one from one of the many companies that issue and maintain Digital ID services.

Receiving Fraudulent and Unsolicited E-mail

You may be a user of online sites for social networking, online banking or day-to-day purchases. You need to be aware of e-mails that claim to be from these sites but are actually hoaxes and may contain malicious content.

You may receive an e-mail claiming to be from a bank but has actually been sent by a spammer in the hopes of obtaining information, such as your online username and password. Similarly, e-mails claiming to be invitations from social networking sites such as Twitter and Facebook are now commonplace. The messages may even contain an attached ZIP file that recipients are asked to open. The attachment may contain a mass-mailing worm, which can cause damage to your computer.



Unsolicited e-mail, or spam, is sometimes a relatively harmless but annoying form of mass marketing. However, spam is also used by scammers to trick people into sending them money. These types of e-mail attract unsuspecting users by, for example, proposing a business arrangement that could earn a very large amount of money. The users are asked to send a relatively small amount of cash to the scammer. The scammer will then keep asking for money, while promising that the user will eventually receive more money in return. Other types of e-mail warn of fake viruses and trick the user into installing malware. In some cases, users are persuaded to forward the e-mail to all their contacts in exchange for money. This is merely a ploy to spread the e-mail to as many people as possible.

Spammers may also use these tactics to collect e-mail addresses, which they can then use to send more spam message. Some spammers may also use your e-mail address or spoof your address to distribute spam and to perpetrate various scams.

Common features of these e-mails include:

- Requests to forward the e-mail to many people.
- Unsubstantiated claims that many other people have won prizes or cash.

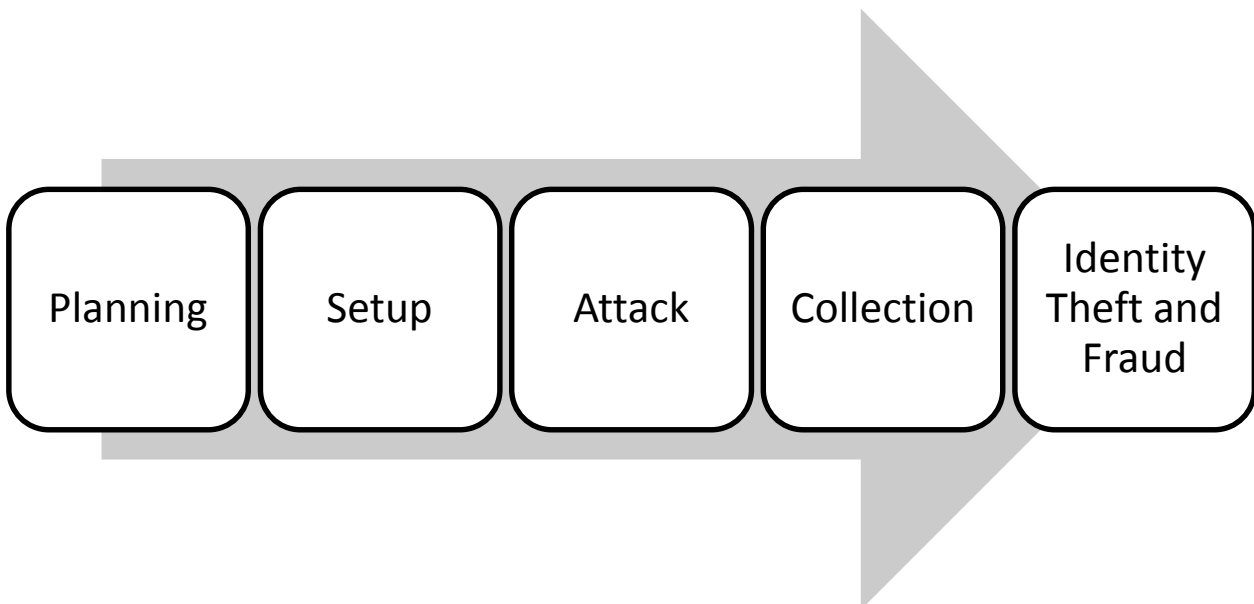
Phishing

Phishing is a type of social engineering attack which fraudulently obtains private and confidential information from the victims. In this type of attack, an e-mail which appears to come from a legitimate business source, such as banks or other

financial institutions, is used to trick users into giving the information to the attackers. They often use the company’s logo and branding and go to great lengths to appear as legitimate as possible. Typically, the phishing e-mail includes links to bogus web sites that look very similar to legitimate web sites. Some phishing e-mails warn of dire consequences if the victim does not provide the requested information.

In addition to stealing personal and financial information, attackers may use this technique to distribute viruses and other malware to unsuspecting users.

The entire process of a phishing attack is shown below:



1. Planning

The perpetrators of the phishing attack decides which company or organisation to spoof and find out how to get the list of customer e-mail addresses for that company. The use of mass-mailing and address collection techniques used is similar to the methods used by spammers.

2. Setup

Once the attackers identify the company to spoof and their intended victims, they prepare the e-mail delivery and data collection methods and tools.

3. Attack

At this point, the perpetrators send the spoofed e-mail messages to the intended victims. These messages appear to come from a legitimate source.

4. Collection

The information entered by victims into the fake web pages is collected and recorded.

5. Identity Theft and Fraud

Using the information collected from the victims, the perpetrators begin to make illegal purchases or transfer money from the victim's accounts.

It is important to know that phishing emails are considered a crime, and many authorities have dedicated email addresses and units allocated to these incidents. You can report phishing emails to the business that is being fraudulently used and possibly to a relevant government authority.

E-mail and Malware

E-mail attachments and links are commonly used methods to install malware on computers. Therefore, it is important to understand what to do when you get an e-mail that has an attachment or link in the e-mail message body.

Attachments can be one of two things:

1. The actual file or document designated in the e-mail.
2. A copy of the expected attachment that has malware embedded in it (file with macro or an executable file).

You should only assume that the attached is legitimate if you know the sender and the attachment is something that you would expect that person to send you. If you have any doubts, do not open the attachment. Confirm with the sender that it is legitimate, or delete it!

6.2 SOCIAL NETWORKING

Social networks are excellent tools for meeting and engaging with friends, colleagues, and people sharing similar interests. They can be used for professional networking and job searches, as a means to generate sales revenue, as a way to express opinions, or as a way to chat with friends. However, there are security risks associated with using these online services.



In some cases, users feel a false sense of anonymity and may inadvertently share private information that can then be viewed by the public. This is especially dangerous when children are involved.

Potential dangers when using social networking sites include:

- Cyber bullying/grooming
- Misleading/dangerous information
- False identities
- Fraudulent links or messages.

Cyber Bullying

Cyber bullying is the use of Internet and related technologies to harass, threaten, embarrass, or target an individual. Although often associated with children or young people, anyone can be subject to cyberbullying.

Sometimes, cyber bullying can be easy to spot. For example, a text message, tweet, or response to a social networking comment that is harsh, mean, or cruel may constitute cyberbullying. Other forms of cyberbullying are less obvious, such as impersonating a victim online or posting potentially damaging or revealing personal information online.

Cyber Grooming

Children and adolescents are increasingly involved in the online world, with many of them having multiple social networking accounts or profiles. These profiles often contain personal information such as home addresses and phone numbers. Perpetrators can use this information to make contact with the child for malicious purposes, often pretending to be another child, even if they are an adult.

The perpetrator makes contact with a child, builds a relationship, and develops trust. Then the perpetrator then takes advantage of that trust to try to exploit them sexually. This is called cyber grooming.

Misleading or Dangerous Information

Be careful not to believe everything you read online. People may post false or misleading information about a range of topics, including their own identities. This may not be done maliciously. However, you should try to verify the authenticity of any information before automatically believing it or taking any action.

False Identities

The Internet makes it easy for people to conceal their identities and motives. It may be sensible to restrict the people who are allowed to contact you on social networks. If you do interact with people you do not know, be careful about the amount of information you reveal and be extremely cautious about meeting them in person.

Fraudulent Links or Messages

Users of social networking services can send messages that may include embedded links to other social network locations or even outside sites. Social network spammers can use these tools to target a certain type of users, or send messages from an account disguised as that of a real person. These messages may include embedded links to pornographic sites or other sites designed to sell something.

It is also important to note that online abuse can be reported to the social network provider – and possibly to a law enforcement agency if the incident is sufficiently serious.

Sharing on Social Networks

You should always think before you post on a social network – in particular you should consider who should be able to read your post.

For, example, at the top of the Facebook page, an **Update Status** box is displayed. This is where you can post your thoughts on any topic you wish, as well as pictures and videos. Below the status box, you can choose how private or public you want your post to be.




A Facebook friend is anyone added to your friends list on Facebook, and are able to view certain information that you post on the site. Depending on your security settings, your Facebook friends may be able to see your photos, job title, birth date, games to play, group membership etc. You may choose who can see your information by changing your security settings.

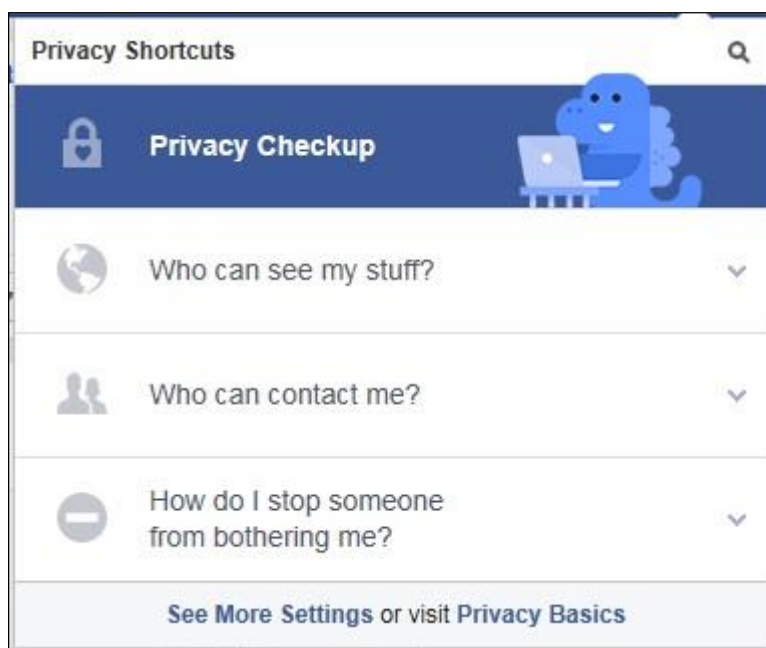
Privacy Settings

An important way of protecting yourself when using a social network is to apply appropriate privacy settings. These settings will typically allow you to control who sees your profile and who you interact with.

For example, Facebook allows us to manage the privacy of our postings and links to apps.

To set the privacy settings:

1. Log in to your Facebook account.
2. Click the drop down arrow next to the **Home** link.
3. Click on **Privacy Shortcuts** icon .



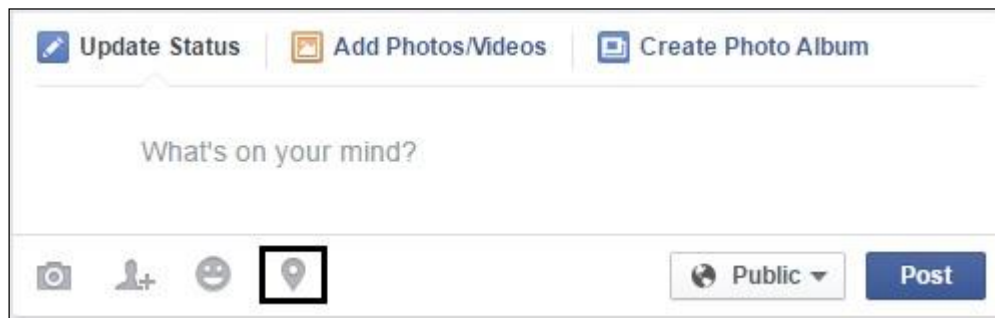
4. Click on the **See More Settings** option.

| Privacy Settings and Tools | | | |
|------------------------------|---|----------|------------------|
| Who can see my stuff? | Who can see your future posts? | Public | Edit |
| | Review all your posts and things you're tagged in | | Use Activity Log |
| | Limit the audience for posts you've shared with friends of friends or Public? | | Limit Past Posts |
| Who can contact me? | Who can send you friend requests? | Everyone | Edit |
| Who can look me up? | Who can look you up using the email address you provided? | Everyone | Edit |
| | Who can look you up using the phone number you provided? | Everyone | Edit |
| | Do you want search engines outside of Facebook to link to your profile? | Yes | Edit |

5. Click on the **Privacy** tab. This option allows you to control who can view your contact details and who can send you friend requests and messages.
6. Select the appropriate options.
7. Under **Timeline and Tagging**, you can set options for status updates, pictures and other items that you can be tagged in.

| | | | |
|--|--|--------------------|---------|
| Who can add things to my timeline? | Who can post on your timeline? | Friends | Edit |
| | Review posts friends tag you in before they appear on your timeline? | Off | Edit |
| Who can see things on my timeline? | Review what other people see on your timeline | | View As |
| | Who can see posts you've been tagged in on your timeline? | Friends of Friends | Edit |
| | Who can see what others post on your timeline? | Friends | Edit |
| How can I manage tags people add and tagging suggestions? | Review tags people add to your own posts before the tags appear on Facebook? | Off | Edit |
| | When you're tagged in a post, who do you want to add to the audience if they aren't already in it? | Friends | Edit |
| | Who sees tag suggestions when photos that look like you are uploaded? | Friends | Edit |

Before posting on social networking sites it is important to take note of the location settings of your post. It is possible to tag an update with a location, for example using the check in feature on Facebook, but this can compromise personal security. If a status indicates that a person is not at home they may be at a higher risk of being burgled, should someone with malicious intentions know of their absence.



Check In feature on Facebook

6.3 VOIP AND INSTANT MESSAGING

Voice over IP (VoIP) is a technology that allows delivery of voice communication sessions over the Internet. VoIP is a very useful and cost-effective way to speak with someone. Similarly, Instant Messaging (IM) is another Internet service that provides an easy way to communicate through text in real time with another person. However, there are some security considerations associated with using these services.

- **Malware** – malware can target specific IM applications in order to spread themselves.
- **Backdoor access** – Access to your systems may be allowed by vulnerabilities in IM and VoIP that allow security measures such as a firewall to be bypassed.
- **Access to files** – some virus that spread through IM may enable file sharing on a computer, allowing a hacker to gain full access.
- **Eavesdropping** – IM and VoIP can be susceptible to monitoring unless it is encrypted.

You can use a variety of strategies to ensure confidentiality when using IM and VoIP:

- **Encryption**
Data encryption is the best solution to ensure the security and privacy when using IM and VoIP. Many well-known IM and VoIP services and clients already use encryption.
- **Non-disclosure of important details**
Refrain from disclosing personal and sensitive details over IM or VoIP. If the data that is being transmitted over the IM network is not encrypted, a network sniffer, which can sniff data on most types of networks, can be used to capture the instant messaging traffic. This may give a hacker access to privileged information.

- **Restricting file sharing**
Avoid sharing files over an IM network as these can be intercepted.

6.4 MOBILE

Smartphones and other mobile devices such as tablets are increasingly used to store personal and business information, and mobile security is therefore crucial for data security.

More and more businesses use smartphones as their main communication tool, and individuals use them to store personal, sensitive data. For this reason, mobile devices are increasingly being targeted by hackers.

These hackers employ techniques such as phishing, bluetooth hijacking, and man-in-the-middle attacks. However, one of the main ways that mobile devices can be targeted is through malicious applications, which are now being developed at a rapid pace and are spreading to vulnerable smartphones and other mobile devices. Using an official application store, such as iTunes or Google Play, offers some protection against installing malware.

If you use a mobile application from an unofficial source, you run certain specific risks:

- Mobile malware can exploit the lack of technical support and quality controls that are associated with an unofficial application store, so downloading from an unofficial source is more risky.
- Apps from an unofficial source may also not be fully tested and quality approved, and may slow down the performance of your mobile device and other applications. They can also result in device instability.
- These apps may also automatically gain permission to access personal data such as contacts, images, and location without the user's knowledge.

Apps from an unofficial source are also more likely to contain hidden costs for the user – for example, you may unknowingly sign up to contracts or in-application purchases.

Mobile applications can extract private information from devices, such as location history, current location, images, contact details etc. Many applications give a list of items they would like access to, and it is important to review application permissions before and during download to know exactly what access the application will have.

Mobile applications may request permission to data including the details of your contacts, location information recorded using the device's GPS capability, and images or videos. Depending on what the application is for, these requests may

be reasonable, but you should always think about the risks of allowing applications to access your data.

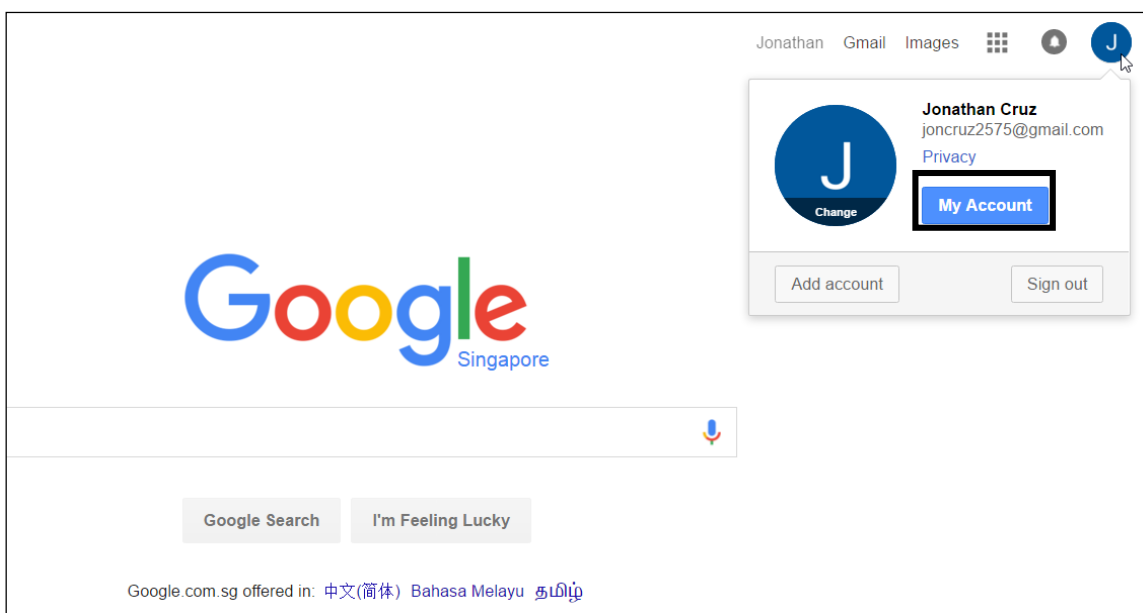
If your mobile device is lost or stolen, there are a variety of emergency or precautionary measures you can take, depending on the operating system and applications that you have.

- **Remote disable** – this function can be installed or enabled on your device so that it can be disabled remotely. Data will be retained on the device, but the user will not be able to access it. This function is useful if you believe that your device has been stolen.
- **Remote wipe** – This function can be installed or enabled on your device so that data can be remotely removed from the device.
- **Locate device** – This function allows you to locate the current location of your device. It uses the device's GPS functionality to track and locate the device's position on a map.

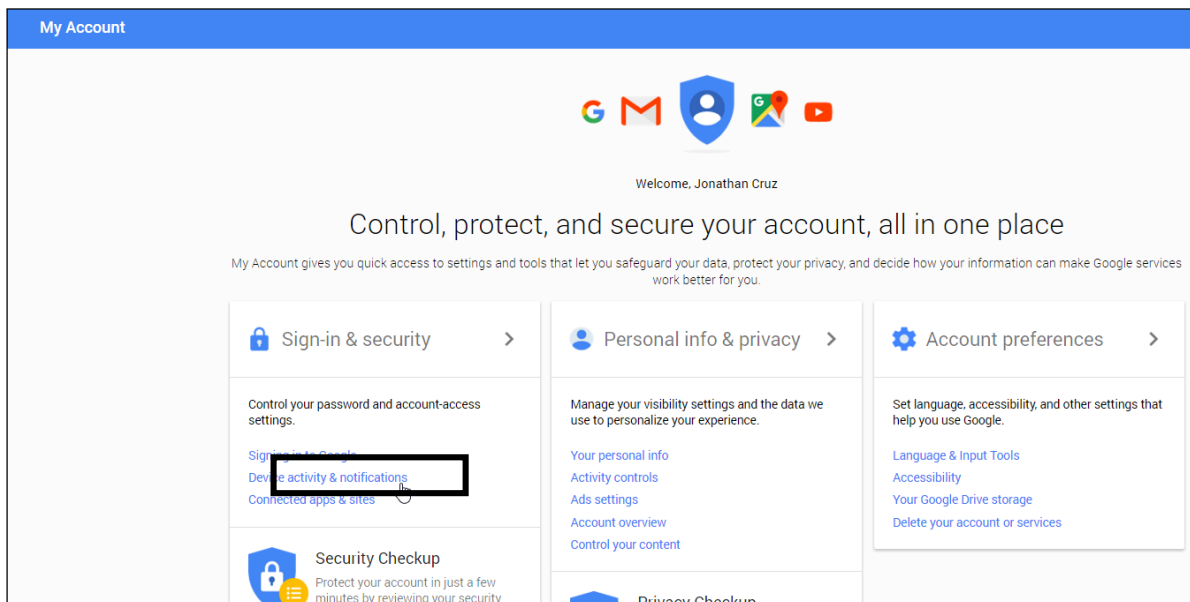
Emergency Features (Android)

For example, in the event that your phone is lost or stolen, you can log in to your Google account to locate your phone, or remotely wipe your phone data.

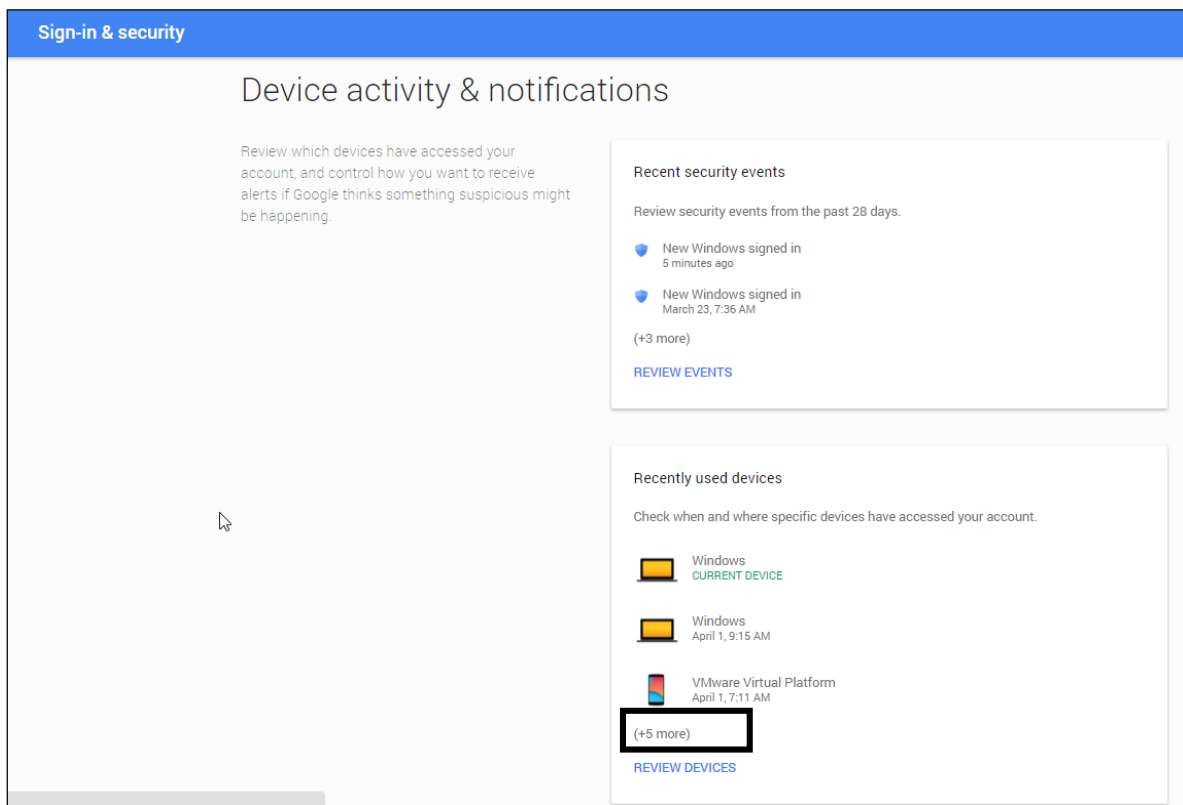
1. Sign in to your Google account.
2. Click the account icon at the upper right corner of the screen.



3. Click **My Account**.
4. Under Sign-in & security, click **Device activity & notification**.

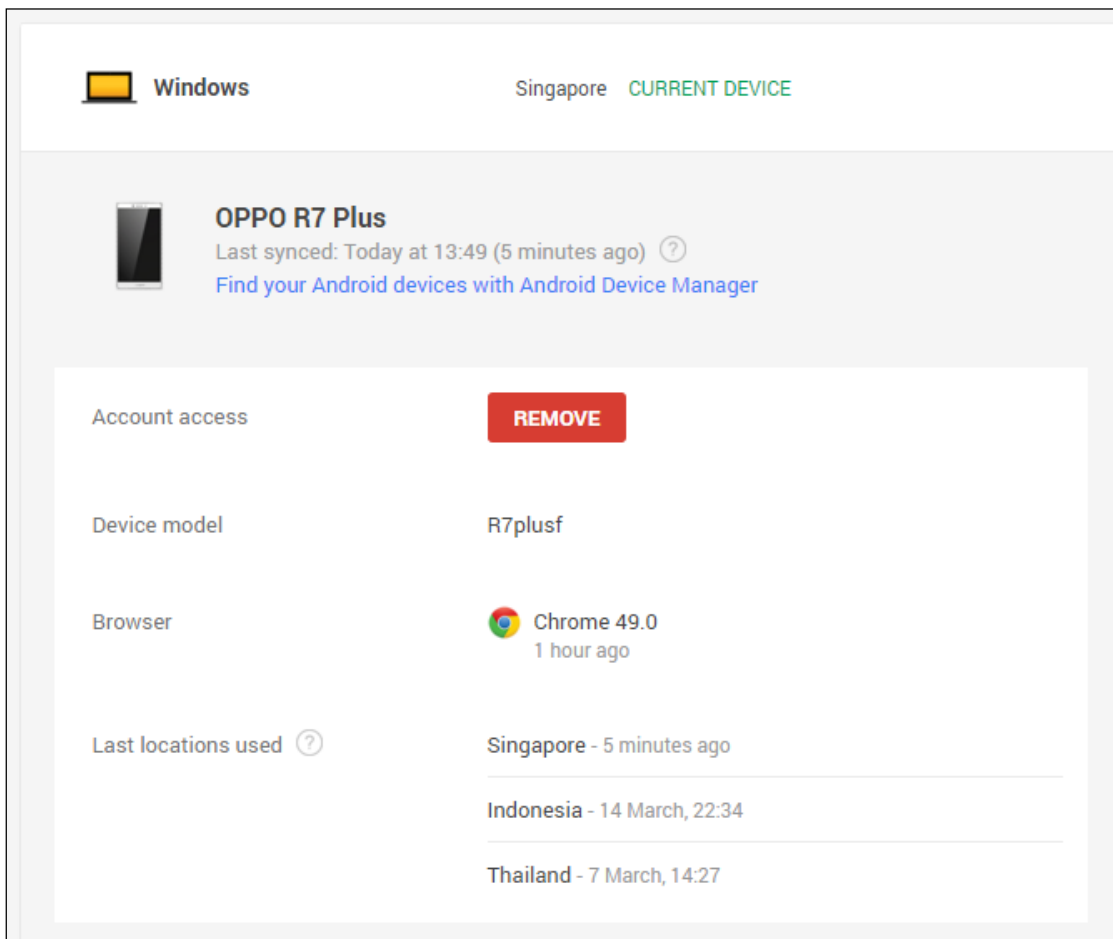


5. Under Recently used devices, select **REVIEW DEVICES**.

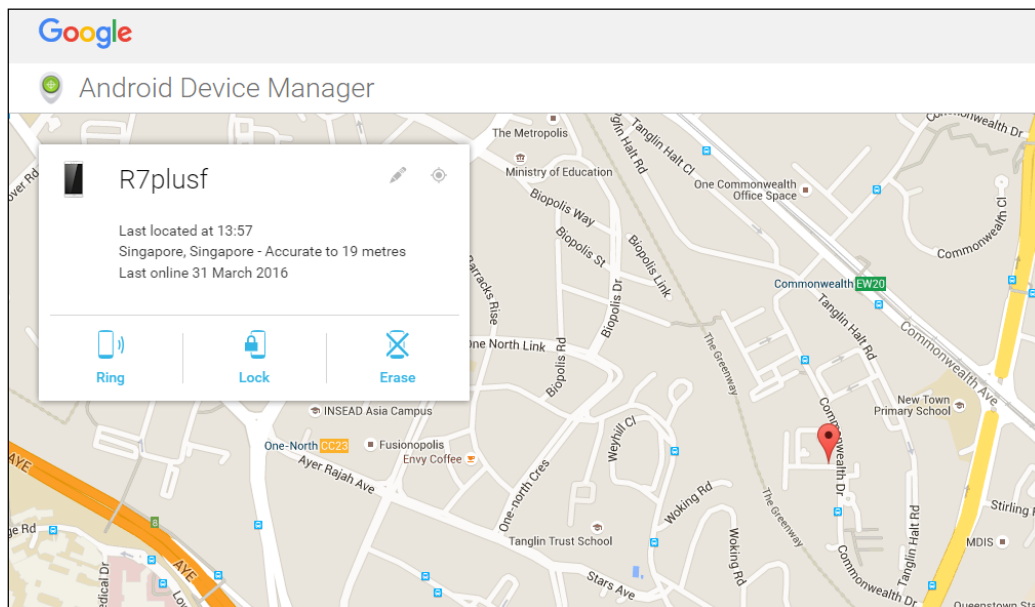


6. Select the devices you want to manage.

7. Click **Find your Android devices with Android Device Manager**.



8. The location of your phone is shown on the map.



9. You can use any of the options presented.

- Ring – make the device ring for five minutes.
- Lock – replace the device lock screen with a new password lock.

New lock screen

Your current lock screen will be replaced with a password lock. Don't use your Google account password.

New Password

Confirm password

Recovery message (optional)

Phone number (optional)

Cancel Lock

- Erase – erase all data on the phone and do a factory reset. All your apps and phone data will be permanently erased.

Erase all data?

This performs a factory reset on your device. Your apps, photos, music and settings will be deleted. After you erase the device, Android Device Manager will no longer work. This reset is permanent. We may not be able to wipe the content of the SD card in your device.

If your device is offline, we will perform the factory reset as soon as it goes online.

Cancel Erase

6.5 REVIEW EXERCISE

1. An e-mail is sent out to mass recipients asking them to verify their bank account details. This is an example of:
 - a. Shoulder surfing
 - b. Phishing
 - c. Encryption
 - d. Cracking

2. Which one of the following details is considered unsafe to share on a social networking site?
 - a. Nickname
 - b. Picture
 - c. Occupation
 - d. Home address

3. The process of redirecting users to a different website without their knowledge is known as:
 - a. Cracking
 - b. Pretexting
 - c. Pharming
 - d. Ethical hacking

4. A secure website can be identified by the web address if it begins with:
 - a. wwws
 - b. https
 - c. html
 - d. http

5. Consider the following questions:
 - a. What was your favourite holiday destination?
 - b. What is the name of your primary school?
 - c. What is my favourite pet's name?

What would the potential security threats be by answering the questions above?

LESSON 7 – SECURE DATA MANAGEMENT

In this section, you will learn about:

- Securing and backing up data
- Secure deletion and destruction

7.1 SECURE AND BACK UP DATA

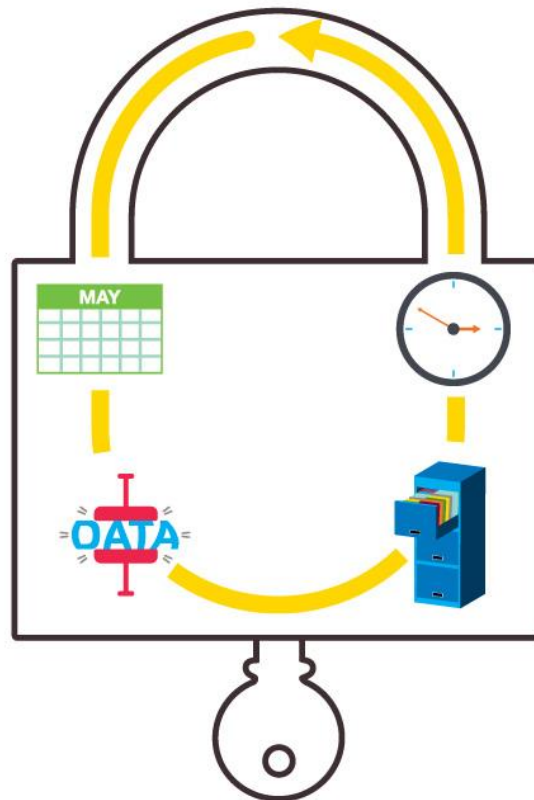
In offices and businesses, many devices – including PCs, laptops, and mobiles - may contain highly sensitive data pertaining to the company or may give access to the company network. If someone were to get hold of one of these devices, the results could be disastrous. Theft of company secrets, identity theft, and unauthorised access to the company network could occur. The same threats apply to your own personal PC, laptop, or mobile device.

There is a range of measures you can take to enhance the physical security of your, or your organisation's, devices:

- **Do not leave unsecured computers or devices unattended** – this will reduce the likelihood of them being stolen. This particularly applies to easily stolen mobile devices, such as laptops, smartphones, and tablets, which you may be using in a public environment.
- **Record details and location of items and equipment**, for example PCs. This allows for equipment to be tracked easily.
- **Use cable locks** to secure computers and devices safely, especially if members of the public have access to the work area.
- In addition, **work areas can be secured** by using access control measures, such as swipe cards or biometric scanning. This will prevent unauthorised individuals from accessing the workplace.

Backup Procedure

One way to avoid loss of important data is to regularly create backups of the data. Important data could be lost due to accidental or malicious deletion, power surges, disk corruption, or physical damage from fires or flood. By regularly backing up important data, you can at least recover most, if not all of your data. It is important to have regular scheduled backups. Also, the backed up data should be stored separately from the original data. This will ensure that if some form of physical disaster damages the originals, the backups will be in a safe location.



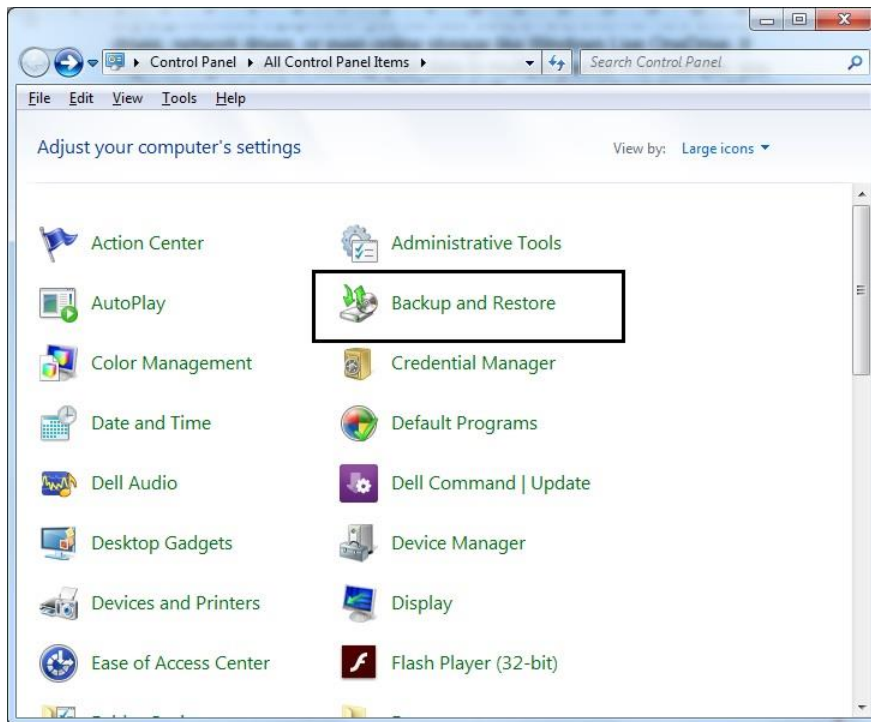
- Schedule** Whenever possible, schedule backups during off peak hours. When system use is low, the backup process takes less time to complete. You will need to carefully plan when to back up key system data.
- Compression** Compressing data during a backup helps reduce the size of files so that they can be stored using less memory than the original file(s). Upon decompression the files will return to their original size.
- Location** To ensure that backups are not lost in case of natural disasters, it is essential that copies of backups are stored off-site. You will also need to include copies of all software you need to install to recover and re-establish system operations.
- Regularity** How often you create backups depends on the value of the data and the frequency with which the data changes. For example, if your data changes on a daily basis, a daily backup may be performed.

Backing Up Data

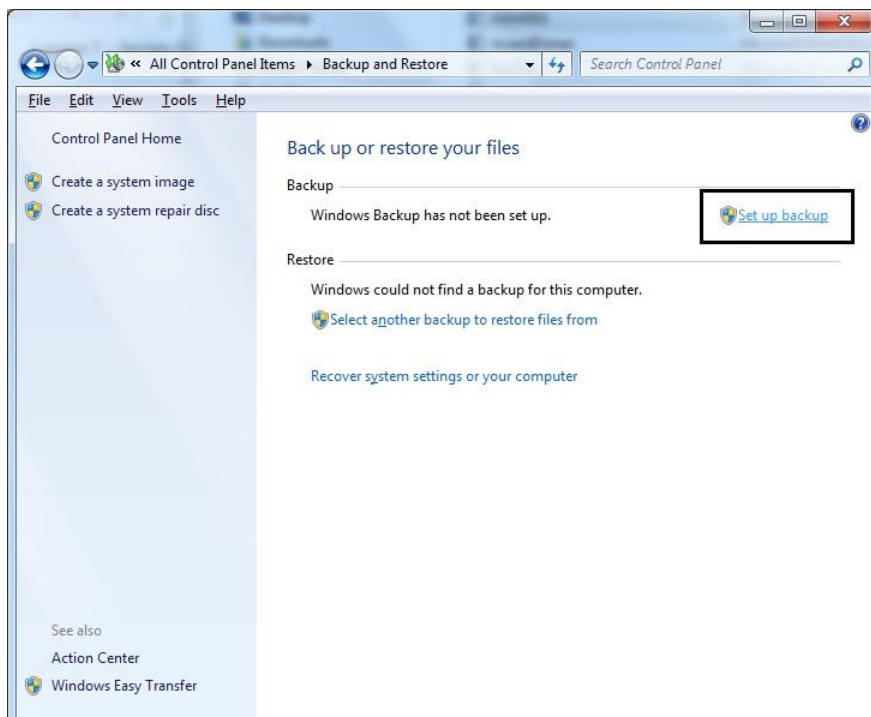
Nowadays, there are many options for backing up your content. You do not need any sophisticated equipment - you can use CDs, DVDs, external hard drives, flash drives, network drives, or even online storage like Microsoft OneDrive. It might be a good idea to back up your data to multiple places. For example, you might choose to back up your content onto both an external hard drive and to an online storage site.

To backup data to a location such as a local drive, external drive/media, cloud service:

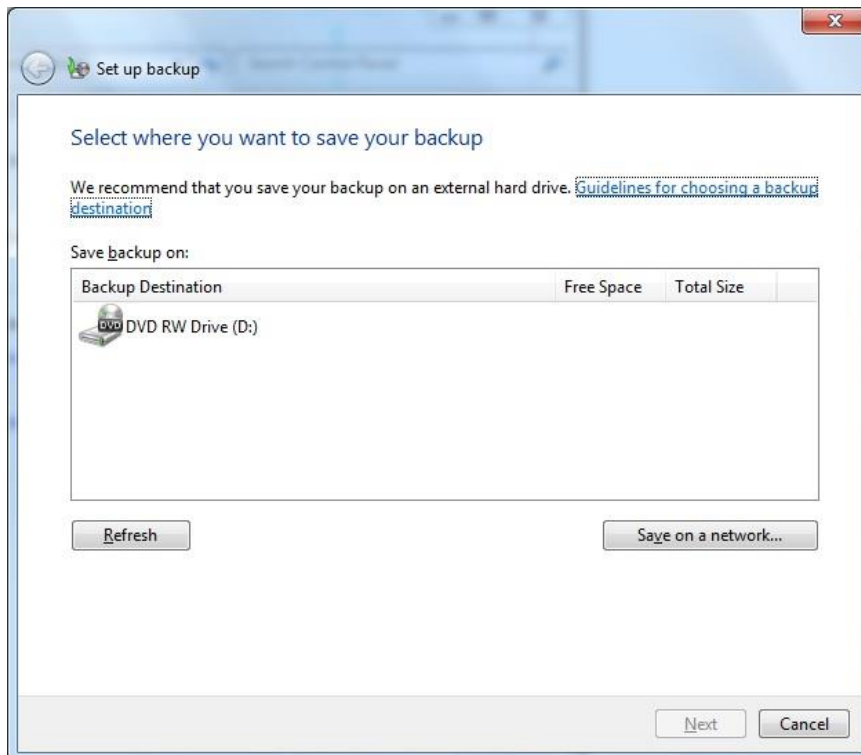
1. Click the **Start** button.
2. Click the **Control Panel**.
3. Click the **Backup and Restore** button.



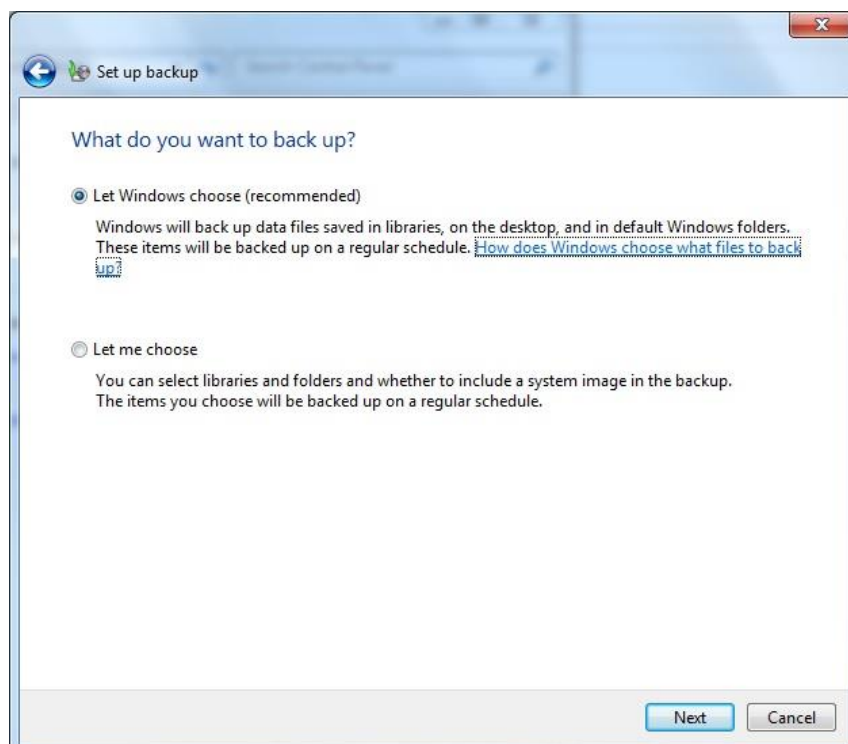
4. Click **Set up Backup**.



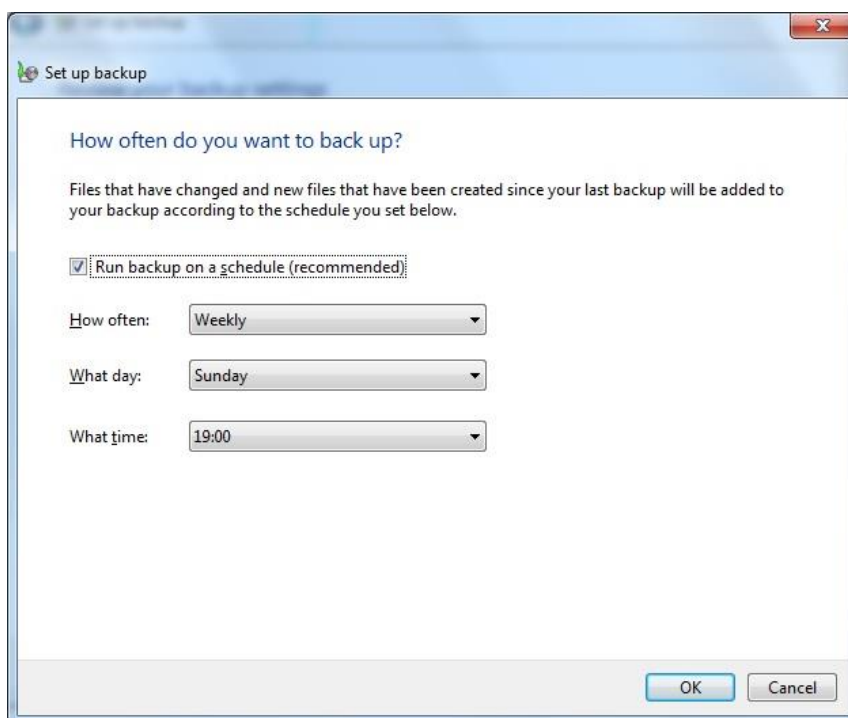
5. Select a **back-up location** (drive/network) and click **Next**.



6. Select the **data** to back up or accept the **recommended default settings**.



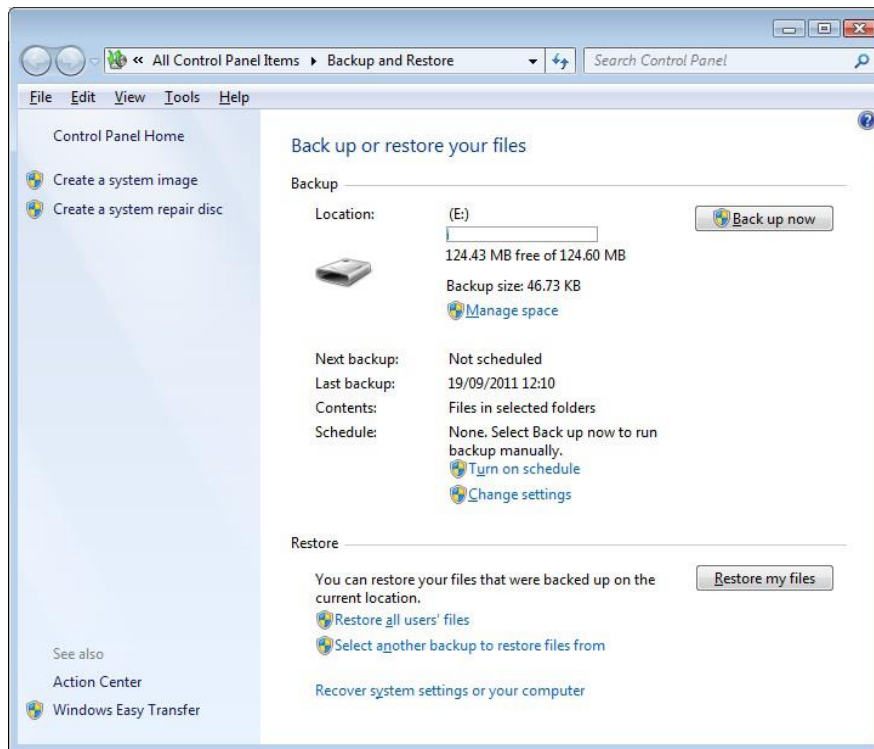
7. Select the **back-up schedule**.



8. Save **Settings** and click **Backup**.

To restore data from a backup location such as a local drive, external drive/media, cloud service:

1. Click the **Start** button.
2. Click **Control Panel**.
3. Click the **Backup and Restore** button.
4. Click **Restore My Files**.
5. Select the files or folders (or items) to restore by using **Search, Browse for Files or Browse for Folders**.



6. Click **Next**.
7. Choose to restore **In the original location** or **In the following location** to choose a new location.
8. Click **Restore**.

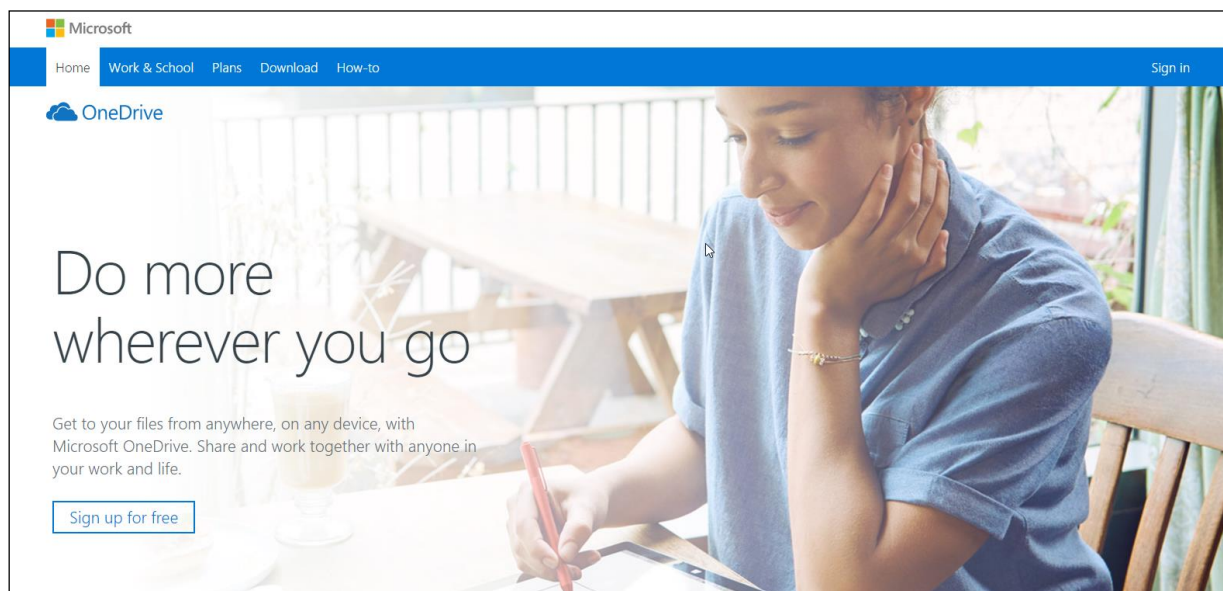
Cloud Back Up

Online storage is increasingly used as a cost-effective and accessible way to back up data. Microsoft OneDrive is one of the options available if online storage space is chosen to backup data. Microsoft offers enough storage for you to store your email, calendar, and contacts.

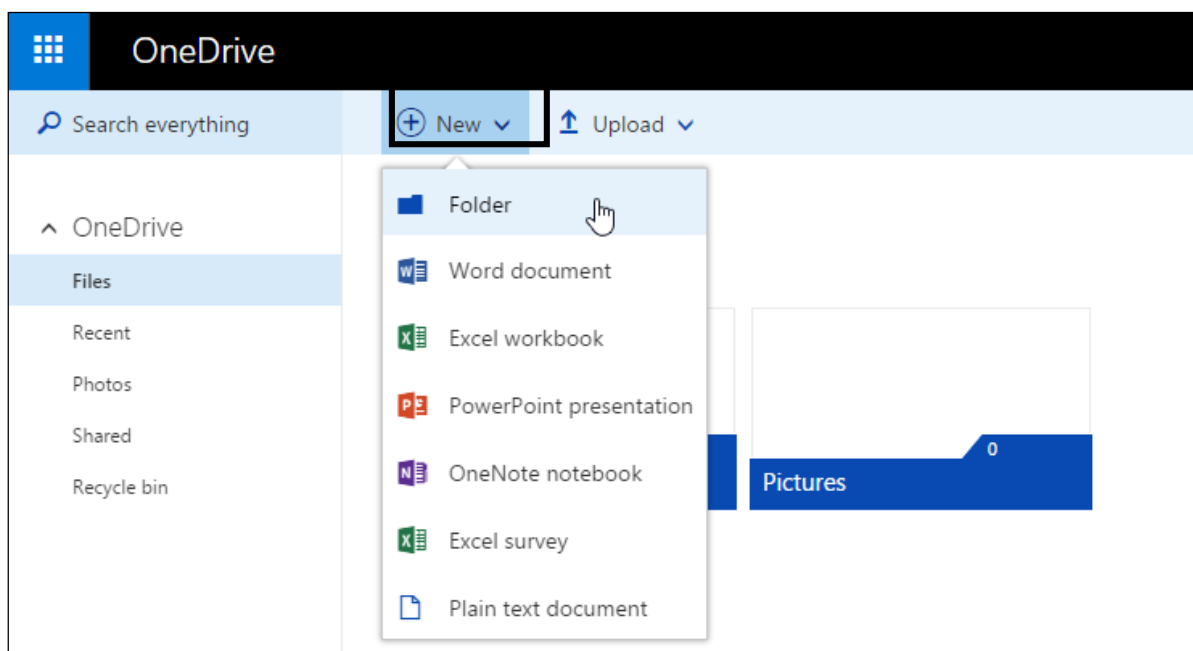
To set up an account with **OneDrive**:

1. Go to the webpage <https://onedrive.live.com> and click on **Sign up for free**.

If you use Outlook, Messenger, or Xbox LIVE, you already have a Windows Live ID. It can be used to sign in to OneDrive.

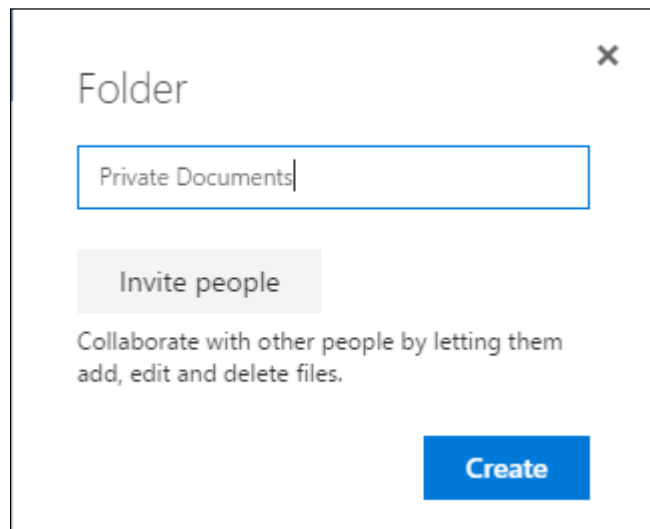


2. Create required folders by clicking on **New**.

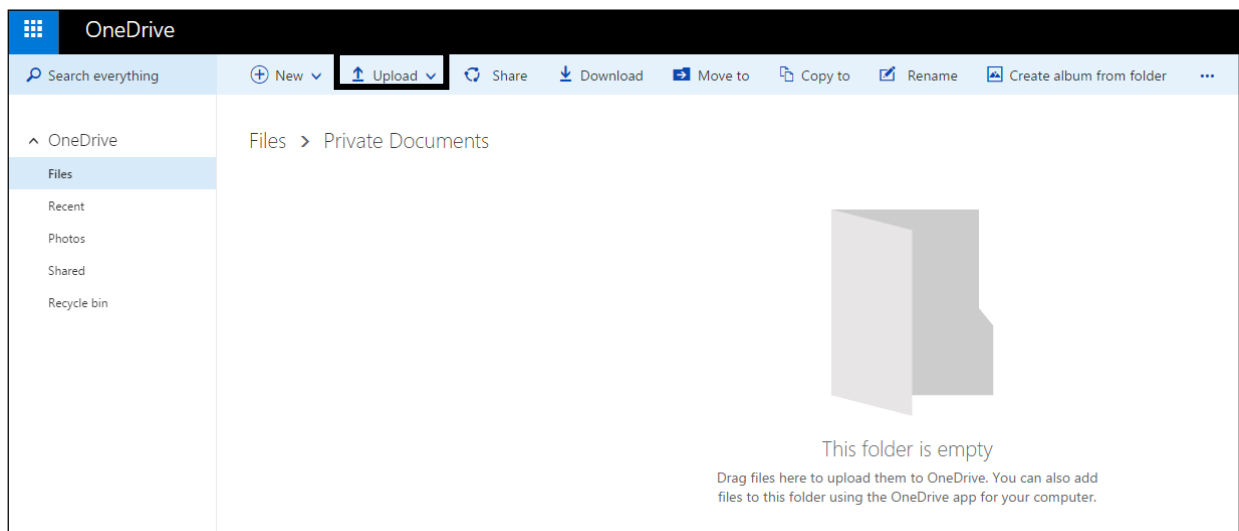


3. Click **Folder**.

4. Enter a name for the folder, and then click **Create**.



5. Click on the folder you just created.
6. Drag and drop files into the folder or click the **Upload** button.



OneDrive for Windows allows you to access OneDrive from your computer. When you install OneDrive, a OneDrive folder is created on your computer and the content is automatically kept in sync between your computers and OneDrive.com, so you can get to your latest files from virtually anywhere. Whenever you add, change, or delete files in one location, all the other locations will be updated.



7.2 SECURE DELETION AND DESTRUCTION

When you need to dispose of a storage device that contains important information, appropriate steps must be taken to ensure that the data is permanently erased and cannot be recovered by unauthorised individuals. Depending on the type of media, such as magnetic media such as USB or hard disks or optical media such as CDs or DVDs, various steps have to be taken to ensure that no remaining data can be recovered.

Data remanence is data that remains on media even after it has been “permanently deleted”. When a user deletes a file, it is usually moved to the trash bin. A user can empty the trash bin, seemingly “permanently” deleting the file. However, the file is not actually deleted. Some remnants of the file remains on the disk until the space occupied by the file is over written with other data. Data remanence exposes people or organisations to the risk of identity theft or disclosure of sensitive information if storage media is not disposed of properly.

Common Methods of Permanently Destroying Data

- **Shredding**
Paper containing sensitive information should be shredded. Shredders are very cost effective. Specialised shredders can also be used to permanently destroy storage media such as DVDs or hard drives.
- **Degaussing**
Degaussing is a process in which the magnetic field of a disk or drive is reduced or removed. This process uses a specialised device called a degausser. When applied to magnetic media, degaussing indiscriminately erases data required to control where data is written or read on the medium.
- **Drive/Media Destruction**
The best way to ensure the destruction of data and avoid data remanence, although it may be time consuming and quite cumbersome, is by physically destroying the data storage medium. The methods used to destroy the storage media must be done in a thorough manner as even a small fragment could contain a large amount of data.

Specific destruction techniques include:

- Physically breaking the media apart, by grinding, shredding, etc.
- Incineration.

- Phase transition (liquefaction or vaporisation of a solid disk).
- Application of corrosive chemicals, such as acids, to recording surfaces.

Using Data Destruction Utilities

Magnetic storage, such as computer hard drives, can be cleaned by software that uses an over-writing or "wiping" processes. USB "flash drive" devices can also be cleaned in this way.

This special software over-writes all the usable storage locations. Most secure file deletion software offers a choice of more and less secure over-writing options. More secure options take more time, given the multiple over-write operations.

There are a few free public domain programs that perform secure over-writes:

- DBAN <http://www.dban.org>
- Eraser <http://eraser.heidi.ie>

Some online services, such as social network sites, Internet forums, blogs, and cloud services, may allow you to delete information but that does not mean it has been permanently erased. There is ongoing debate regarding what companies and websites do with posted information, even after it has supposedly been deleted from public view. Remaining constantly vigilant when online will help minimise the threat of incriminating information being shared online, but know that even if you have deleted something from a social network site or forum it may not have completely been erased.

7.3 REVIEW EXERCISE

1. Which of the following is not a feature of a backup procedure?
 - a. Regularity
 - b. Schedule
 - c. Volume
 - d. Location

2. Which of the following is not used as a backup method?
 - a. Network drive
 - b. Random access memory
 - c. Dropbox
 - d. Flash drive

3. Residual traces of deleted data that still remains is known as:
 - a. Degaussing
 - b. Data remanence
 - c. Data permanence
 - d. Indexing

ECDL Syllabus

| Ref | ECDL Task Item | Location | Ref | ECDL Task Item | Location |
|-------|--|---------------------------|-------|---|-----------------------|
| 1.1.1 | Distinguish between data and information. | 1.1 Data Threats | 1.3.1 | Understand the term social engineering and its implications like: unauthorised computer and device access, unauthorised information gathering, fraud. | 1.3 Personal Security |
| 1.1.2 | Understand the term cybercrime. | 1.1 Data Threats | 1.3.2 | Identify methods of social engineering like: phone calls, phishing, shoulder surfing. | 1.3 Personal Security |
| 1.1.3 | Recognise malicious, accidental threats to data from individuals, service providers, and external organisations. | 1.1 Data Threats | 1.3.3 | Understand the term identity theft and its implications: personal, financial, business, legal. | 1.3 Personal Security |
| 1.1.4 | Recognise threats to data from force majeure like: fire, floods, war, earthquake. | 1.1 Data Threats | 1.3.4 | Identify methods of identity theft like: information diving, skimming, pretexting. | 1.3 Personal Security |
| 1.1.5 | Recognise threats to data from using cloud computing like: data control, potential loss of privacy. | 1.1 Data Threats | 1.4.1 | Understand the effect of enabling / disabling macro security settings. | 1.4 File Security |
| 1.2.1 | Understand basic characteristics of information security like: confidentiality, integrity, availability. | 1.2 Value of Information | 1.4.2 | Understand the advantages, limitations of encryption. Be aware of the importance of not disclosing or losing the encryption password, key, and certificate. | 1.4 File Security |
| 1.2.2 | Understand the reasons for protecting personal information like: avoiding identity theft, fraud, maintaining privacy. | 1.2. Value of Information | 1.4.3 | Encrypt a file, folder, drive. | 1.4 File Security |
| 1.2.3 | Understand the reasons for protecting workplace information on computers and devices like: preventing theft, fraudulent use, accidental data loss, sabotage. | 1.2 Value of Information | 1.4.4 | Set a password for files like: documents, spreadsheets, compressed files. | 1.4 File Security |
| 1.2.4 | Identify common data/privacy protection, retention and control principles like: transparency, legitimate purposes, proportionality. | 1.2 Value of Information | 2.1.1 | Understand the term malware. Recognise different ways that malware can be concealed on computers and devices like: Trojans, rootkits, backdoors. | 2.1 Types and Methods |
| 1.2.5 | Understand the terms data subjects and data controllers and how data/privacy protection, retention and control principles apply to them. | 1.2 Value of Information | 2.1.2 | Recognise types of infectious malware and understand how they work like: viruses, worms. | 2.1 Types and Methods |
| 1.2.6 | Understand the importance of adhering to guidelines and policies for ICT use and how to access them. | 1.2 Value of Information | 2.1.3 | Recognise types of data theft, profit generating/extortion malware and understand how they work like: adware, spyware, botnets, keystroke logging and diallers. | 2.1 Types and Methods |

| Ref | ECDL Task Item | Location | Ref | ECDL Task Item | Location |
|-------|---|------------------------------|-------|---|------------------------------|
| 2.2.1 | Understand how anti-virus software works and its limitations. | 2.2 Protection | 3.1.3 | Understand the role of the network administrator in managing authentication, authorisation and accounting, monitoring and installing relevant security patches and updates, monitoring network traffic, and in dealing with malware found within a network. | 3.1 Networks and Connections |
| 2.2.2 | Understand that anti-virus software should be installed on computers and devices. | 2.2 Protection | 3.1.4 | Understand the function, limitations of a firewall in personal, work environment. | 3.1 Networks and Connections |
| 2.2.3 | Understand the importance of regularly updating software like: anti-virus, web browser, plug-in, application, operating system. | 2.2 Protection | 3.1.5 | Turn the personal firewall on, off. Allow, block an application, and service/feature access through a personal firewall. | 3.1 Networks and Connections |
| 2.2.4 | Scan specific drives, folders, files using anti-virus software. Schedule scans using anti-virus software. | 2.2 Protection | 3.2.1 | Recognise different options for wireless security and their limitations like: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) filtering, Service Set Identifier (SSID) hiding. | 3.2 Wireless Security |
| 2.2.5 | Understand the risks of using obsolete and unsupported software like: increased malware threats, incompatibility. | 2.2 Protection | 3.2.2 | Understand that using an unprotected wireless network can lead to attacks like: eavesdroppers, network hijacking, man in the middle. | 3.2 Wireless Security |
| 2.3.1 | Understand the term quarantine and the effect of quarantining infected/suspicious files. | 2.2 Protection | 3.2.3 | Understand the term personal hotspot. | 3.2 Wireless Security |
| 2.3.2 | Quarantine, delete infected/suspicious files. | 2.2 Protection | 3.2.4 | Enable, disable a secure personal hotspot, and securely connect, disconnect devices. | 3.2 Wireless Security |
| 2.3.3 | Understand that a malware attack can be diagnosed and resolved using online resources like: websites of operating system, anti-virus, web browser software providers, websites of relevant authorities. | 2.2 Protection | 4.1.1 | Identify measures for preventing unauthorised access to data like: username, password, PIN, encryption, multi-factor authentication. | 4.1 Methods |
| 3.1.1 | Understand the term network and recognise the common network types like: local area network (LAN), wide area network (WAN), virtual private network (VPN). | 3.1 Networks and Connections | 4.1.2 | Understand the term one-time password and its typical use. | 4.1 Methods |
| 3.1.2 | Understand how connecting to a network has implications for security like: malware, unauthorised data access, maintaining privacy. | 3.1 Networks and Connections | 4.1.3 | Understand the purpose of a network account. | 4.1 Methods |

| Ref | ECDL Task Item | Location | Ref | ECDL Task Item | Location |
|-------|---|--------------------------------|-------|---|------------------------------|
| 4.1.4 | Understand that a network account should be accessed through a user name and password and locked, logged off when not in use. | 4.1 <i>Methods</i> | 6.1.1 | Understand the purpose of encrypting, decrypting an e-mail. | 6.1 <i>E-mail</i> |
| 4.1.5 | Identify common biometric security techniques used in access control like: fingerprint, eye scanning, face recognition, hand geometry. | 4.1 <i>Methods</i> | 6.1.2 | Understand the term digital signature. | 6.1 <i>E-mail</i> |
| 4.2.1 | Recognise good password policies, like: adequate password length, adequate letter, number and special characters mix, not sharing passwords, changing them regularly, different passwords for different services. | 4.2 <i>Password Management</i> | 6.1.3 | Identify possible fraudulent e-mail, unsolicited e-mail. | 6.1 <i>E-mail</i> |
| 4.2.2 | Understand the function, limitations of password manager software. | 4.2 <i>Password Management</i> | 6.1.4 | Identify common characteristics of phishing like: using names of legitimate organisations, people, false web links, logos and branding, encouraging disclosure of personal information. | 6.1 <i>E-mail</i> |
| 5.1.1 | Select appropriate settings for enabling, disabling autocomplete, autosave when completing a form. | 5.1 <i>Browser Settings</i> | 6.1.5 | Be aware that you can report phishing attempts to the legitimate organisation, relevant authorities. | 6.1 <i>E-mail</i> |
| 5.1.2 | Delete private data from a browser like: browsing history, download history, cached Internet files, passwords, cookies, autocomplete data. | 5.1 <i>Browser Settings</i> | 6.1.6 | Be aware of the danger of infecting a computer or device with malware by opening an e-mail attachment that contains a macro or an executable file. | 6.1 <i>E-mail</i> |
| 5.2.1 | Be aware that certain online activity (purchasing, banking) should only be undertaken on secure web pages using a secure network. | 5.2 <i>Secure Browsing</i> | 6.2.1 | Understand the importance of not disclosing confidential or personal identifiable information on social networking sites. | 6.2 <i>Social Networking</i> |
| 5.2.2 | Identify ways to confirm the authenticity of a website like: content quality, currency, valid URL, company or owner information, contact information, security certificate, validating domain owner. | 5.2 <i>Secure Browsing</i> | 6.2.2 | Be aware of the need to apply and regularly review appropriate social networking account settings like: account privacy, location. | 6.2 <i>Social Networking</i> |
| 5.2.3 | Understand the term pharming. | 5.2 <i>Secure Browsing</i> | 6.2.3 | Apply social networking account settings: account privacy, location. | 6.2 <i>Social Networking</i> |
| 5.2.4 | Understand the function and types of content-control software like: Internet filtering software, parental control software. | 5.2 <i>Secure Browsing</i> | 6.2.4 | Understand potential dangers when using social networking sites like: cyber bullying, grooming, malicious disclosure of personal content, false identities, fraudulent or malicious links, content, messages. | 6.2 <i>Social Networking</i> |
| | | | 6.2.5 | Be aware that you can report inappropriate social network use or behaviour to the service provider, relevant authorities. | 6.2 <i>Social Networking</i> |

| Ref | ECDL Task Item | Location | Ref | ECDL Task Item | Location |
|-------|--|---------------------------------------|-------|--|--|
| 6.3.1 | Understand the security vulnerabilities of instant messaging (IM) and Voice over IP (VoIP) like: malware, backdoor access, access to files, eavesdropping. | <i>6.3 VoIP and Instant Messaging</i> | 7.1.2 | Recognise the importance of having a backup procedure in case of loss of data from computers and devices. | <i>7.1 Secure and Back Up Data</i> |
| 6.3.2 | Recognise methods of ensuring confidentiality while using IM and VoIP like: encryption, non-disclosure of important information, restricting file sharing. | <i>6.3 VoIP and Instant Messaging</i> | 7.1.3 | Identify the features of a backup procedure like: regularity/frequency, schedule, storage location, data compression. | <i>7.1 Secure and Back Up Data</i> |
| 6.4.1 | Understand the possible implications of using applications from unofficial application stores like: mobile malware, unnecessary resource utilisation, access to personal data, poor quality, and hidden costs. | <i>6.4 Mobile</i> | 7.1.4 | Back up data to a location like: local drive, external drive/media, cloud service. | <i>7.1 Secure and Back Up Data</i> |
| 6.4.2 | Understand the term Application Permissions. | <i>6.4 Mobile</i> | 7.1.5 | Restore data from a backup location like: local drive, external drive/media, cloud service. | <i>7.1 Secure and Back Up Data</i> |
| 6.4.3 | Be aware that mobile applications can extract private information from the mobile device like: contact details, location history, images. | <i>6.4 Mobile</i> | 7.2.1 | Distinguish between deleting and permanently deleting data. | <i>7.2 Secure Deletion and Destruction</i> |
| 6.4.4 | Be aware of emergency and precautionary measures if a device is lost like: remote disable, remote wipe, locate device. | <i>6.4 Mobile</i> | 7.2.2 | Understand the reasons for permanently deleting data from drives or devices. | <i>7.2 Secure Deletion and Destruction</i> |
| 7.1.1 | Recognise ways of ensuring physical security of computers and devices like: do not leave unattended, log equipment location and details, use cable locks, access control. | <i>7.1 Secure and Back Up Data</i> | 7.2.3 | Be aware that content deletion may not be permanent on services like: social network site, blog, Internet forum, cloud service. | <i>7.2 Secure Deletion and Destruction</i> |
| | | | 7.2.4 | Identify common methods of permanently deleting data like: shredding, drive/media destruction, degaussing, using data destruction utilities. | <i>7.2 Secure Deletion and Destruction</i> |

Congratulations! You have reached the end of the ECDL IT Security book. You have learned about the key skills in ensuring security when online, including:

- Understanding the key concepts relating to the importance of secure information and data, physical security, privacy and identity theft.
- Protecting a computer, device, or network from malware and unauthorised access.
- Understanding the types of networks, connection types, and network specific issues, including firewalls.
- Browsing the World Wide, Web; communicating on the Internet securely.
- Understanding security issues related to communications, including e-mail and instant messaging.
- Back-up and restoring data appropriately and safely; securely disposing of data and devices.

Having reached this stage of your learning, you should now be ready to undertake ECDL certification testing. For further information on taking this test, please contact your ECDL test centre.

