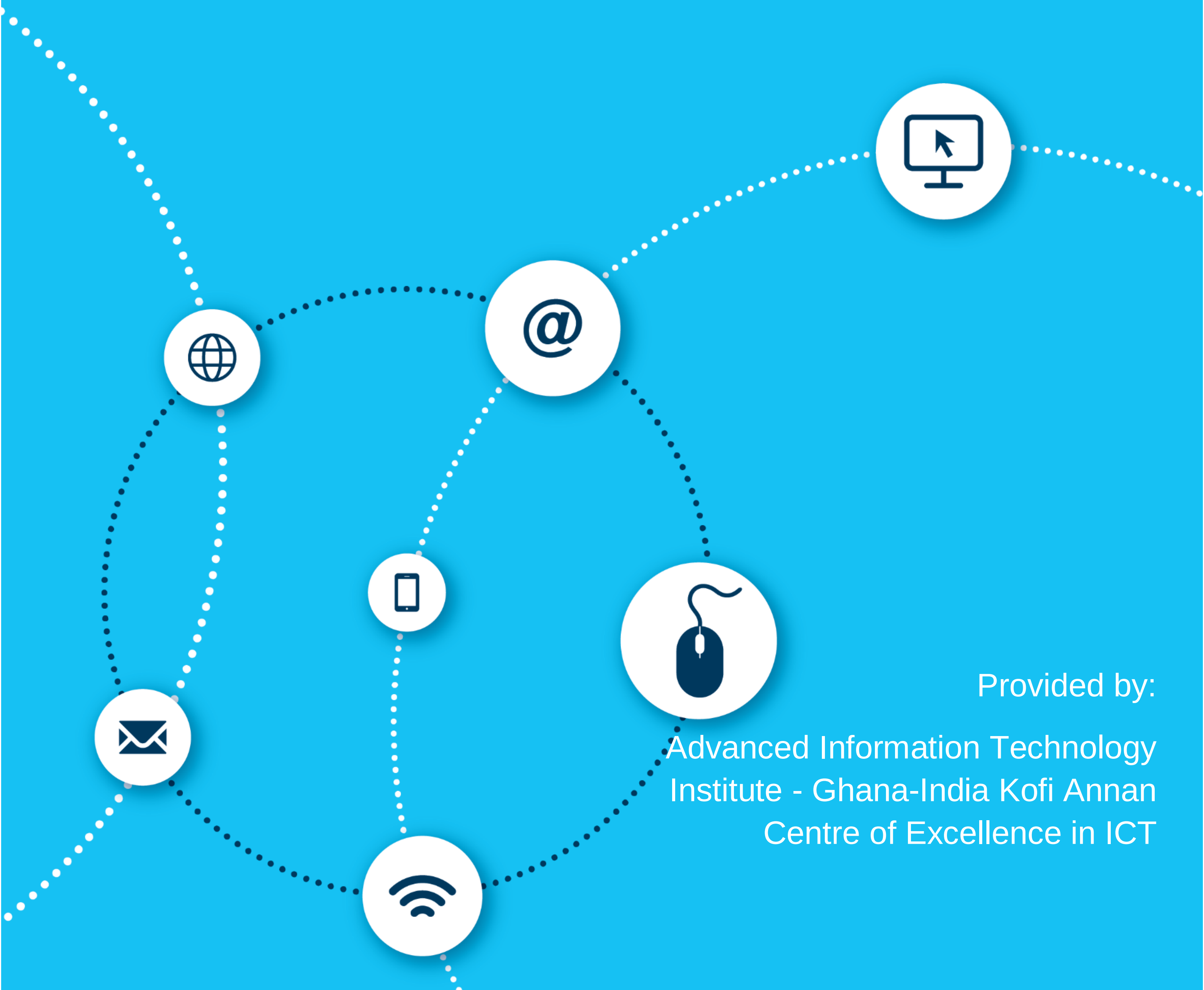
ICDL Africa

ICDL IT SECURITY

Syllabus 1.0
Learning Material



Provided by:

Advanced Information Technology
Institute - Ghana-India Kofi Annan
Centre of Excellence in ICT

This courseware may be used to assist candidates to prepare for the ECDL 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 the National Operator 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.

ICDL IT Security

Maintaining IT security in daily life 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 ICDL IT Security module will help you understand the primary concepts underlying the secure use of IT 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 the candidate 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 needed to understand the essential theories 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 – ICDL IT Security.

ICDL IT SECURITY

LESSON 1 –
SECURITY CONCEPTS

In this section, you will learn how to:

- Recognise data threats
- Understand the value of information
- Understand personal security
- Understand the term social engineering
- Enable or disable macro security
- Applying file security
- Understanding the advantage and limitation of encryption

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.

- **Cracking**
  The process of attempting to guess or crack passwords to gain access to a computer system or network.

- **Ethical Hacking**
  To attack security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them.

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.

1.2 VALUE 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 financial information.

Measures for Preventing Unauthorized Access to Data

- **Use a good password**

  The most common way to protect your computer's data is to setup user accounts with usernames and passwords. Anyone not having a username, or not knowing the correct password will be denied access. For this to be effective passwords chosen must not be easy to guess. Passwords should be a random combination of lowercase letters, uppercase letters and numbers (and symbols if this is allowed). Some computer systems replace the typing of usernames and passwords with other forms of user identification such as ID cards, fingerprint readers or voice-print recognition

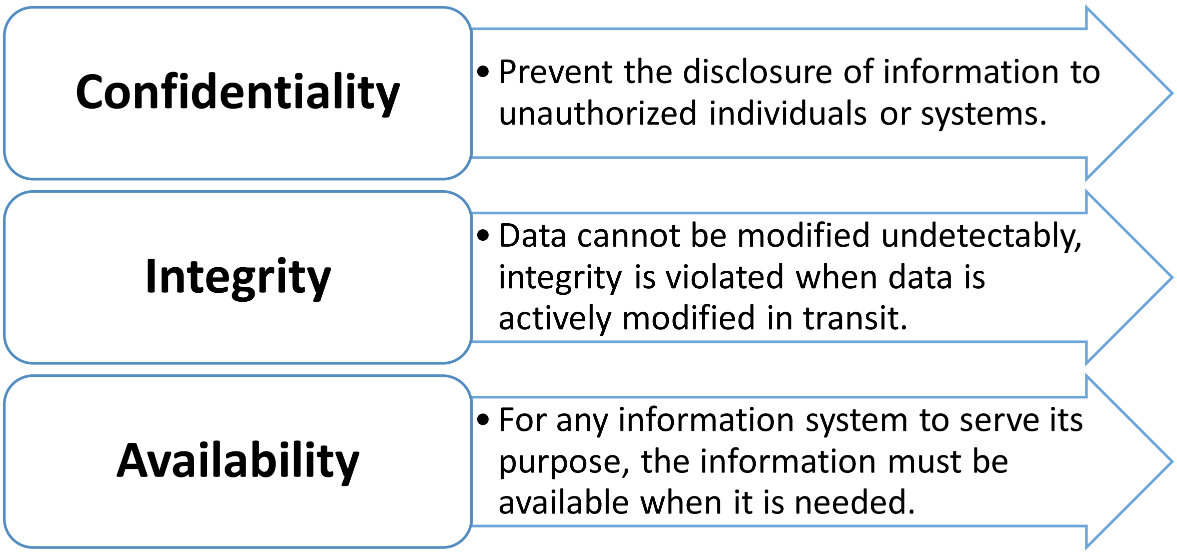
- **Encrypt data**

  Encryption is the process of using a cipher to make information unreadable to anyone who does not have the key to the cipher. This is a technique that allows you to prevent unauthorised access to data.

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.



Confidentiality

- Prevent the disclosure of information to unauthorized individuals or systems.

Integrity

- Data cannot be modified undetectably, integrity is violated when data is actively modified in transit.

Availability

- For any information system to serve its purpose, the information must be available when it is needed.

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.

Guidelines and Policies for ICT Use

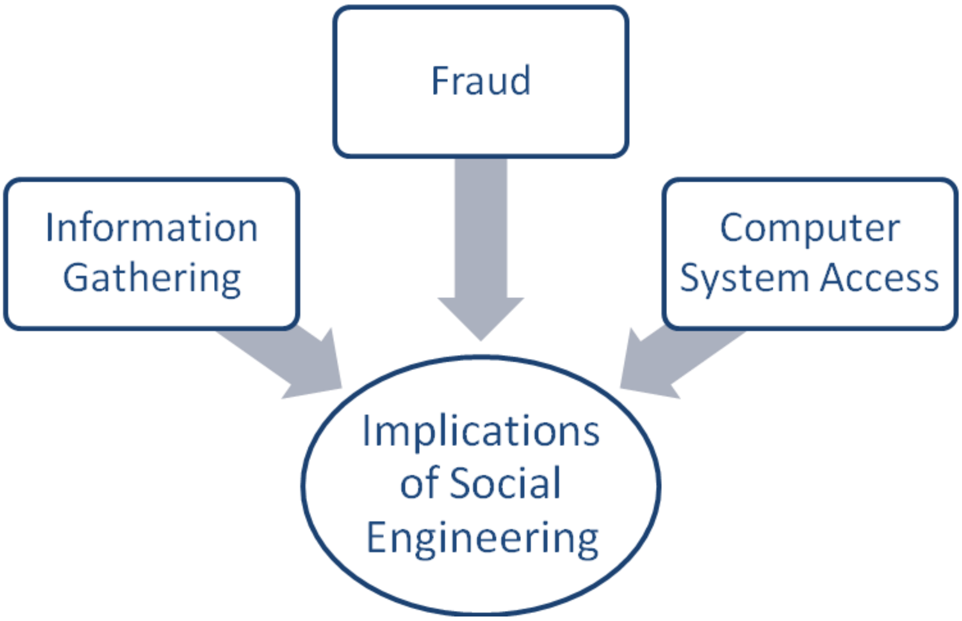
Many organisations, including private companies, public organisations, and educational institutions have guidelines and policies regarding how people should use the organisations ICT systems.

These guidelines and policies provide a standard for users to follow and ensure that there is a clear position on how ICT should be used to ensure the protection of the organisation's data. In many organisations, following these policies is a requirement.

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.

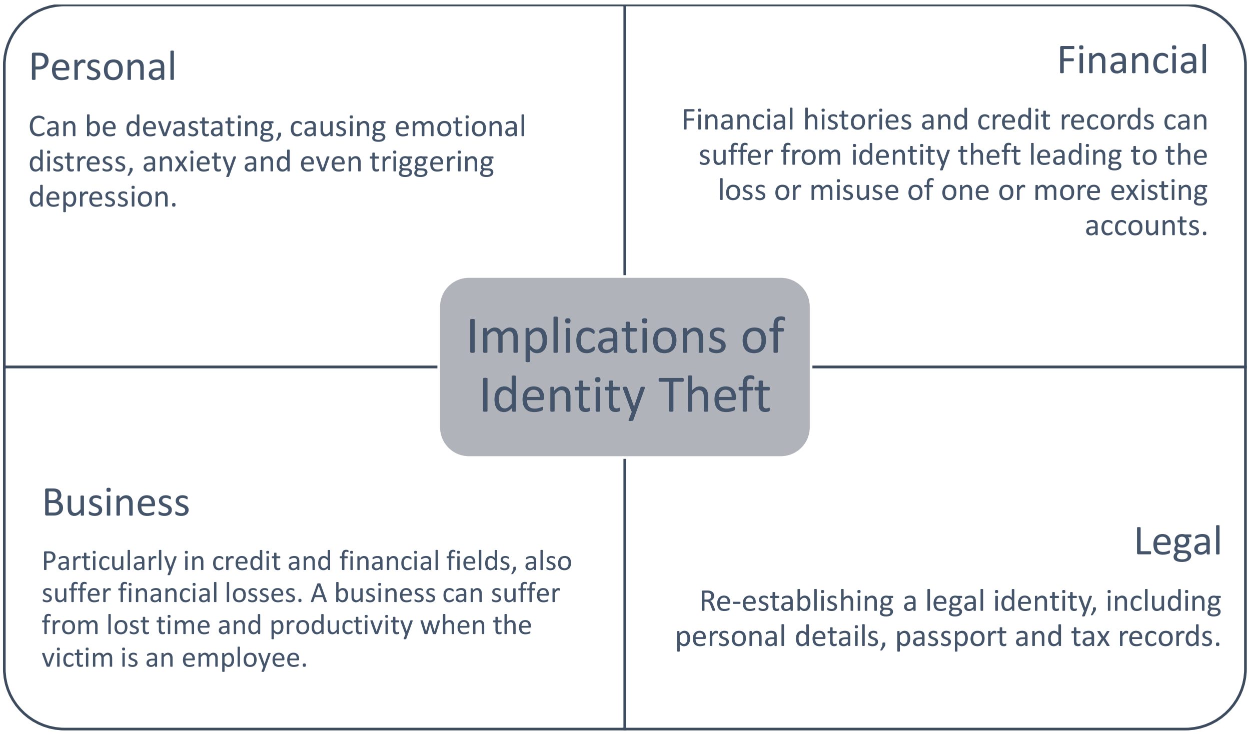
- **Phishing**
  A type of social engineering attack wherein the perpetrator sends an e-mail that appears to come from a legitimate source (for example, a banks). The e-mail usually requests for verification of information, sometimes warning of dire consequences if the recipient fails to comply. A phishing 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.



Implications of Identity Theft

Personal

Can be devastating, causing emotional distress, anxiety and even triggering depression.

Financial

Financial histories and credit records can suffer from identity theft leading to the loss or misuse of one or more existing accounts.

Business

Particularly in credit and financial fields, also suffer financial losses. A business can suffer from lost time and productivity when the victim is an employee.

Legal

Re-establishing a legal identity, including personal details, passport and tax records.

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 revel 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

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 2010**

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

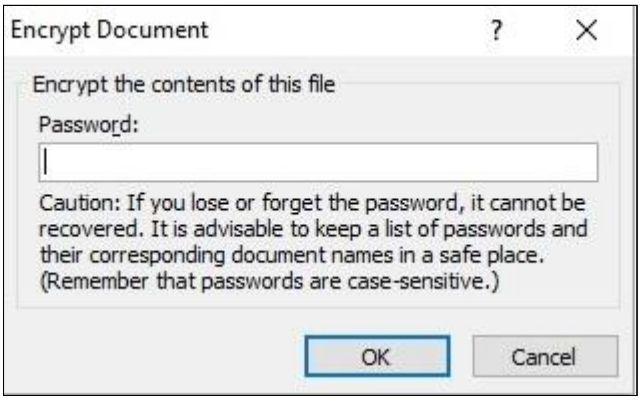
5. Click **OK**.
6. Click **OK**.

Setting File Passwords

You can set protect your files by using a password. In Microsoft Office, for example, you can use passwords to help prevent other people from opening and modifying your documents and spreadsheets.

Example: To set file password for Microsoft Word 2010 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, in the **Password** box, type a password.



Encrypt Document

Encrypt the contents of this file

Password:

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

6. Click **OK**.
7. In the **Confirm Password** dialog box, type the password again in the **Re-enter password** box, and then click **OK**.
8. Save the file.

To protect a spreadsheet when using Excel 2010, you follow a similar process. Click on the **File** tab, click **Info**, and click **Protect Workbook**. You then set your password.

You can also protect data contained in a compressed folder if, for example, you are sending the data to someone else. You set a password by selecting the encryption option when compressing the folder.

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 authorization or exceeds authorized access is known as:

   a. Cracking
   b. Phishing
   c. Hacking
   d. Pretexting

2. Which of the following is not a basic characteristic of information security?

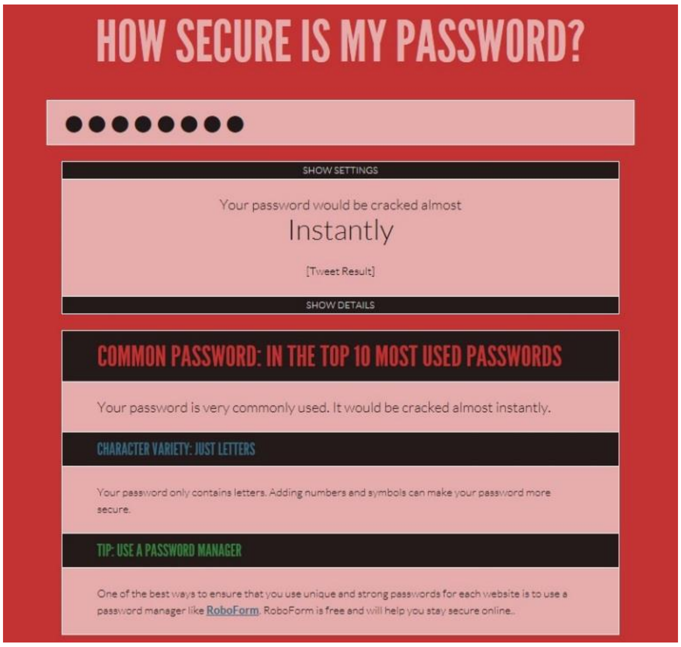
   a. Confidentiality
   b. Locality
   c. Integrity
   d. Availability

3. Which one of the following term describes the process of someone monitoring you keying in your ATM pin with malicious intent?
   a. Shoulder surfing
   b. Phishing
   c. Cyber bullying
   d. Cracking

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?

●●●●●●●●

SHOW SETTINGS

Your password would be cracked almost

Instantly

[Tweet Result]

SHOW DETAILS

COMMON PASSWORD: IN THE TOP 10 MOST USED PASSWORDS

Your password is very commonly used. It would be cracked almost instantly.

CHARACTER VARIETY: JUST LETTERS

Your password only contains letters. Adding numbers and symbols can make your password more secure.

TIP: USE A PASSWORD MANAGER

One of the best ways to ensure that you use unique and strong passwords for each website is to use a password manager like RoboForm. RoboForm is free and will help you stay secure online..

LESSON 2 - MALWARE

In this section, you will learn about:

- Definition and function of malware
- Recognize types of infectious malware
- Using anti-virus software

2.1 Definition and Function 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.

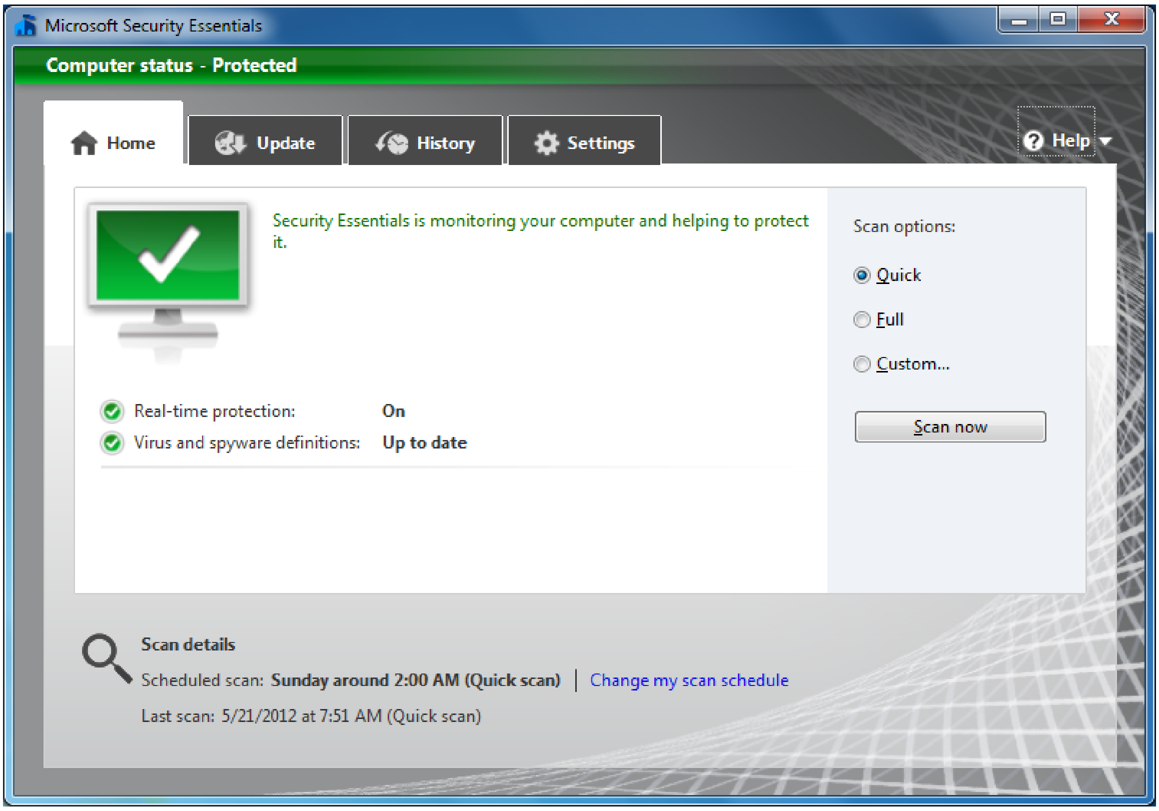
Using an Anti-Virus Software

Software: Microsoft Security Essentials

Scanning

1. Open **Microsoft Security Essentials**.

2. In the **Home** tab, select a **Quick scan** or a **Full scan**.



Computer status - Protected

Security Essentials is monitoring your computer and helping to protect it.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom...

Scan details

Scheduled scan: Sunday around 2:00 AM (Quick scan) | Change my scan schedule

Last scan: 5/21/2012 at 7:51 AM (Quick scan)

3. Click **Scan now**.

Scanning Specific Drives

2. In the **Home** tab, select **Custom**.

3. Click **Scan now**.

4. Check the required drive and folders.

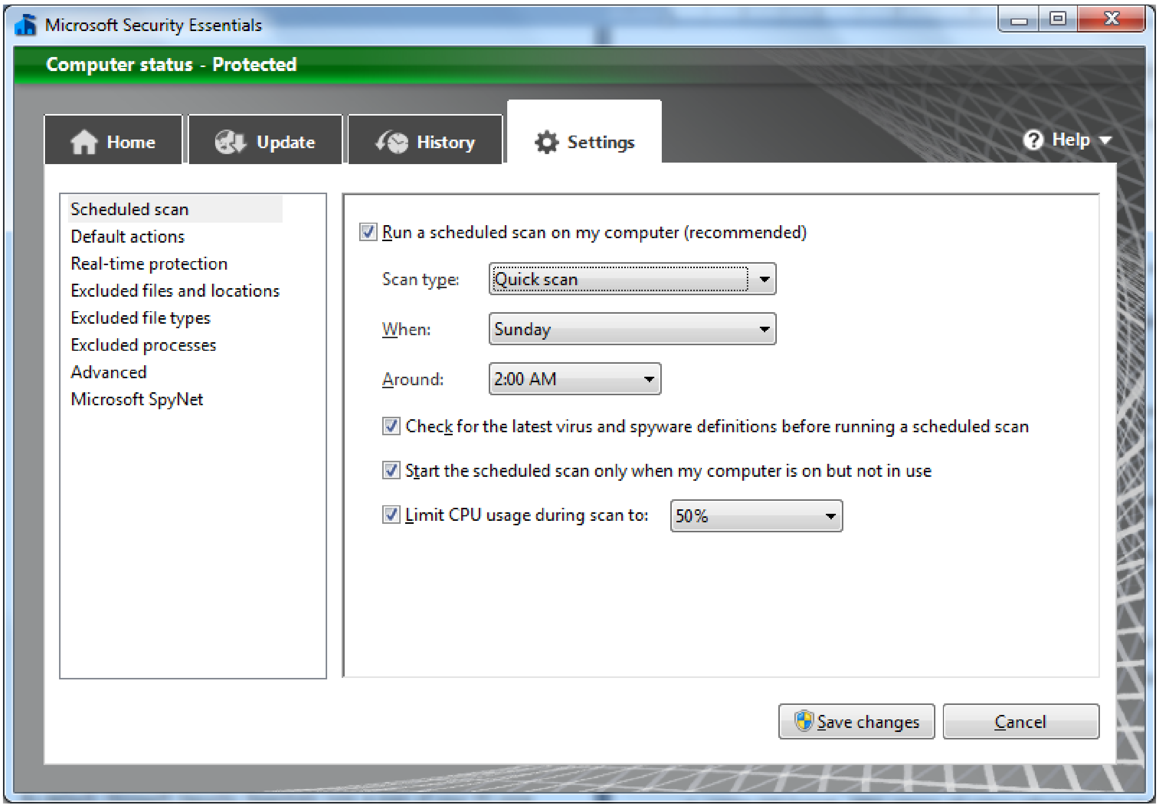
5. Click **OK**.

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.



☑ Run a scheduled scan on my computer (recommended)

Scan type: Quick scan

When: Sunday

Around: 2:00 AM

☑ Check for the latest virus and spyware definitions before running a scheduled scan

☑ Start the scheduled scan only when my computer is on but not in use

☑ Limit CPU usage during scan to: 50%

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.

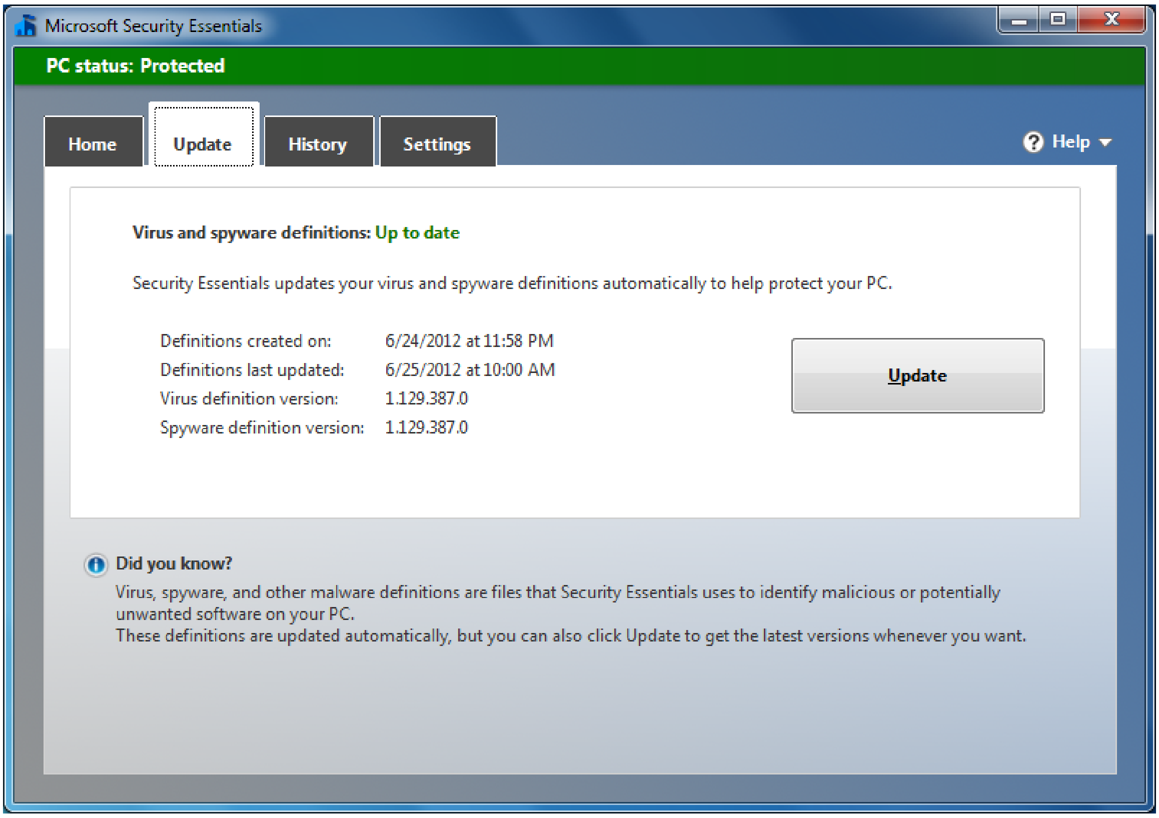
Updating Anti-Virus Software

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.

<u>Updating Virus Definition</u>

1. Open **Microsoft Security Essentials**.

2. In the **Update** tab, click **Update**.



Virus and spyware definitions: Up to date

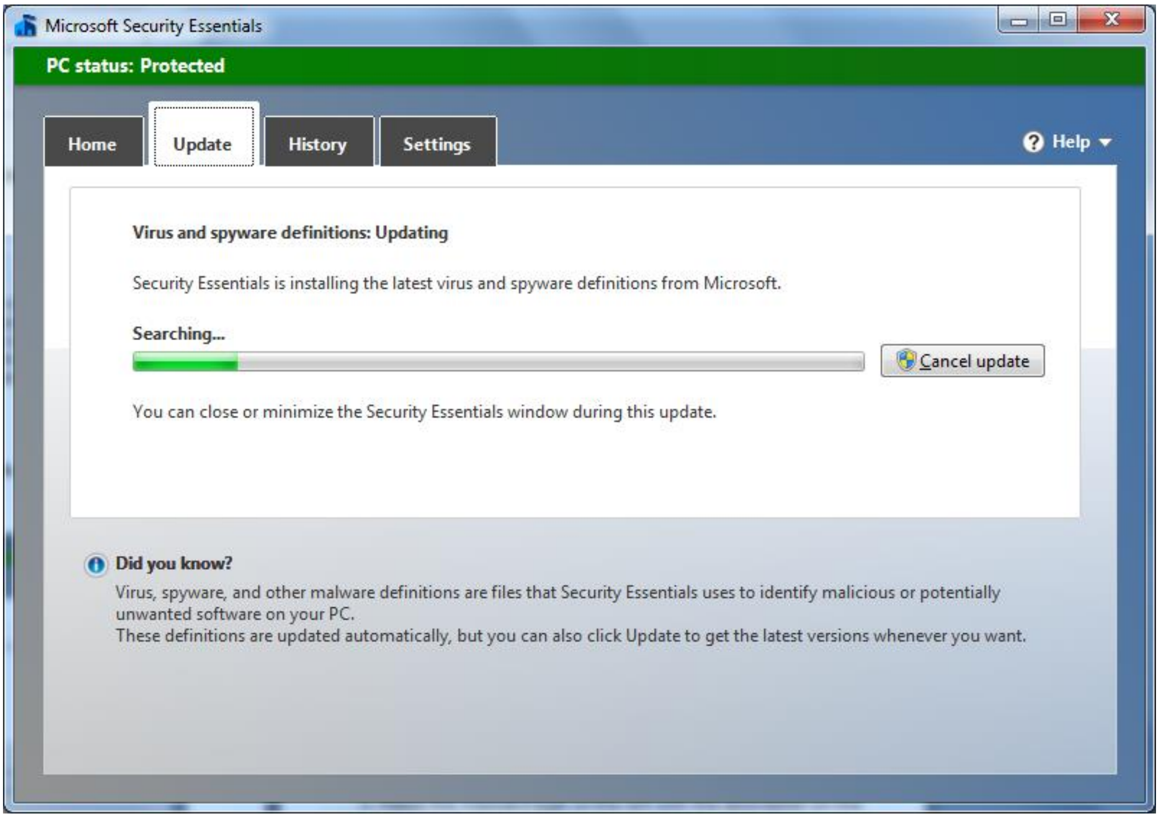
Security Essentials updates your virus and spyware definitions automatically to help protect your PC.

Definitions created on:	6/24/2012 at 11:58 PM
Definitions last updated:	6/25/2012 at 10:00 AM
Virus definition version:	1.129.387.0
Spyware definition version:	1.129.387.0

Did you know?

Virus, spyware, and other malware definitions are files that Security Essentials uses to identify malicious or potentially unwanted software on your PC.
These definitions are updated automatically, but you can also click Update to get the latest versions whenever you want.

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



Virus and spyware definitions: Updating

Security Essentials is installing the latest virus and spyware definitions from Microsoft.

Searching...

You can close or minimize the Security Essentials window during this update.

Did you know?

Virus, spyware, and other malware definitions are files that Security Essentials uses to identify malicious or potentially unwanted software on your PC.
These definitions are updated automatically, but you can also click Update to get the latest versions whenever you want.

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

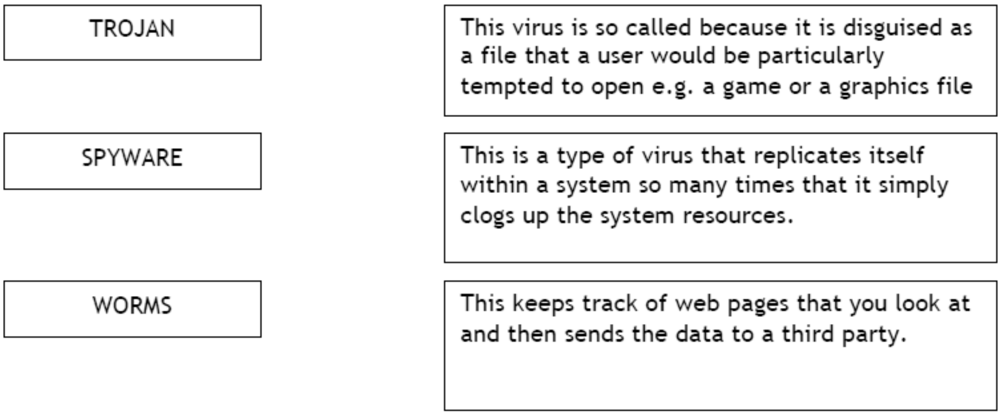
3. A network of infected computers used to distribute malware is known as:

    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

SPYWARE

WORMS

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

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

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 how to:

- Understand and recognize common network types
- Identify options for connecting to a network
- Understand wireless security
- Understand purpose of access control
- Identify common biometric security techniques

3.1 NETWORKS

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.

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.

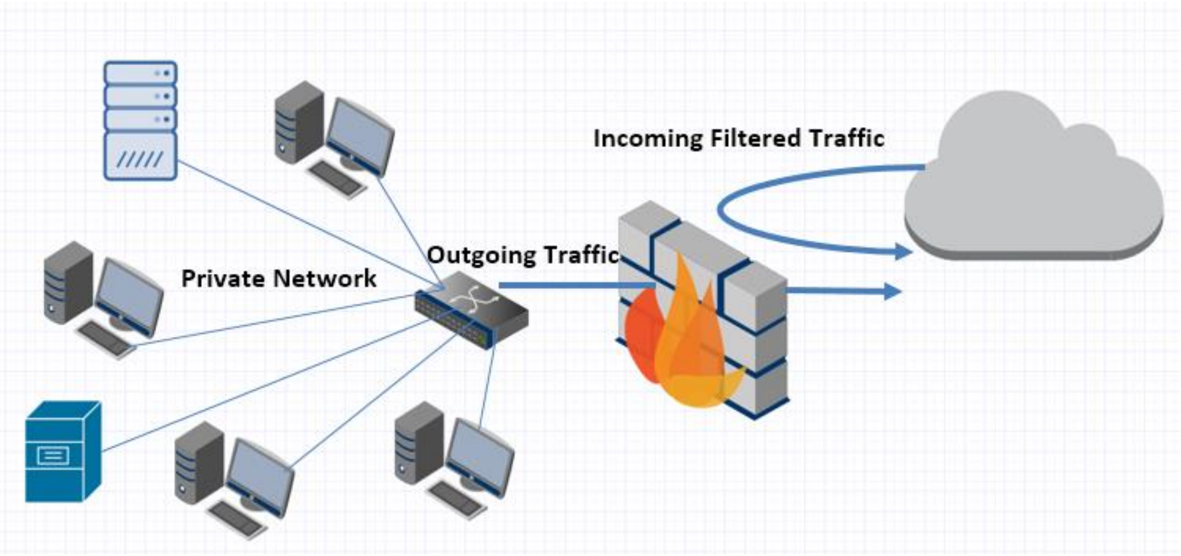
Security-related activities include:

- 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.

3.2 Network Connections

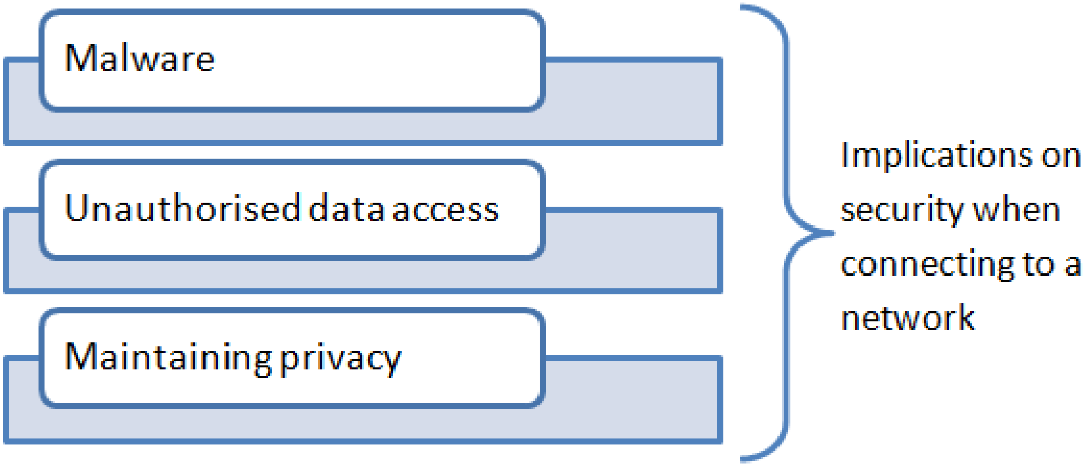
Options for connecting to a network include:

- A cable connection, for example using an Ethernet cable

- A wireless connection, for example using a laptop or mobile device.

Security Implications of Connecting to a Network

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.

3.3 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.

Types of Wireless Security

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. If you use a network that is not security using wireless security techniques, then you run the risk of an eavesdropper accessing your private data.

Common types of wireless security 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.

Connecting to Wireless Network

If you have a device such as a laptop, you can see a list of available wireless networks, and then connect to one of those networks, no matter where you are. The wireless networks appear only if your computer has a wireless network adapter installed and the adapter is turned on.

1. Click on the network icon (📶 or 🖧) in the taskbar notification area.

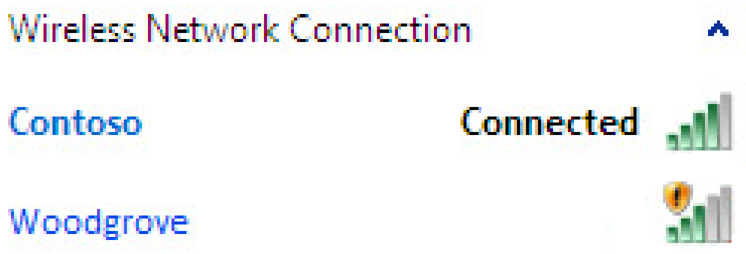
2. In the list of available wireless networks, click a network.

3. Click **Connect**.

Secured networks require a network security key or password. To connect to one of those networks, ask the network administrator or the service provider for the security key or password.

The list of available wireless networks indicates whether or not a network is secured. If you do connect to an unsecured network, you need to be aware that someone may be able to access your activity, including the websites you visit, the files you send and receive, and the user names and passwords you use.

When you view available wireless networks in Connect to a Network, wireless networks that are not security enabled are flagged with a yellow shield icon.



Wireless Network Connection

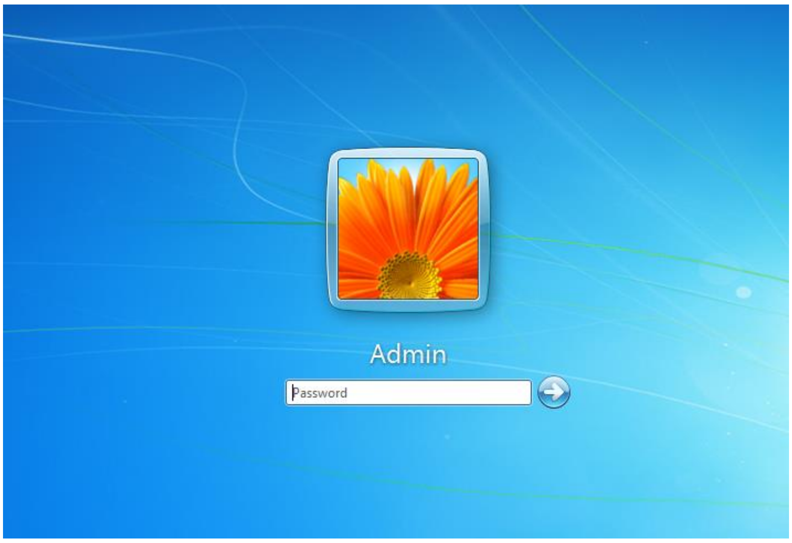
Contoso Connected

Woodgrove

3.4 ACCESS CONTROL

Network Accounts

A network account is needed for a user to access the network. A user is assigned rights and permissions together with the network account when the account is set up by a network administrator. This determines what the user can do on the network.



Windows log in screen

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.

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.

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.

3.5 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 unauthorized source
   c. Encrypt information
   d. Filter incoming information

3. List two 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

5. Which of the following biometric security method is considered the least expensive?

   a. Fingerprint scanning
   b. Facial recognition
   c. Eye scanning
   d. Voice recognition

LESSON 4 -
SECURE WEB USE

In this section, you will learn how to:

- Identify secure websites
- Be aware of pharming
- Validate digital certificate
- Understand appropriate setting for allowing and blocking cookies
- Understand types and purpose of content-control software

4.1 WEB BROWSING

There are a range of security considerations that you should keep in when browsing and carrying out transactions online.

Identify Secure Websites

Whenever you are asked to provide sensitive information on a website, you need to be able to identify if the page is secure or not. In particular, online activities such as online shopping or financial transactions should only be undertaken on secure web pages.

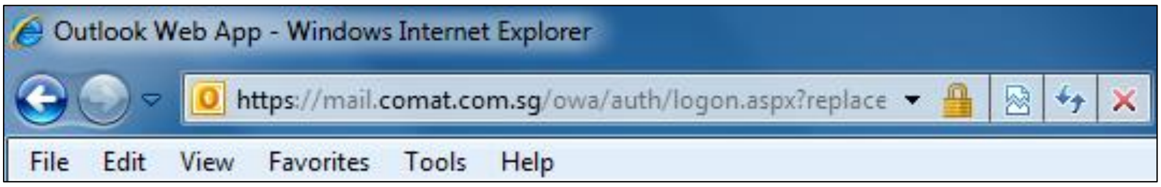
There are two commonly-used indications that a web page is secure:

- **The URL starts with https**

  Normally, when browsing the web, the URLs (or web page addresses) start with the letters http. However, over a secure connection the address displayed should start with https, indicating that a secure connection has been established between your computer and web server.

- **A lock icon is displayed**

  Web browsers generally display a lock icon somewhere in the window of the browser if the connection is secure.



Outlook Web App - Windows Internet Explorer

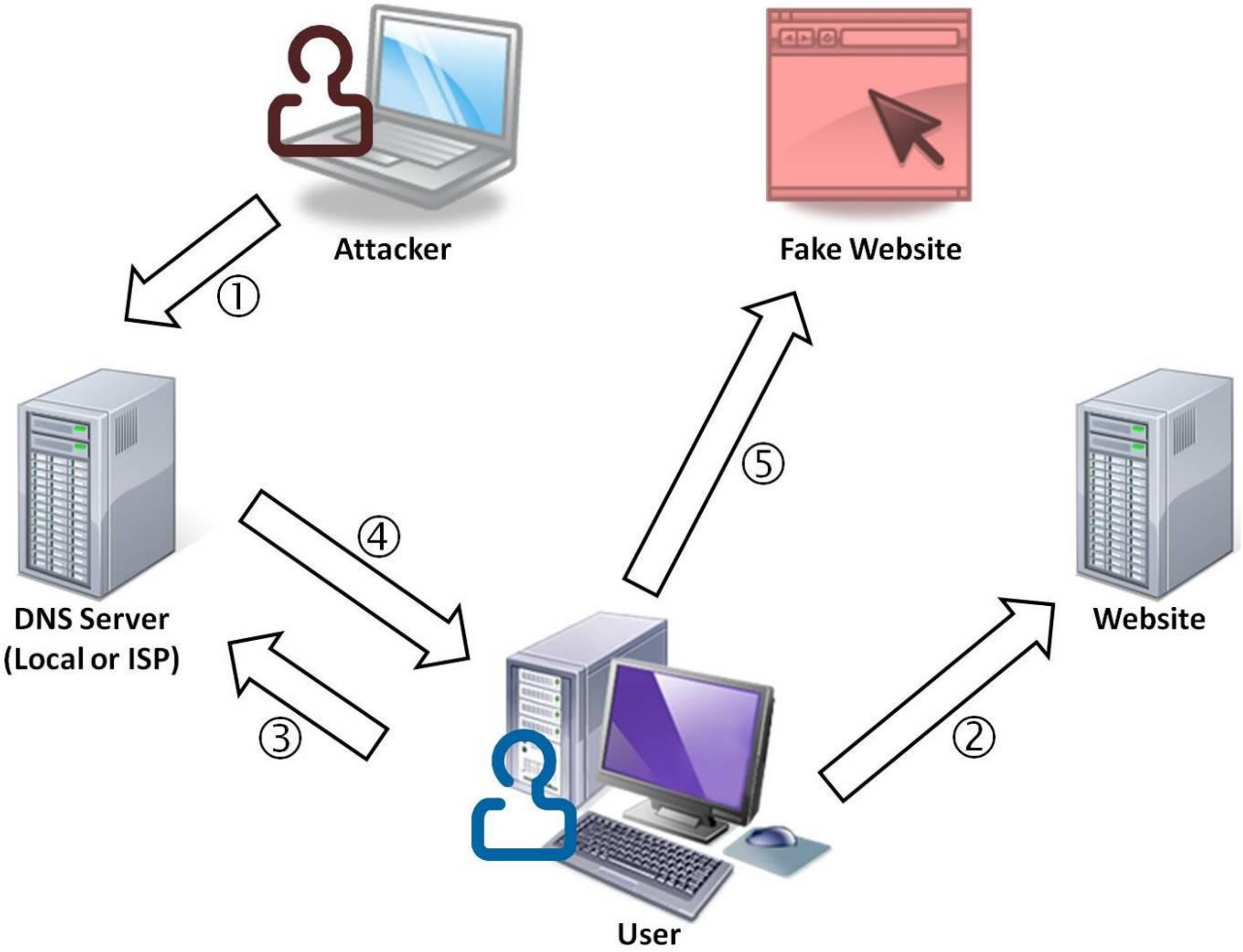
https://mail.comat.com.sg/owa/auth/logon.aspx?replace

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 carried 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.

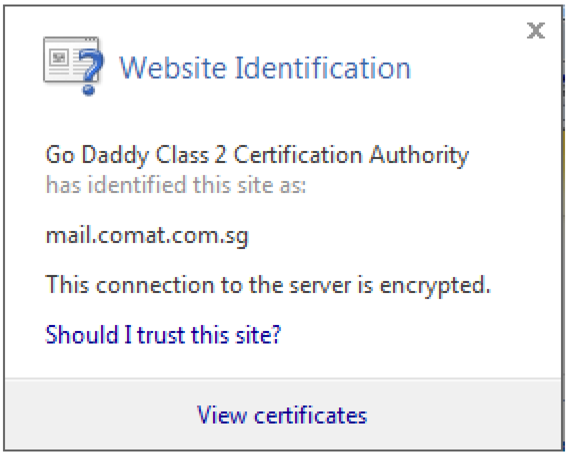
The user's computer now interprets the poisoned reply to be the correct IP address of the website. The user has now been tricked into visiting the fake website controlled by the attacker instead of the original website.

Digital Certificate

A digital certificate is an electronic document, issued by a certification authority that establishes a web site's credentials. The certificate contains the name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can check that the certificate is real.

To view a digital certificate:

1. Click on the lock icon in the web browser address bar.



Website Identification

Go Daddy Class 2 Certification Authority
has identified this site as:

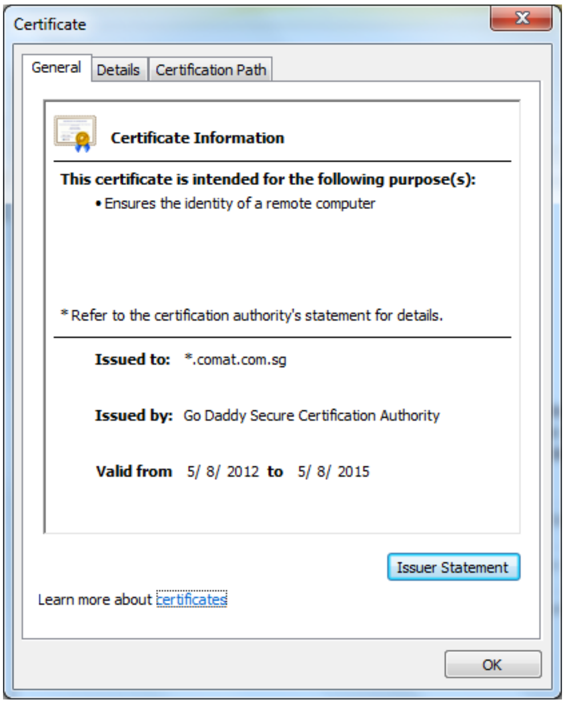
mail.comat.com.sg

This connection to the server is encrypted.

Should I trust this site?

View certificates

2. Click on the **View certificates** link.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.comat.com.sg

Issued by: Go Daddy Secure Certification Authority

Valid from 5/ 8/ 2012 to 5/ 8/ 2015

Issuer Statement

Learn more about certificates

OK

3. Click **OK**.

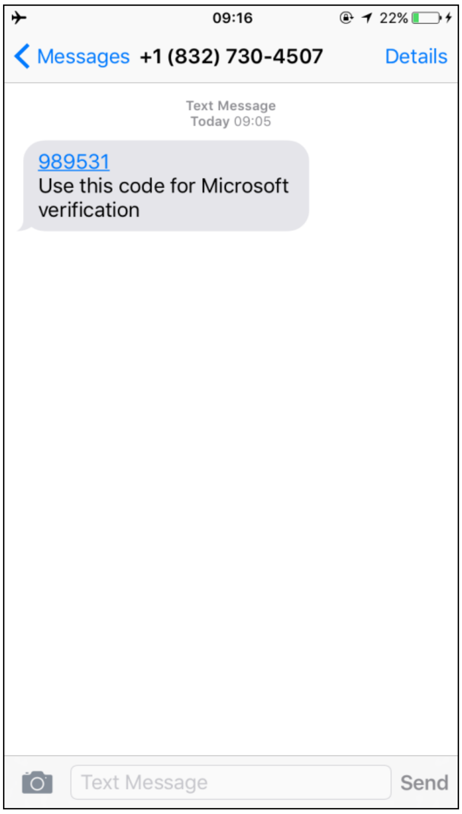
Popular authorized certificate retailers are VeriSign, SafeCert, Thawte, and Go Daddy.

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.



Text Message
Today 09:05

989531
Use this code for Microsoft verification

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.

Front

Back

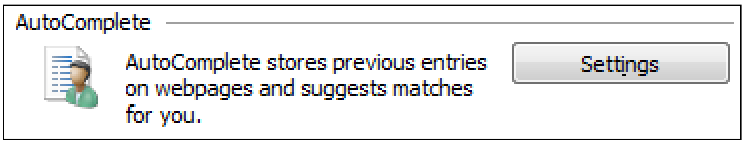
Setting AutoComplete Options

A browser's autocomplete function will save any words typed into browser fields and then suggest matches when you type again in those fields. This can save you time and be convenient – for example, your passwords and user names can be stored and recalled.

However, this is a security risk when you are using a shared or public computer, because other people could potential access this information. To prevent against this, you need to disable certain autocomplete features.

To Set AutoComplete Options:

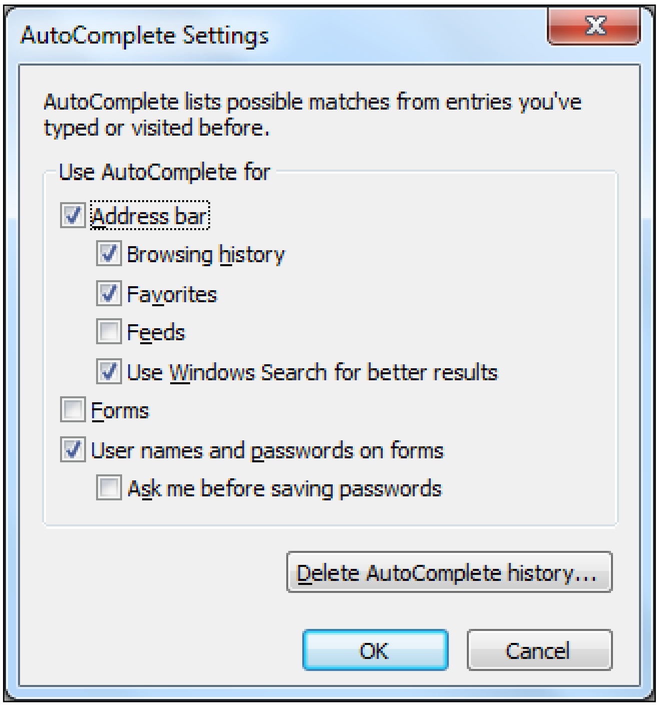
1. In Internet Explorer, click the **Tools** menu.
2. Click **Internet Options**.
3. Select the **Contents** tab.
4. Click on the **Settings** button in the AutoComplete section.



AutoComplete

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

5. Check or uncheck the appropriate options.



AutoComplete Settings

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

Use AutoComplete for

☑ Address bar
- ☑ Browsing history
- ☑ Favorites
- □ Feeds
- ☑ Use Windows Search for better results

□ Forms

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

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

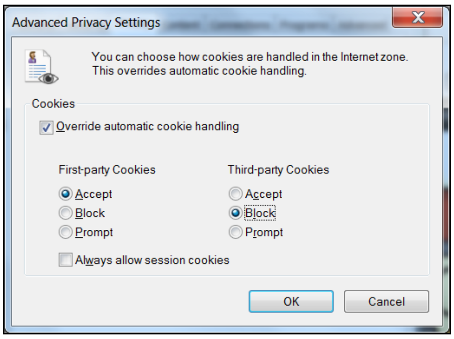
Cookies

A cookie is a piece of data stored by a website within a browser, and then later sent back to the same website by the browser.

Websites use cookies to offer a personalized and consistent experience to users and to gather information about website use. With a trusted website, cookies can improve your experience by allowing the site to learn your preferences or allowing you to skip having to sign in every time you use the site. However, some cookies, such as those associated with advertising, might put your privacy at risk by tracking sites you visit.

To block or allow cookies based on their type:

1. In Internet Explorer, click on **Tools** menu.
2. Click on **Internet Options**.
3. Select the **Privacy** tab.
4. Click the **Advanced** button.
5. Check / uncheck cookies options as required; for example, to block third party cookies (i.e. cookies from sites other than the one you are visiting).



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
● Accept	○ Accept
○ Block	● Block
○ Prompt	○ Prompt

□ Always allow session cookies

6. Click **OK**.

Clearing Private Data from a Browser

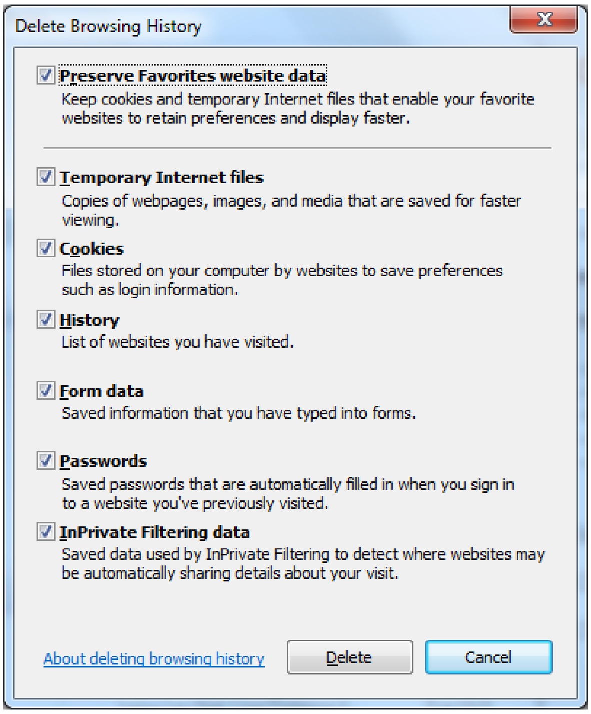
Browsers stores the following types of information on your computer or device:

- 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 use a public computer and do not want any of your personal details to be left behind, you should delete this information.

1. In Internet Explorer, click the **Tools** menu.

2. Click **Delete Browsing History….**



Delete Browsing History

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

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

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

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

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

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

☑ **InPrivate Filtering data**
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.

3. Select the required options to clear.

4. Click **Delete**.

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.

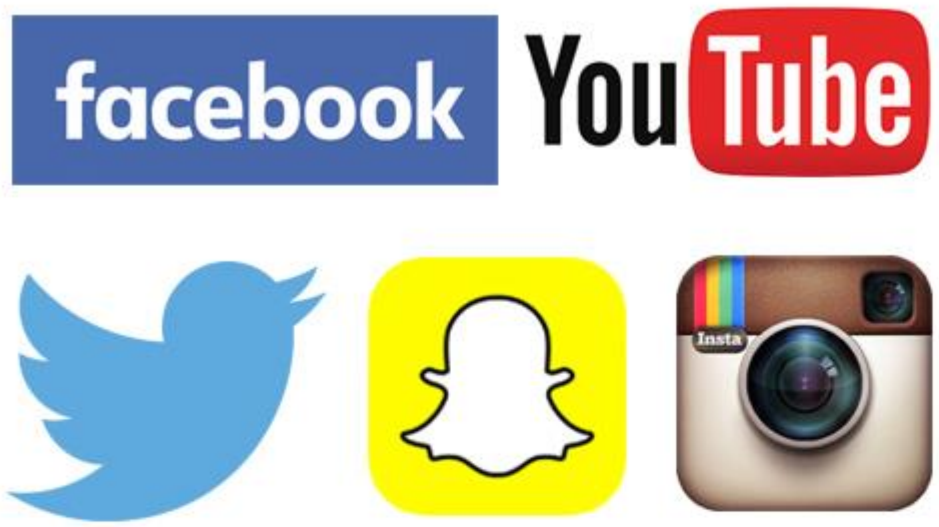
- **Content-limited (or filtered) ISPs**

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.

4.2 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.

You should always be aware of not disclosing confidential information when you are on social networking sites.

Examples of confidential information include passwords, PIN numbers, and personal financial information. If you are engaging in social networking activities relating to your work you also need to ensure that you do not disclose important company information, for example client details.

Disclosing such information could lead to personal information, company information, client information or finances being stolen or misused.

It is important to set appropriate account privacy settings. If your account is public, everyone will be able to view your personal details. Therefore, you need to review and change your privacy settings to ensure that personal details are hidden.

Other 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.

4.3 REVIEW EXERCISE

1. How do you identify a secure web site?

   ____

   ____

   ____

   ____

2. What is the purpose of a cookie?

   ____

   ____

   ____

   ____

3. List two potential dangers when using social networking sites.

   ____

   ____

4. Which of the following terms describes an attack in which the victim's computer is infected with malicious code that re-directs them to bogus websites?

   a. Phishing
   b. Malware
   c. Pharming
   d. Cookies

LESSON 5 - COMMUNICATIONS

In this section, you will learn how to:

- Understand purpose of encrypting and decrypting e-mail
- Create and add digital signature
- Identify common characteristics of phishing
- Recognise security risks associated with Instant Messaging

5.1 Encrypting and Decrypting E-Mail

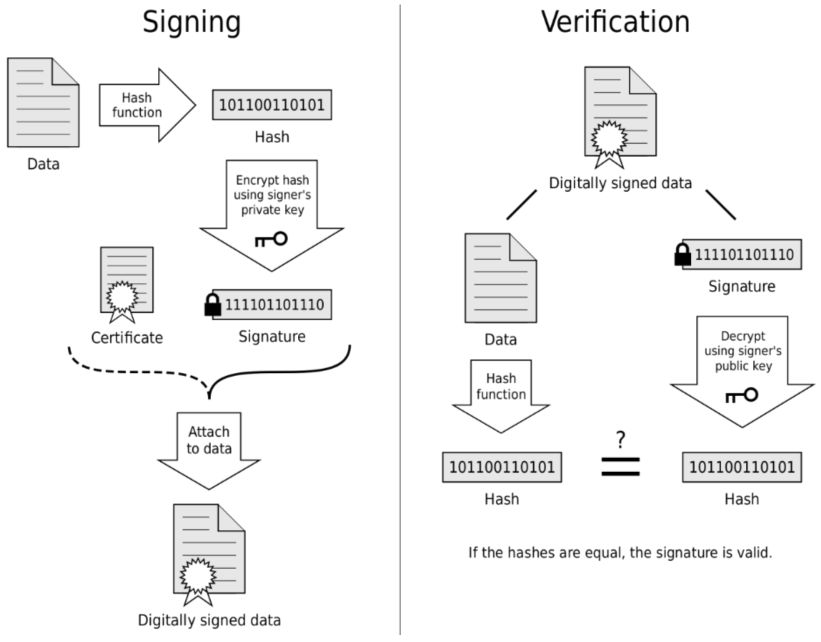
E-mail is a crucial tool for many individuals as well as organisations. There are important security considerations associated with using e-mail, however. You can take steps to ensure that your e-mail content is secure and to verify the identity of the sender of an e-mail. You also need to be aware of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

Encrypting 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.

5.2 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:

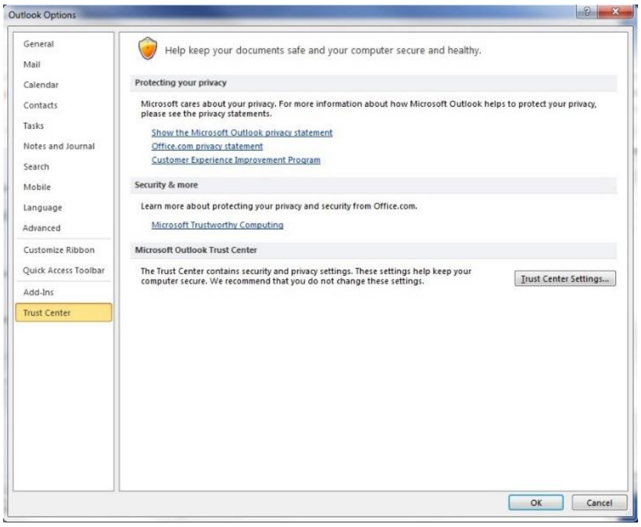


If you work in a large organisation, your employer may have obtained a digital ID for you. If you want to get a digital ID for your own use, you can get one from one of the many companies that issue and maintain Digital ID services.

You can also digitally sign your e-mail messages.

To digitally sign all outgoing messages in Microsoft Outlook 2010:

1. Click the **File** tab.
2. Click **Options**.
3. Click **Trust Centre**.



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

Protecting your privacy

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

Show the Microsoft Outlook privacy statement
Office.com privacy statement
Customer Experience Improvement Program

Security & more

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

Microsoft Trustworthy Computing

Microsoft Outlook Trust Center

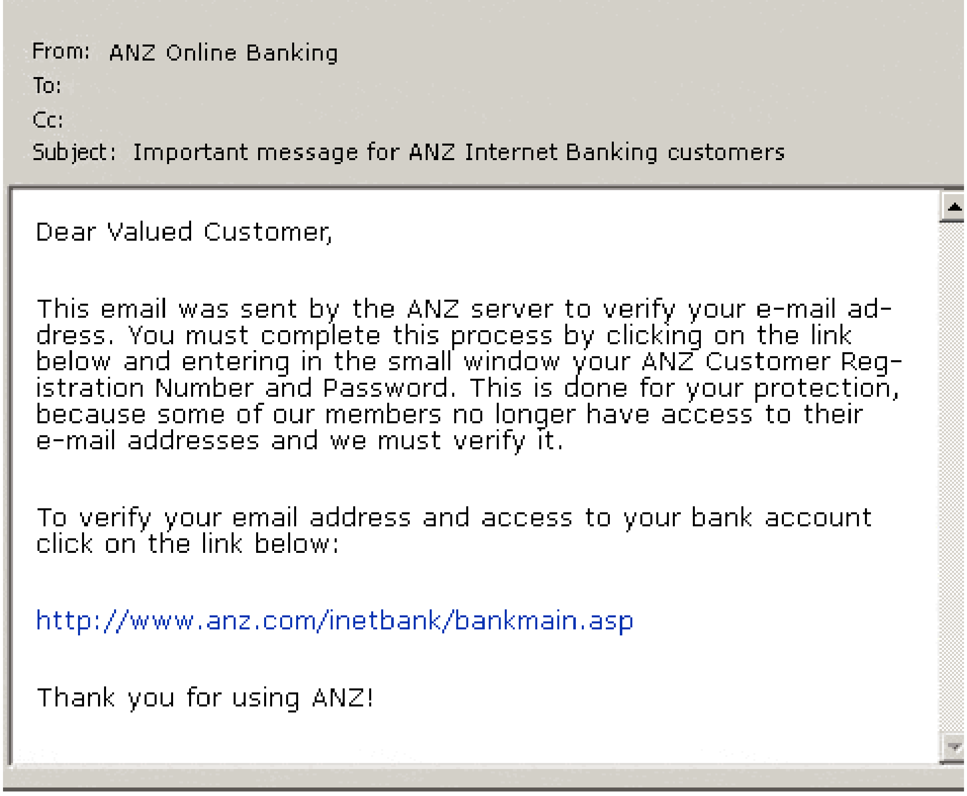
The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

4. Click **Trust Centre Settings**.
5. Click **E-mail Security**.
6. Under **Encrypted e-mail**, select **Add digital signature to outgoing messages**.
7. Click **OK**.
8. Click **OK**.

5.3 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.



From: ANZ Online Banking
To:
Cc:
Subject: Important message for ANZ Internet Banking customers

Dear Valued Customer,

This email was sent by the ANZ server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your ANZ Customer Registration Number and Password. This is done for your protection, because some of our members no longer have access to their e-mail addresses and we must verify it.

To verify your email address and access to your bank account click on the link below:

http://www.anz.com/inetbank/bankmain.asp

Thank you for using ANZ!

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:

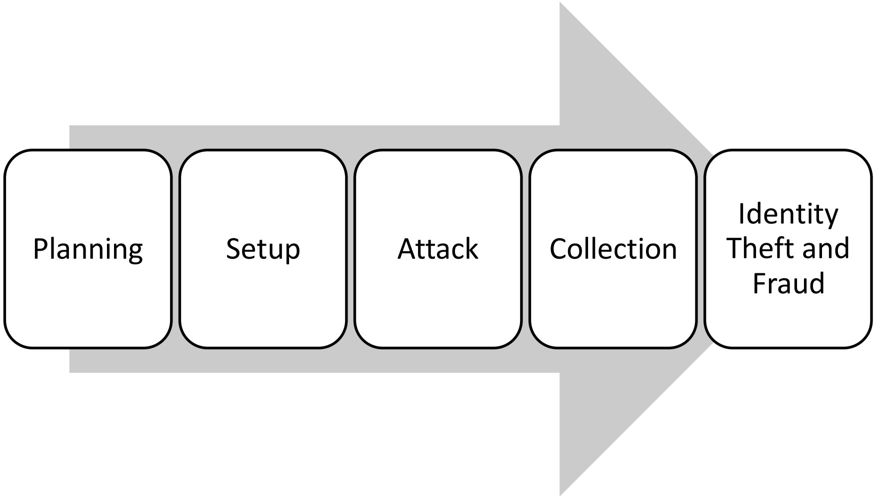
- Requests to forward the e-mail to many people.
- Unsubstantiated claims that many other people have won prizes or cash.

5.4 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.

5.5 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!

5.6 INSTANT MESSAGING

Instant messaging (IM) is a form of Internet communication that delivers an instantaneous transmission of text-based messages from sender to receiver. IM delivers a message to a contact instantly as long as the contact is online.

Most IM programs provide these features:

- **Instant messages**
  Send text messages back and forth with a contact who is online.

- **Web links**
  Share links to your favourite Web sites.

- **Video**
  Send and view videos, and chat face to face with contacts.

- **Images**
  Share images, for example photos taken by a mobile device.

- **Files**
  Share files by sending them directly to your contacts.

- **Talk**
  Use the VoIP telephony to actually talk with your contacts.

- **Mobile capability**
  Can be used on mobile devices, such as smart phones.

Some of the popular IM providers are Facebook Messenger, WhatsApp, and Google+ Hangouts.

Because IM networks not only transfer text messages but also files, IM can potentially transfer malware and provide an access point for backdoor Trojan horses. Hackers can get backdoor access to computers through IM, effectively bypassing desktop and perimeter firewall implementations. This can provide access to your computer or server, compromising your information.

Methods of ensuring confidentiality while using IM include:

- **Encryption**
  One of the best ways to secure the information being transmitted along via IM is to encrypt it, and some IM services offer encryption.

- **Non-disclosure of important details**
  In general, you should refrain from disclosing personal and sensitive details over IM. 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.

- **Restrict file sharing**
  Avoid sharing files or folders using UM as this can compromise security and facilitate the sharing of malware.

5.7 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 is a unique digital mark applied to a message?

    a. Encryption
    b. Decryption
    c. Pretexting
    d. Digital signature

3. Name two strategies that reduce security risks linked to using Instant Messaging:

    ____

    ____

    ____

    ____

LESSON 6 -
SECURE DATA MANAGEMENT

In this section, you will learn about:

- Securing and backing up data
- Secure destruction

6.1 SECURING AND BACKING UP DATA

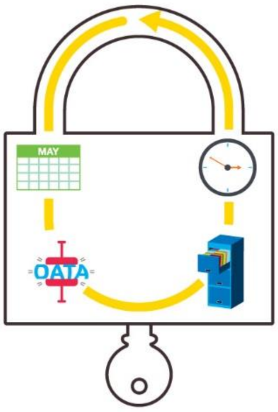
In offices and businesses, many devices – including PCs, laptops, and mobiles – may contain highly sensitive data pertaining to the company or may give access to the company network. If someone were to get hold of one of these devices, the results could be disastrous. Theft of company secrets, identity 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 organisations, 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.

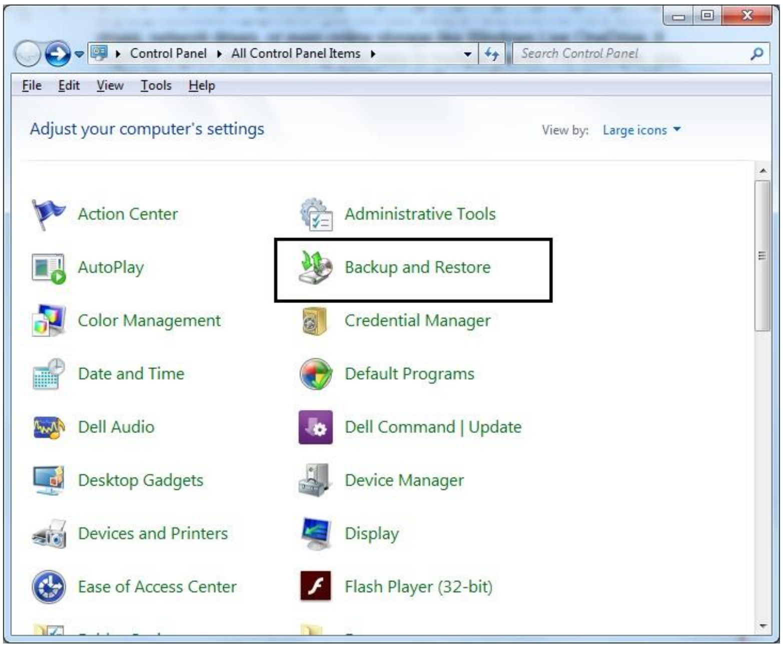
Regularity How often you create backups depends on the value of the data and the frequency with which the data changes. For example, if your data changes on a daily basis, a daily backup may be performed.

Back up Data

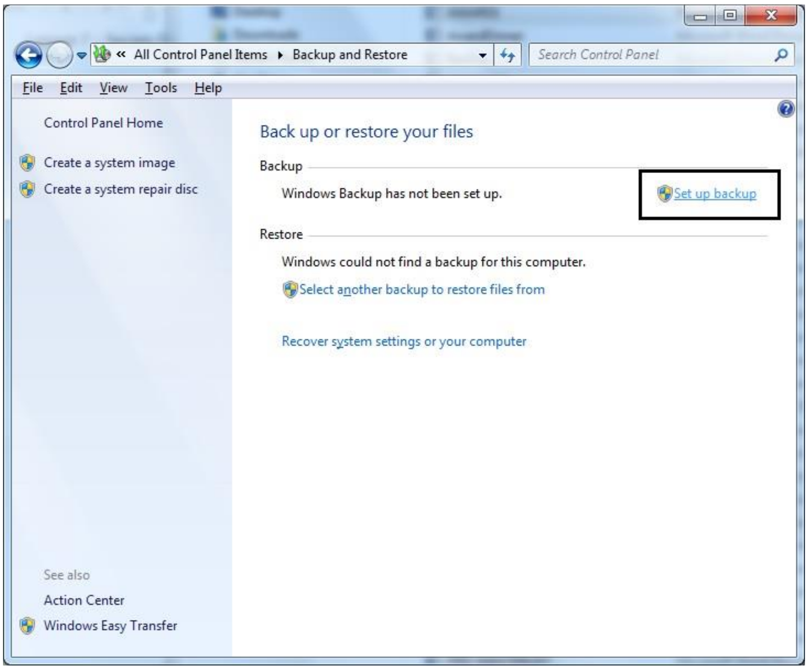
Nowadays, there are many options for backing up your content. You do not need any sophisticated equipment - you can use CDs, DVDs, external hard drives, flash drives, network drives, or even online storage like Microsoft OneDrive. It might be a good idea to back up your data to multiple places. For example, 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. In Windows 7, click the **Start** button.
2. Click the **Control Panel**.
3. Click the **Backup and Restore** button.



4. Click **Set up Backup**.


« All Control Panel Items ▸ Backup and Restore
Search Control Panel
File Edit View Tools Help
Control Panel Home
Create a system image
Create a system repair disc
See also
Action Center
Windows Easy Transfer
Set up backup
Select another backup to restore files from
Recover system settings or your computer

Back up or restore your files

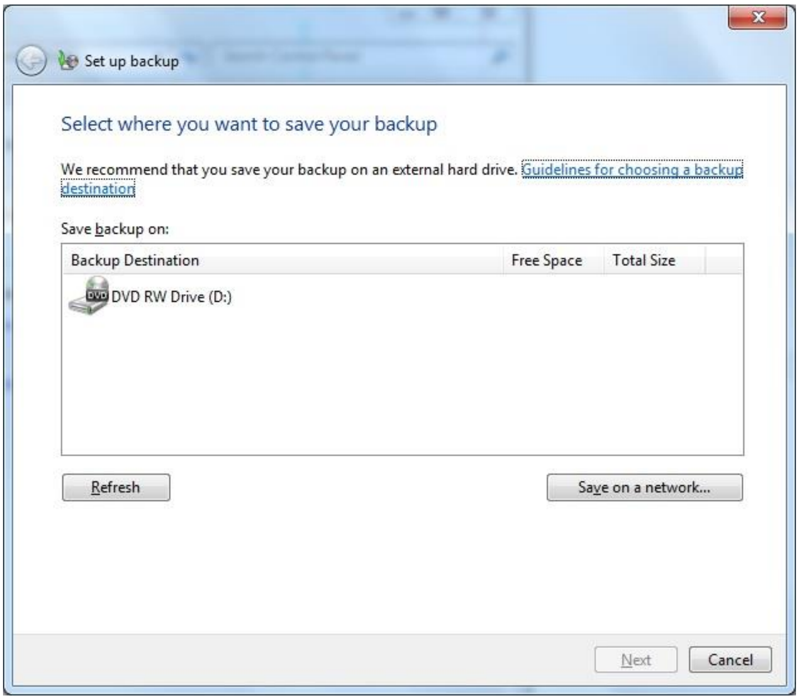
Backup

Windows Backup has not been set up.

Restore

Windows could not find a backup for this computer.

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



Set up backup

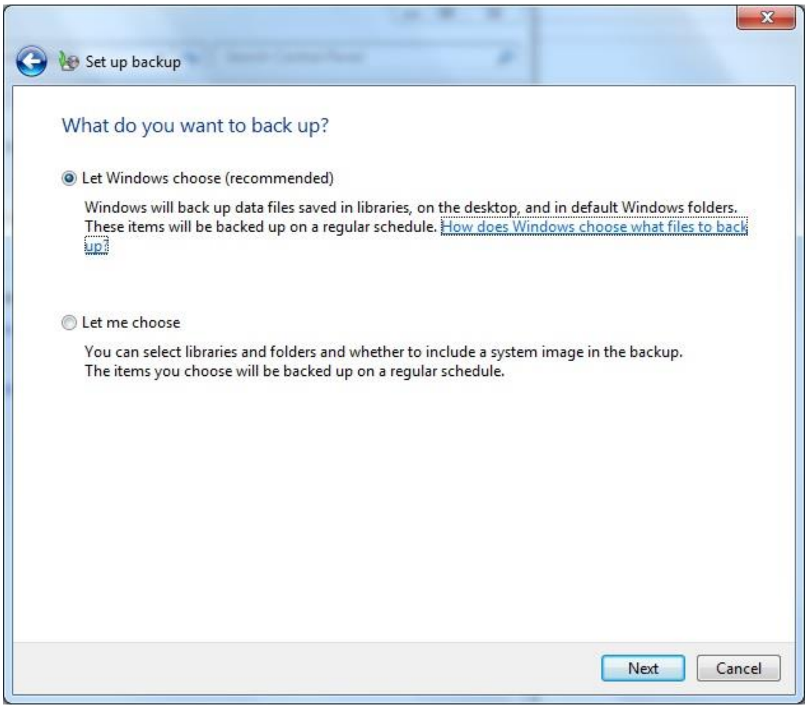
Select where you want to save your backup

We recommend that you save your backup on an external hard drive. Guidelines for choosing a backup destination

Save backup on:

Backup Destination	Free Space	Total Size
DVD RW Drive (D:)		

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



Set up backup

What do you want to back up?

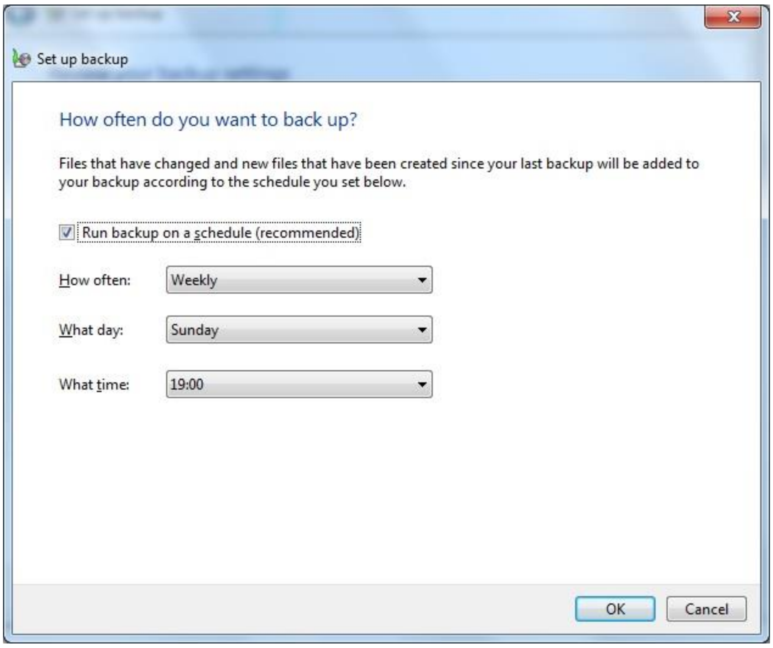
● Let Windows choose (recommended)

Windows will back up data files saved in libraries, on the desktop, and in default Windows folders. These items will be backed up on a regular schedule. How does Windows choose what files to back up?

○ Let me choose

You can select libraries and folders and whether to include a system image in the backup. The items you choose will be backed up on a regular schedule.

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



Set up backup

How often do you want to back up?

Files that have changed and new files that have been created since your last backup will be added to your backup according to the schedule you set below.

☑ Run backup on a schedule (recommended)

How often: Weekly

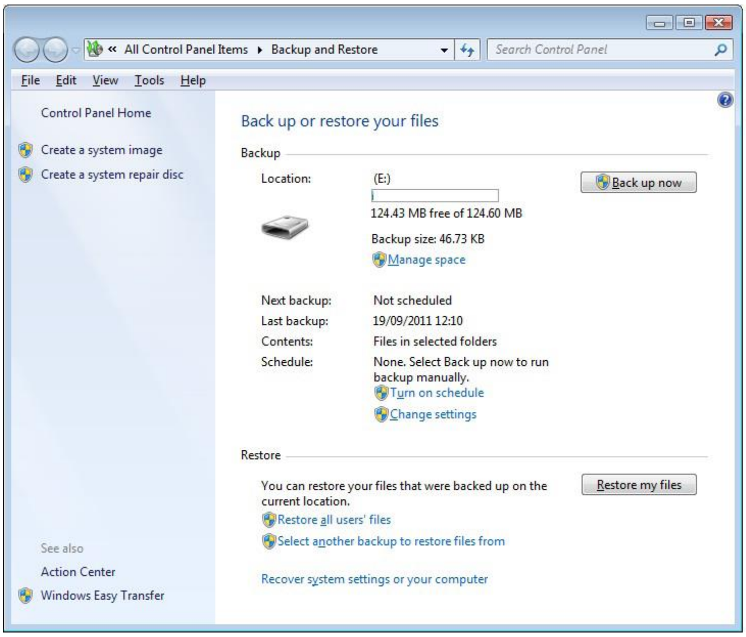
What day: Sunday

What time: 19:00

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

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

1. In Windows 7, 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.**



Back up or restore your files

Backup

Location: (E:)

124.43 MB free of 124.60 MB

Backup size: 46.73 KB

Next backup: Not scheduled

Last backup: 19/09/2011 12:10

Contents: Files in selected folders

Schedule: None. Select Back up now to run backup manually.

Restore

You can restore your files that were backed up on the current location.

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

6.2 SECURE 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.

6.3 REVIEW EXERCISE

1. Which of the following is not a features of 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. DVD
   d. Flash drive

3. Residual traces of deleted data that still remains is known as

   a. Degaussed data
   b. Data remanence
   c. Data permanence
   d. Data indexing

ICDL Syllabus

Ref	ICDL Task Item	Location
1.1.1	Distinguish between data and information.	*1.1 Data Threats*
1.1.2	Understand the term cybercrime.	*1.1 Data Threats*
1.1.3	Understand the difference between hacking, cracking and ethical hacking.	*1.1 Data Threats*
1.1.4	Recognise threats to data from force majeure like: fire, floods, war, earthquake.	*1.1 Data Threats*
1.1.5	Recognise threats to data from: employees, service providers and external individuals.	*1.1 Data Threats*
1.2.1	Understand the reasons for protecting personal information like: avoiding identity theft, fraud.	*1.2 Value of Information*
1.2.2	Understand the reasons for protecting commercially sensitive information like: preventing theft or misuse of client details, financial information.	*1.2 Value of Information*
1.2.3	Identify measures for preventing unauthorised access to data like: encryption, passwords.	*1.2 Value of Information*
1.2.4	Understand basic characteristics of information security like: confidentiality, integrity, availability.	*1.2 Value of Information*
1.2.5	Identify the main data/privacy protection, retention and control requirements in your country.	*1.2 Value of Information*

Ref	ICDL Task Item	Location
1.2.6	Understand the importance of creating and adhering to guidelines and policies for ICT use.	*1.2 Value of Information*
1.3.1	Understand the term social engineering and its implications like: information gathering, fraud, computer system access.	*1.3 Personal Security*
1.3.2	Identify methods of social engineering like: phone calls, phishing, shoulder surfing.	*1.3 Personal Security*
1.3.3	Understand the term identity theft and its implications: personal, financial, business, legal.	*1.3 Personal Security*
1.3.4	Identify methods of identity theft like: information diving, skimming, pretexting.	*1.3 Personal Security*
1.4.1	Understand the effect of enabling/ disabling macro security settings.	*1.4 File Security*
1.4.2	Set a password for files like: documents, compressed files, spreadsheets.	*1.4 File Security*
1.4.3	Understand the advantages and limitations of encryption.	*1.4 File Security*
2.1.1	Understand the term malware.	*2.1 Definition and Function of Malware*
2.1.2	Recognise different ways that malware can be concealed like: Trojans, rootkits and back doors.	*2.1 Definition and Function of Malware*
2.2.1	Recognise types of infectious malware and understand how they work like: viruses, worms.	*2.1 Definition and Function of Malware*

Ref	ICDL Task Item	Location
2.2.2	Recognise types of data theft, profit generating/extortion malware and understand how they work like: adware, spyware, botnets, keystroke logging and diallers.	*2.1 Definition and Function of Malware*
2.3.1	Understand how anti-virus software works and its limitations.	*2.2 Protection*
2.3.2	Scan specific drives, folders, files using anti-virus software. Schedule scans using anti-virus software.	*2.2 Protection*
2.3.3	Understand the term quarantine and the effect of quarantining infected/suspicious files.	*2.2 Protection*
2.3.4	Understand the importance of downloading and installing software updates, anti-virus definition files.	*2.2 Protection*
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*
3.1.2	Understand the role of the network administrator in managing the authentication, authorisation and accounting within a network.	*3.1 Networks*
3.1.3	Understand the function and limitations of a firewall.	*3.1 Networks*
3.2.1	Recognise the options for connecting to a network like: cable, wireless.	*3.2 Network Connections*

Ref	ICDL Task Item	Location
3.2.2	Understand how connecting to a network has implications for security like: malware, unauthorised data access, maintaining privacy.	*3.2 Network Connections*
3.3.1	Recognise the importance of requiring a password for protecting wireless network access.	*3.3 Wireless Security*
3.3.2	Recognise different types of wireless security like: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).	*3.3 Wireless Security*
3.3.3	Be aware that using an unprotected wireless network can allow wireless eavesdroppers to access your data.	*3.3 Wireless Security*
3.3.4	Connect to a protected/unprotected wireless network.	*3.3 Wireless Security*
3.4.1	Understand the purpose of a network account and how it should be accessed through a user name and password.	*3.4 Access Control*
3.4.2	Recognise good password policies, like: not sharing passwords, changing them regularly, adequate password length, adequate letter, number and special characters mix.	*3.4 Access Control*
3.4.3	Identify common biometric security techniques used in access control like: fingerprint, eye scanning.	*3.4 Access Control*
4.1.1	Be aware that certain online activity (purchasing, financial transactions) should only be undertaken on secure web pages.	*4.1 Web Browsing*

Ref	ICDL Task Item	Location
4.1.2	Identify a secure website like: https, lock symbol.	*4.1 Web Browsing*
4.1.3	Be aware of pharming.	*4.1 Web Browsing*
4.1.4	Understand the term digital certificate. Validate a digital certificate.	*4.1 Web Browsing*
4.1.5	Understand the term one-time password.	*4.1 Web Browsing*
4.1.6	Select appropriate settings for enabling, disabling autocomplete, autosave when completing a form.	*4.1 Web Browsing*
4.1.7	Understand the term cookie.	*4.1 Web Browsing*
4.1.8	Select appropriate settings for allowing, blocking cookies.	*4.1 Web Browsing*
4.1.9	Delete private data from a browser like: browsing history, cached internet files, passwords, cookies, autocomplete data.	*4.1 Web Browsing*
4.1.10	Understand the purpose, function and types of content-control software like: internet filtering software, parental control software.	*4.1 Web Browsing*
4.2.1	Understand the importance of not disclosing confidential information on social networking sites.	*4.2 Social Networking*
4.2.2	Be aware of the need to apply appropriate social networking account privacy settings.	*4.2 Social Networking*

Ref	ICDL Task Item	Location
4.2.3	Understand potential dangers when using social networking sites like: cyber bullying, grooming, misleading/ dangerous information, false identities, fraudulent links or messages.	*4.2 Social Networking*
5.1.1	Understand the purpose of encrypting, decrypting an e-mail.	*5.1 Encrypting and Decrypting E-Mail*
5.1.2	Understand the term digital signature.	*5.2 Digital Signature*
5.1.3	Create and add a digital signature.	*5.2 Digital Signature*
5.1.4	Be aware of the possibility of receiving fraudulent and unsolicited e-mail.	*5.3 Receiving Fraudulent and Unsolicited E-Mail*
5.1.5	Understand the term phishing. Identify common characteristics of phishing like: using names of legitimate companies, people, false web links.	*5.4 Phishing*
5.1.6	Be aware of the danger of infecting the computer with malware by opening an e-mail attachment that contains a macro or an executable file.	*5.5 E-Mail and Malware*
5.2.1	Understand the term instant messaging (IM) and its uses.	*5.6 Instant Messaging*
5.2.2	Understand the security vulnerabilities of IM like: malware, backdoor access, access to files.	*5.6 Instant Messaging*
5.2.3	Recognise methods of ensuring confidentiality while using IM like: encryption, non-disclosure of important information, restricting file sharing.	*5.6 Instant Messaging*

Ref	ICDL Task Item	Location
6.1.1	Recognise ways of ensuring physical security of devices like: log equipment location and details, use cable locks, access control.	*6.1 Securing and Backing up Data*
6.1.2	Recognise the importance of having a back-up procedure in case of loss of data, financial records, web bookmarks/history.	*6.1 Securing and Backing up Data*
6.1.3	Identify the features of a back-up procedure like: regularity/frequency, schedule, storage location.	*6.1 Securing and Backing up Data*
6.1.4	Back up data.	*6.1 Securing and Backing up Data*
6.1.5	Restore and validate backed up data.	*6.1 Securing and Backing up Data*
6.2.1	Understand the reason for permanently deleting data from drives or devices.	*6.2 Secure Destruction*
6.2.2	Distinguish between deleting and permanently destroying data.	*6.2 Secure Destruction*
6.2.3	Identify common methods of permanently destroying data like: shredding, drive/media destruction, degaussing, using data destruction utilities.	*6.2 Secure Destruction*

Congratulations! You have reached the end of the ICDL IT Security book.

You have learned about the key skills relating to ensure security when online, including:

- 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.

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

Advanced Information Technology Institute - Ghana-India Kofi Annan Centre of Excellence in ICT
AITI-KACE, PMB State House
Second Avenue, Accra
Ghana
icdlafrica.org