Curriculum Topic 15 out of 15:

SYSTEM SECURITY, ICT ETHICAL ISSUES AND EMERGING TECHNOLOGIES

Background

- As computers get involved in almost all aspects of our lives, there are quite a number of emerging issues that need extra attention. Such emerging issues range from computer system features, environmental concerns, legal and ethical issues, system security and users of computer applications.
- Therefore, it is increasingly becoming important that students of ICT learn how to safeguard their computer systems, uphold ethical values while using ICT systems as they explore emerging technologies.
- **Learning Outcome:** The learner should be able to explain and discuss the emerging issues, computer security and privacy issues.

Presentation Outline

UACE Sub – ICT Topic 15:

System Security, ICT Ethical Issues and Emerging Technologies

- Sub Topic 1. Computer System Security
- Sub Topic 2. Privacy and ICT Ethical Issues
- Sub Topic 3. Emerging Technologies
- Sub Topic 4. ICT Industry

Sub Topic 1: Computer System Security

Sub topic Objectives:

a. Computer security

i. Explaining the various forms of computer security (data and physical security).

ii. Identifying security threats for (hardware and software).

iii. Explaining the meaning of a computer virus.

iv. Explaining how viruses are spread on standalone and networked computers.

b. Internet and network attacks

v. Explaining the concept of hacking.

vi. Explaining how denial of service attacks, backdoors, spoofing are carried out.

c. Data protection in computer systems

vii. Identifying appropriate ways of protecting data in computer systems.

d. Computer crime

viii. Identifying types of computer crimes

a. Computer security

i. Forms of computer security (data and physical security)

- ***Data Security*** *refers to protective measures that are applied to ensure integrity, availability and confidentiality of data or information*.
  - **Integrity** means prevention of unauthorized modification of data and data corruption. ***Data corruption*** *refers to errors in data that may occur during reading, writing, processing, storage or transmission of said data which may introduce unintended/unwanted changes to the original data*.
  - **Availability** means prevention of unauthorized withholding of data access (Intended users can access whenever they need to access).
  - **Confidentiality** means to avoid unauthorized disclosure of data third parties.

a. Computer security

i. Forms of computer security (data and physical security)

- **Physical Security** refers to the measures put in place by protect computer systems from physical damage and mitigate physical security risks. Physical security includes:
- Locked doors.
- Burglar proofs.
- Parameter fences.
- Security guards.
- Server room environmental protection, optimisation.
- Concrete walls.
- Lightening conductors.
- Fire extinguishers.
- Strategic server and storage placement, etc.

a. Computer security
ii. Security threats for (hardware and software)

- What is a computer security risk?
  - **Action that causes loss of or damage to computer system**

a. Computer security
ii. Security threats for (hardware and software)

- Security threats to computers-based information systems, private or confidential data include:
  - system failure
  - information theft
  - hardware theft
  - software theft
  - Internet and network attacks such as hackers
  - Malicious programs (computer viruses, worms and trojan horses)
  - unauthorised access and use
  - unauthorized alteration,
  - Malicious destruction of hardware, software, data or network resources, as well as sabotage.

a. Computer security
ii. Security threats for (hardware and software)

Information system failure

- Some of the causes of computerized information system failure include
  1. Hardware failure due to improper use.
  2. Unstable power supply as result of brownout or blackout and vandalism.
  3. Network breakdown.
  4. Natural disasters
  5. Program failure

Control measures against hardware failure

- Protect computers against brownout or blackout which may cause physical damages or data loss
  by using surge protectors and Uninterruptible power supply (UPS).
- For critical systems, most
  organizations have put into place fault tolerant systems. A **fault tolerant system** has redundant or duplicate storage, peripherals devices and software that provide a fail-over capability to backup components in the event of system failure.

  Disaster recovery plans

  Disaster recovery plan involves establishing offsite storage of an organization's databases so that
  in case of disaster or fire accidents, the company would have backup copies to reconstruct lost
  data

  Data backup

a. Computer security
ii. Security threats for (hardware and software)

- Hardware theft and hardware vandalism

➢ **Hardware theft is act of stealing computer equipment**

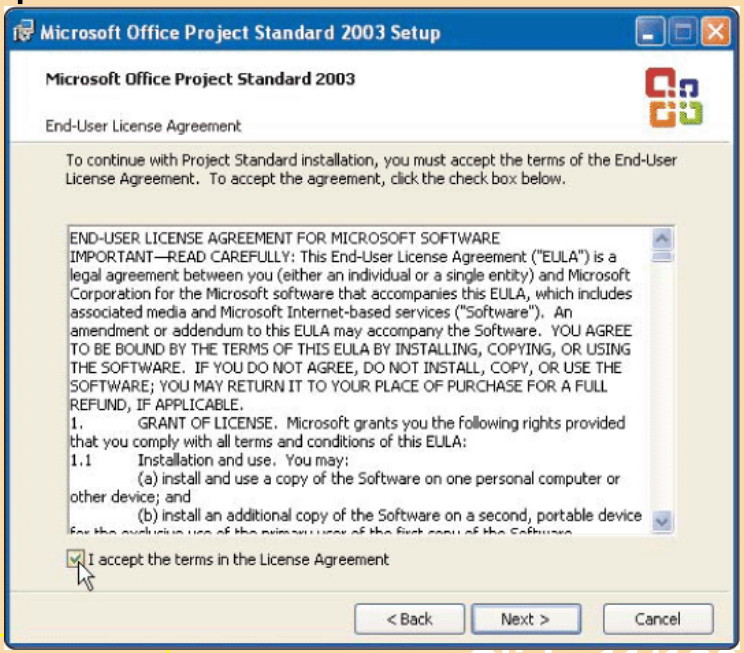
- Cables sometimes used to lock equipment
- Some notebook computers use passwords, possessed objects, and biometrics as security methods
- For PDAs, you can password-protect the device

➢ **Hardware vandalism is the act of defacing or destroying computer equipment**

a. Computer security
ii. Security threats for (hardware and software)

- **Software theft** **is** the act of stealing or illegally copying software or intentionally erasing programs.
- **Software piracy** is illegal duplication of copyrighted software.
- To guard against software theft and piracy, product activation is used.
- **Product activation** allows user to input product identification number online or by phone and receive unique installation identification number.

- A **license agreement** gives the right to use software. Single-user license agreement allows user to install software on one computer, make backup copy, and sell software after removing from computer.



a. Computer security
ii. Security threats for (hardware and software)

- **Internet and Network Attacks**
- Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises. In an organization, network administrators usually take measures to protect a network from security risks. On the Internet, where no central administrator is present, the security risk is greater.
- Internet and network attacks that jeopardize security include computer viruses, worms, Trojan horses, and rootkits; botnets; denial of service attacks; back doors; and spoofing.

a. Computer security

ii. Security threats for (hardware and software)

- **Unauthorized access and Use**
  - **Unauthorized access** is the use of a computer or network without permission. **Unauthorized use** is the use of a computer or its data for unapproved or possibly illegal activities.
  - Unauthorized use includes a variety of activities: an employee using an organization's computer to send personal e-mail messages, or someone gaining access to a bank computer and performing an unauthorized transfer.

a. Computer security
ii. Security threats for (hardware and software)

Information theft

- Information theft is yet another type of computer security risk. **Information theft** occurs when someone steals personal or confidential information. An unethical company executive may steal or buy stolen information to learn about a competitor. A corrupt individual may steal credit card numbers to make fraudulent purchases.
- **Safeguards against Information Theft:** Most companies attempt to prevent information theft by implementing the user identification and authentication controls.
- To protect information on the Internet and networks, companies and individuals use a variety of encryption techniques.

a. Computer security
iii. Explaining the meaning of a computer virus.

- A computer virus is a potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user's knowledge or permission. Once the virus infects the computer, it can spread throughout and may damage files and system software, including the operating system.
- Computer viruses, worms, Trojan horses, and rootkits are classified as **malware** (short for malicious software)
- Unscrupulous programmers write malware and then test it to ensure it can deliver its payload. The **payload** is the destructive event or prank the program is intended to deliver.

a. Computer security
iii. Explaining the meaning of a computer virus.

- What is the difference between viruses, worms, and rootkit and Trojan horses?

Virus is a potentially damaging computer program

Can spread and damage files

Worm copies itself repeatedly, using up resources and possibly shutting down computer or network

A **rootkit** is a program that hides in a computer and allows someone from a remote location to take full control of the computer.

Trojan horse hides within or looks like legitimate program until triggered

Does not replicate itself on other computers

a. Computer security
iii. Explaining the meaning of a computer virus.

- Macro Viruses

- Macros are procedures / instructions saved in an application, such as word processing or spreadsheet program.

- To protect the system from a macro viruses: Set macro security level in applications that displays warning that opened document contains macro.

iii. Explaining the meaning of a computer virus.

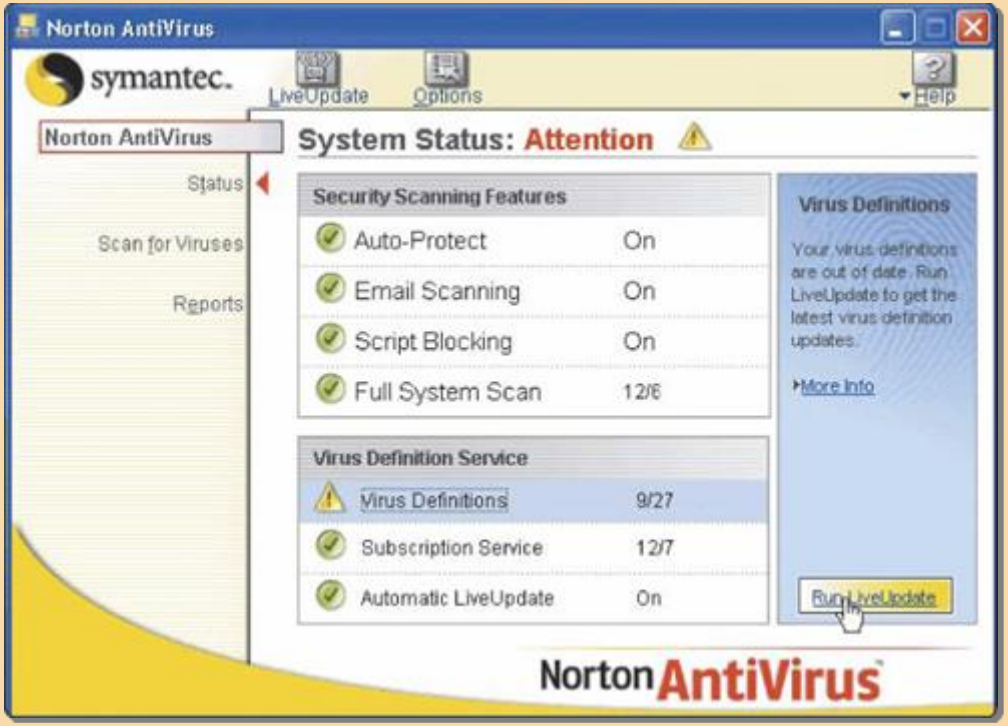
Symptoms of computer infected by viruses

- Operating system runs much slower than usual
- Available memory is less than expected
- Files become corrupted
- Screen displays unusual message or image
- Unknown programs or files mysteriously appear
- Music or unusual sound plays randomly
- Existing programs and files disappear
- Programs or files do not work properly
- System properties change
- Operating system does not start up
- Operating system shuts down unexpectedly

a. Computer security

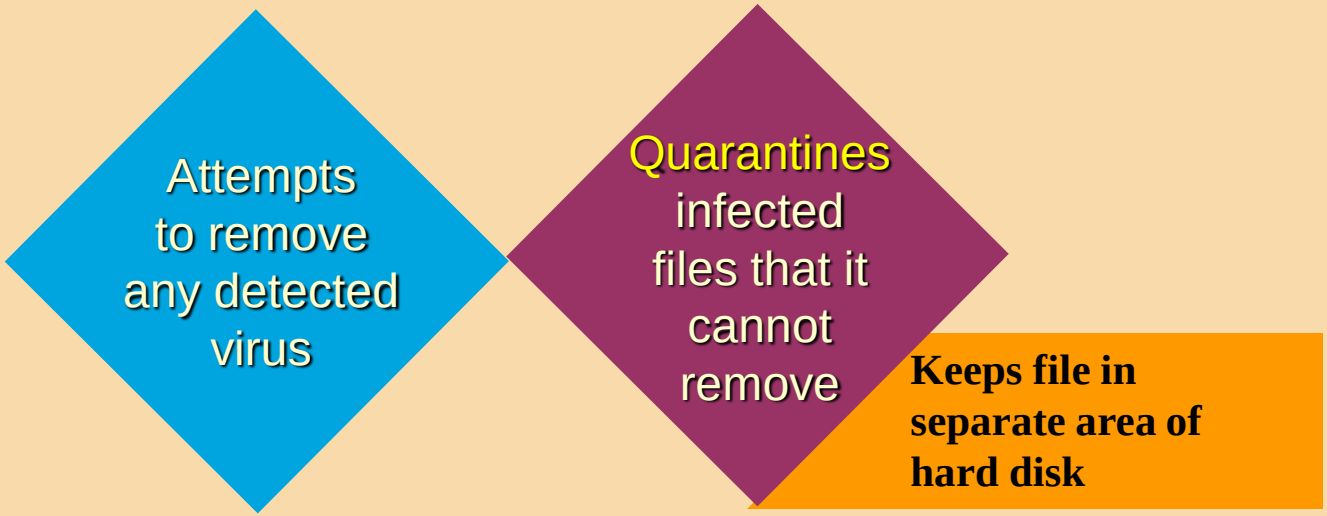
iii. Explaining the meaning of a computer virus.

- What is a virus signature?
  - **Specific pattern of virus code**
    - Also called **virus definition**
  - **Antivirus programs look for virus signatures**
  - an antivirus program **Identifies and removes computer viruses**
  - **Most also protect against worms and Trojan horses**



a. Computer security
iii. Explaining the meaning of a computer virus.

- What happens if an antivirus program identifies an infected file?

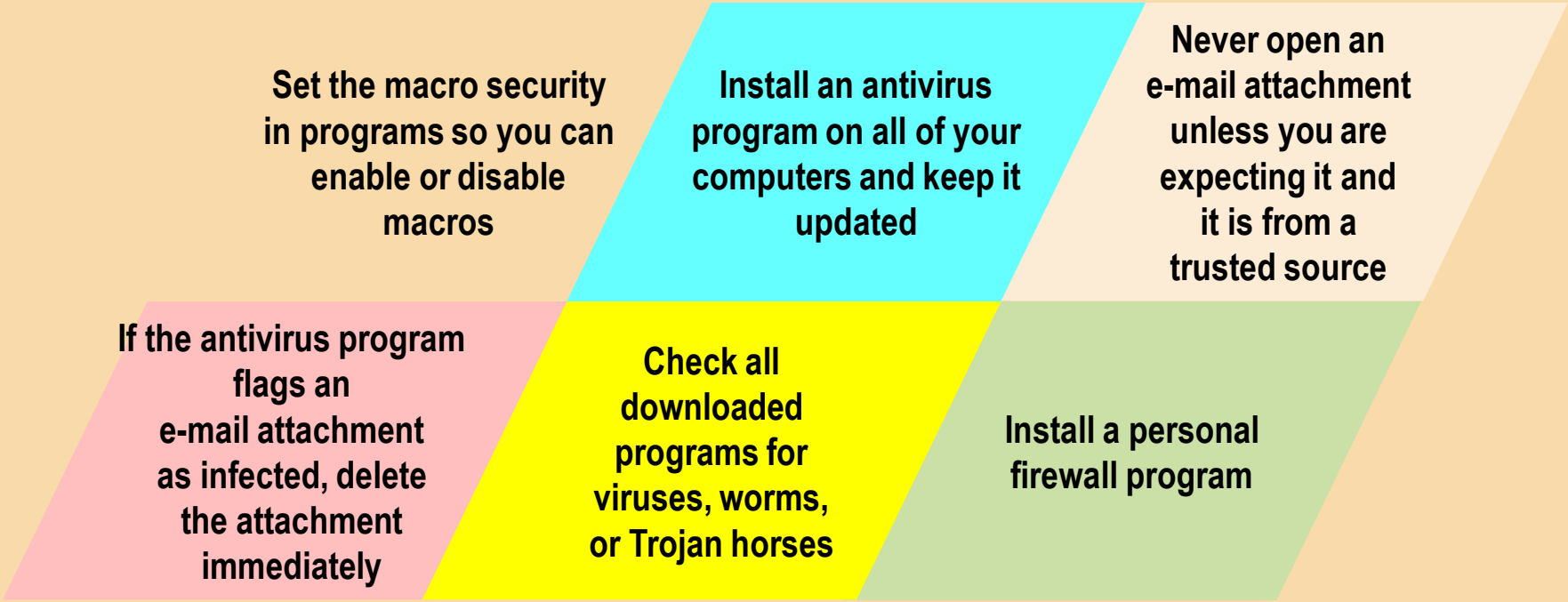


- Control measures against viruses

- To protect an information system against viruses:
- Install the latest versions of anti-virus software on the computers. Make sure that you continuously update the anti-virus software with new virus definition to counter the new viruses.
- Always scan removable storage media for viruses before using them.
- Scan mail attachments for viruses before opening or downloading an attachment.
- Always keep a **Recovery Disk**: A Removable disk that contains uninfected copy of key operating system commands
  that enables computer to restart. Also called rescue disk

iii. Explaining the meaning of a computer virus.

•What are some tips for preventing virus, worm, macro virus and Trojan horse infections?



iv. How viruses are spread on standalone and networked computers.

- Standalone computer is one which is not connected to any other computer. However networked computer is the one which is connected to any other computer for the purpose of exchanging data, information or resources. The table below shows some ways how viruses spread on standalone and networked computers.

Standalone computer	**Networked computer**
1.Distributed through flash disks	1.Through downloading email attachment
2.By using floppy diskettes	2.Playing games on internet
3.Through opening infected programs or documents on CR/DVD discs	3.Downloading infected files from internet

iv. How viruses are spread on standalone and networked computers.

v. The concept of hacking.

Hacking and cracking

- The term hacker refers to someone who accesses a computer or network illegally. Originally it was a complimentary word for a computer enthusiast.
- A cracker also is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action.
- Both hackers and crackers have advanced computer and network skills.
- Some hackers claim the intent of their security breaches is to improve security, and may be hired by software companies to test the security of new software systems.

v. The concept of hacking.

- A **script kiddie** has the same intent as a cracker but does not have the technical skills and knowledge. Script kiddies often use prewritten hacking and cracking programs to break into computers.
- A **cyber extortionist** is someone who uses e-mail as a vehicle for extortion.
- A **cyber terrorist** is someone who uses the Internet or network to destroy or damage computers for political reasons. The cyber terrorist might target the nation's air traffic control system, electricity-generating companies, or a telecommunications infrastructure.

vi. Explaining how denial of service attacks, backdoors, spoofing are carried out.

- A **denial of service attack**, or **DoS attack**, is an assault whose purpose is to disrupt computer access to an Internet service.
- The attackers may use an unsuspecting computer to send an influx of confusing data messages or useless traffic to a computer network. The victim computer network slows down considerably and eventually becomes unresponsive or unavailable, blocking legitimate visitors from accessing the network.
- Perpetrators have a variety of motives for carrying out a DoS attack. Those who disagree with the beliefs or actions of a particular organization claim political anger motivates their attacks. Some perpetrators use the attack as a vehicle for extortion. Others simply want the recognition.

vi. Explaining how denial of service attacks, backdoors, spoofing are carried out.

- A **botnet** is a group of compromised computers connected to a network such as the Internet that are used as part of a network that attacks other networks, usually for nefarious purposes.
- A compromised computer, known as a **zombie**, is one whose owner is unaware the computer is being controlled remotely by an outsider. Cybercriminals use botnets to send spam via e-mail, spread viruses and other malware, or commit a denial of service attack.

vi. Explaining how denial of service attacks, backdoors, spoofing are carried out.

- What is a **denial of service attack**?

Also called DoS attack	Hacker uses unsuspecting computer, called zombie, to execute attack on other systems
The victim computer network eventually jams, blocking legitimate visitors from accessing the network	Many of the latest antivirus and firewall programs include provisions to protect from DoS attacks

vi. Explaining how denial of service attacks, backdoors, spoofing are carried out.

- **Backdoors**
- A **back door** is a program or set of instructions in a program that allow users to bypass security controls when accessing a program, computer, or network.
- Once perpetrators gain access to unsecure computers, they often install a back door or modify an existing program to include a back door, which allows them to continue to access the computer remotely without the user's knowledge.

vi. Explaining how denial of service attacks, backdoors, spoofing are carried out.

- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network.
- E-mail spoofing occurs when the sender's address or other components of the e-mail header are altered so that it appears the e-mail originated from a different sender. E-mail spoofing commonly is used for virus hoaxes, spam, and phishing scams.
- IP spoofing occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source. Perpetrators of IP spoofing trick their victims into interacting with a deceptive Web site.

vii. Identifying appropriate ways of protecting data in computer systems.

- **Data encryption**

  Data on transit over the network faces many dangers of being tapped, listened to or copied to unauthorized destinations. Such data can be protected by mixing up into a form that only the sender and receiver is able to understand. This is by reconstructing the original message from the mix which is called data encryption.

What is Data encryption?

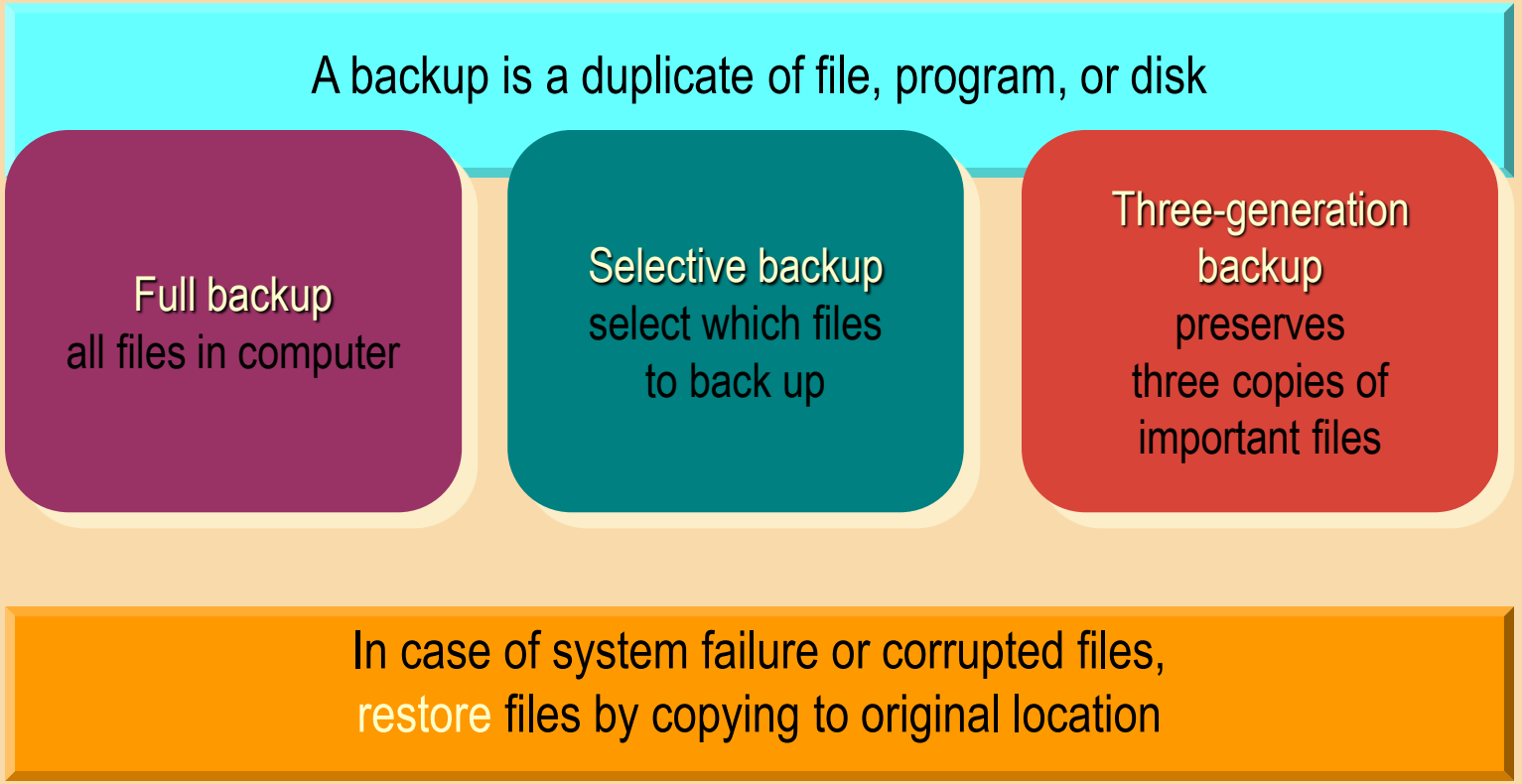
- **Process of converting plaintext (readable data) into ciphertext (unreadable characters)**
- **Safeguards against information theft**
- **Encryption key (formula) often uses more than one method**
- **To read the data, the recipient must decrypt, or decipher, the data**

vii. Identifying appropriate ways of protecting data in computer systems.

- **Surge protectors**
  - **Protect computers and equipment from electrical power disturbances**
  - **Uninterruptible power supply (UPS) is surge protector that provides power during power loss**

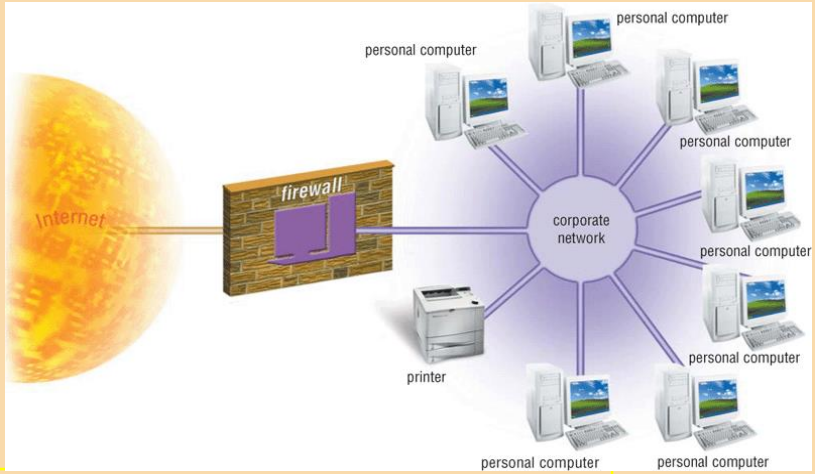
vii. Identifying appropriate ways of protecting data in computer systems.

- **Backups** - the ultimate safeguard



vii. Identifying appropriate ways of protecting data in computer systems.

- What is a **firewall**?
  - **Security system consisting of hardware and/or software that prevents unauthorized network access**
- A firewall is a device or software system that filters the data and information exchanged between different networks by enforcing the host networks access control policy. The main aim of a firewall is to monitor and control access to or from protected networks. People who do not have permission (remote requests) cannot access firewall restricted sites outside their network.



vii. Identifying appropriate ways of protecting data in computer systems.

Use of acceptable use policy (AUP)

- The AUP outlines the computer activities for which the computer and network may and may not be used.
- An organization's AUP should specify the acceptable use of computers by employees for personal reasons.
- Some organizations prohibit such use entirely. Others allow personal use on the employee's own time such as a lunch hour.

vii. Identifying appropriate ways of protecting data in computer systems.

- **Intrusion Detection Software**
- To provide extra protection against hackers and other intruders, large organizations sometimes use intrusion detection software to identify possible security breaches.
- **Intrusion detection software** automatically analyzes all network traffic, assesses system vulnerabilities, identifies any unauthorized access (intrusions), and notifies network administrators of suspicious behavior patterns or system breaches.
- To utilize intrusion detection software requires the expertise of a network administrator because the programs are complex and difficult to use and interpret. These programs also are quite expensive.

vii. Identifying appropriate ways of protecting data in computer systems.

Identifying and Authenticating Users

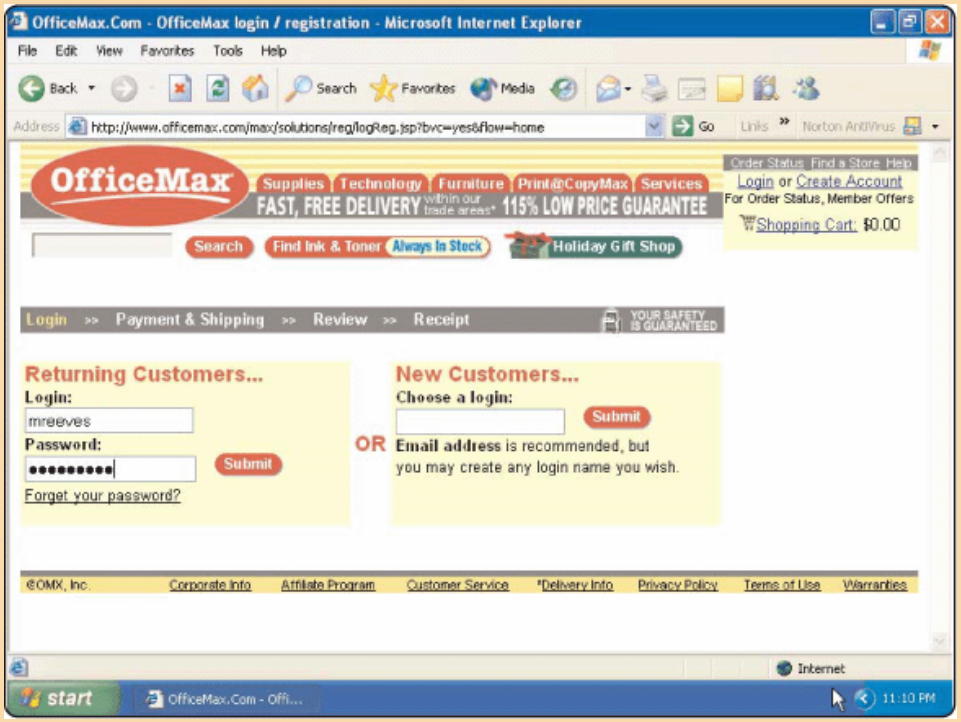
- Many organizations use access controls to minimize the chance that a perpetrator intentionally may access or an employee accidentally may access confidential information on a computer.
- An **access control** is a security measure that defines who can access a computer, when they can access it, and what actions they can take while accessing the computer. In addition, the computer should maintain an **audit trail** that records in a file both successful and unsuccessful access attempts.
- An unsuccessful access attempt could result from a user mistyping his or her password, or it could result from a hacker trying thousands of passwords. Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security.

vii. Identifying appropriate ways of protecting data in computer systems.

- How can companies protect against hackers?

vii. Identifying appropriate ways of protecting data in computer systems.

- **User Names and Passwords**
  - A username is Unique combination of characters that identifies user
  - Password is private combination of characters associated with the user name that allows access to computer resources



vii. Identifying appropriate ways of protecting data in computer systems.

- How can you make your password more secure?
  - **Longer passwords provide greater security**

PASSWORD PROTECTION

		AVERAGE TIME TO DISCOVER	
Number of Characters	Possible Combinations	Human	Computer
1	36	3 minutes	.000018 second
2	1,300	2 hours	.00065 second
3	47,000	3 days	.02 second
4	1,700,000	3 months	1 second
5	60,000,000	10 years	30 seconds
10	3,700,000,000,000,000	580 million years	59 years

- *Possible characters include the letters A–Z and numbers 0–9*
- *Human discovery assumes 1 try every 10 seconds*
- *Computer discovery assumes 1 million tries per second*
- *Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations*

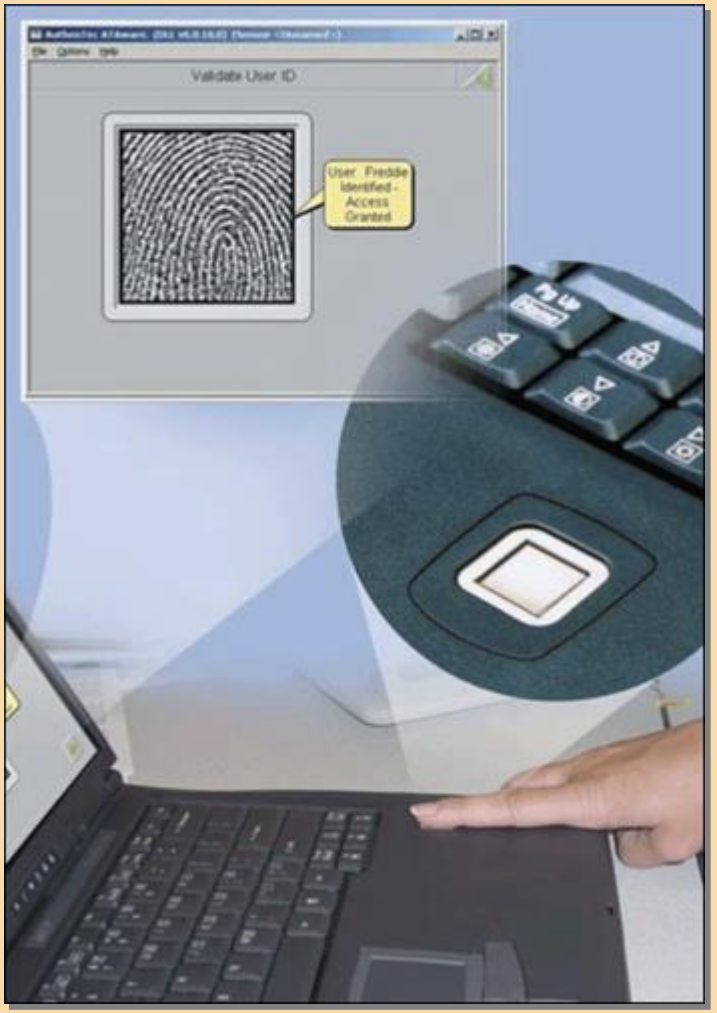
vii. Identifying appropriate ways of protecting data in computer systems.

- **Possessed objects**
  - **Items that you must carry to gain access to computer or facility, e.g badges, cards, smart cards, and keys. Often used with numeric password called personal identification number (PIN) e.g ATM pin.**
  - Access control can be enhanced by implementing multilevel authentication policies such as assigning users log on accounts, use of smart cards and a personal identification number (PIN).
- **Security monitors** are programs that monitor and keep a log file or record of computer systems and protect them from unauthorized access.

vii. Identifying appropriate ways of protecting data in computer systems.

Biometric devices

- **Authenticates person's identity using a human characteristic**
  - Fingerprint, hand geometry, voice, signature, and iris
- Biometric security is a growing form of unauthorized control measure that takes the user's attributes such as voice, fingerprints and facial recognition. For example, you can log on swap a finger on a finger print swap windows.



vii. Identifying appropriate ways of protecting data in computer systems.

Callback systems

User connects to computer only after the computer calls that user back at a previously established telephone number

Some networks utilize callback systems as an access control method to authenticate remote or mobile users

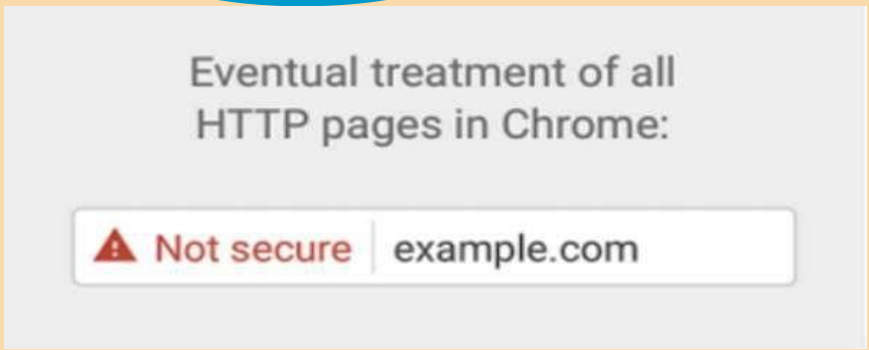
Callback systems work best for users who regularly work at the same remote location, such as at home or branch office

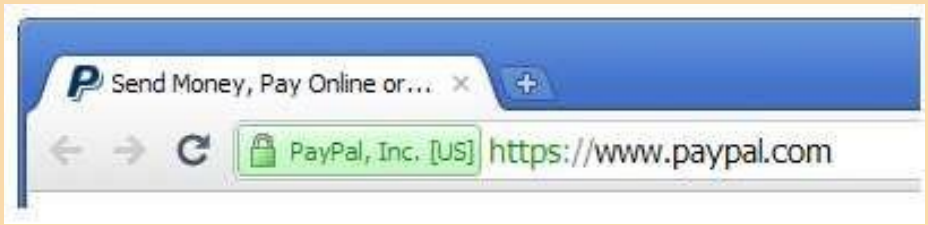
vii. Identifying appropriate ways of protecting data in computer systems.

- **Secure web data transmission using HTTP+SSL = HTTPS**

Many Web browsers use encryption

A Secure site
is Web site that uses encryption to secure data





Users apply for SSL certificate from a certificate authority (CA). A CA is an Authorized person or company that issues and verifies SSL certificates.

viii. Identifying types of computer crimes

The following are some examples of crimes perpetuated by use of computers.

- **Physical theft**
- The physical theft of computer hardware and software is the most widespread related crime especially in developing countries.
- The most common issues now, we here cases of people breaking into an office or firm and stealing computers, hard disks and other valuable computer accessories. In most cases such theft can be done by untrustworthy employees of firm or by outsiders. The reason behind an act may be commercial, destruction to sensitive information or sabotage.

Control measures against theft

- Employ security agents to keep watch over information centers and restricted backup sites.
- Reinforce weak access points like windows, door and roofing with metallic grills and strong padlocks.
- Motivate workers so that they feel a sense of belonging in order to make them proud and trusted custodians of the company resources.
- Insure the hardware resources with a reputable insurance firm.

viii. Identifying types of computer crimes

Piracy

- Piracy is a form of intellectual property theft which means illegal copying of software, information or data. Software, information and data are protected by copyright and patent laws.
- **Control measures against piracy**
- There are several ways of reducing piracy
- Enforce laws that protect the owners of data and information against piracy.
- Make software cheap enough to increase affordability.
- Use licenses and certificates to identify original software.
- Set installation passwords that deter illegal installation of software.

viii. Identifying types of computer crimes

Fraud

- Fraud is stealing by false pretense. Fraudsters can be either employees in a company, non-existent company that purports to offer internet services such as selling vehicles etc. other form of fraud may also involve computerized production and use of counterfeit documents. This is due to the dynamic growth of internet and mobile computing, sophisticated cybercrimes.

Sabotage

- Sabotage refers to illegal destruction of data and information with the aim of crippling services delivery, or causing great loss to an organization. Sabotage is usually carried out by disgruntled employees or competitors with the intention of causing harm to an organization.

viii. Identifying types of computer crimes

- **Eavesdropping**
- Eavesdropping refers to tapping into communication channels to get information. Hackers mainly use eavesdropping to access private or confidential information from internet users or from poorly secured information system.
- **Surveillance (monitoring)**
- Surveillance refers to monitoring use of computer system and networks using background programs such as spyware and cookies. The information gathered may be used for one reason or the other e.g. spreading sabotage.

viii. Identifying types of computer crimes

- **Industrial espionage**
- Industrial espionage involves spying on a competitor to get information that can be used to cripple the competitor.
- **Accidental access**
- Threats to data and information come from peoples unknowingly giving out information to strangers is or unauthorized persons.
- **Alteration**
- Alteration is the illegal modification of private or confidential data and information with the aim of misinforming users. Alteration is usually done by people who wish to cancel the truth or sabotage certain operations.
- Alteration comprises the integrity of data and information making it unreliable.

Sub Topic 2. Privacy and ICT Ethical Issues

Sub topic Objectives:

a. ICT ethics and society

i. define and describe ethical issues in ICT.

ii. describe information accuracy.

b. Intellectual property

iii. explain the concept of intellectual property rights

c. Information privacy

iv. explain the different aspects of information privacy and violation

a. ICT ethics and society

- What are ICT ethics?

Moral guidelines that govern use of computers and information systems

- Ethics is knowing and understanding what is right and what is wrong, and then doing the right thing right.
- In simple terms, ethics are standards of moral conduct.
- Quite often, people in society do the wrong things either out of ignorance or deliberately to achieve selfish interests.

a. ICT ethics and society

- In today's society, computers are involved to some extent in almost every aspect of life and sometimes they often perform life-critical tasks.
- This makes it very important to carefully consider the issues of ethics in use of computers and software.
- Ethical principles are important because they help us navigate through difficult situations and reflect the way to relate with our friends and community.

a. ICT ethics and society

- **Three useful ethical principles:**
- An act is ethical if society benefits from the act.
- An act is ethical if people are treated as an end and not as a means to an end.
- An act is ethical if it is fair to all parties involved.
- **Computer ethics** involves use of computers & software in morally acceptable way.
- Standards or guidelines are important in this industry, because technology changes are outstripping the legal system's ability to keep up.

a. ICT ethics and society

Computer Ethics for Computer Professionals

According to the Association for Computing Machinery (ACM) code, a computing professional:

- Contributes to society and human well-being.
- Always avoids harm to others.
- Should be honest and trustworthy.
- Should exercise fairness and takes action not to discriminate.
- Honors property rights, including copyrights and patents
- Gives proper credit when using the intellectual property of others.
- Respects other individuals' rights to privacy.
- Honors confidentiality.

a. ICT ethics and society

- **Code of Conduct**
- A **code of conduct** is a written guideline that helps determine whether a specific action is ethical or unethical.

IT CODE OF CONDUCT
1. Computers may not be used to harm other people.
2. Employees may not interfere with others' computer work.
3. Employees may not meddle in others' computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' computer resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

b. Intellectual property

- Intellectual property (IP) refers to a creation on one's mind and innovativeness, such as work created by inventors, authors, and artists.
- Intellectual property rights—rights to which creators are entitled for their work
- A copyright gives authors and artists exclusive rights to duplicate, publish, and sell their materials.
- A common infringement of copyright is software piracy.
- A trademark protects a company's logos and brand names.

c. Information privacy

- Information privacy refers to the right of individuals and companies to deny or restrict the collection and use of information about them.
- In the past, information privacy was easier to maintain because information was kept in separate locations.
- Today, huge databases store this data online.
- Much of the data is personal and confidential and should be accessible only to authorized users.
- Many individuals and organizations, however, question whether this data really is private.

c. Information privacy

Concerns related to collection and use of private data are:

- Data should not be disclosed to other people without the owner's permission.
- Data and information should be kept secured against loss or exposure
- Data and information should be kept longer than necessary
- Data and information should be accurate and up to date.
- Data and information should be collected, used and kept for specified lawful purposes.

c. Information privacy

- **What is information privacy?**

Right of individuals and companies to restrict collection and use of information about them

Difficult to maintain today because data is stored online

Employee monitoring is using computers to observe employee computer use

Its Legal for employers to use monitoring software programs

c. Information privacy

What are some ways to safeguard personal information?

- Limit the amount of information you provide to Web sites; fill in only required information
- Inform merchants that you do not want them to distribute your personal information
- Set up a free e-mail account; use this e-mail address for merchant forms
- Sign up for e-mail filtering through your Internet service provider or use an antispam program.
- Do not reply to spam for any reason
- Install a personal firewall
- Turn off file and print sharing on your Internet connection
- Surf the Web anonymously with a program such as Freedom Web Secure or through an anonymous Web site such as Anonymizer.com
- Install a cookie manager to filter cookies
- Clear your history file when you are finished browsing.

c. Information privacy

- **What is an electronic profile?**

Refers to a set of data collected when you fill out a form on the Web, e.g. a user profile on Amazon or a Facebook profile.

- Merchants may sell the contents of their databases to national marketing firms and Internet advertising firms.
- Many companies today allow people to specify whether they want their personal information distributed.

c. Information privacy

Cookies

- E-commerce and other Web applications often rely on cookies to identify users. A **cookie** is a small text file that a Web server stores on your computer. Cookie files typically contain data about you, such as your user name or viewing preferences.
- Many commercial Web sites send a cookie to your browser, and then your computer's hard disk stores the cookie.
- The next time you visit the Web site, your browser retrieves the cookie from your hard disk and sends the data in the cookie to the Web site.

c. Information privacy

- **What is a cookie?**

c. Information privacy

Web sites use cookies for a variety of purposes:

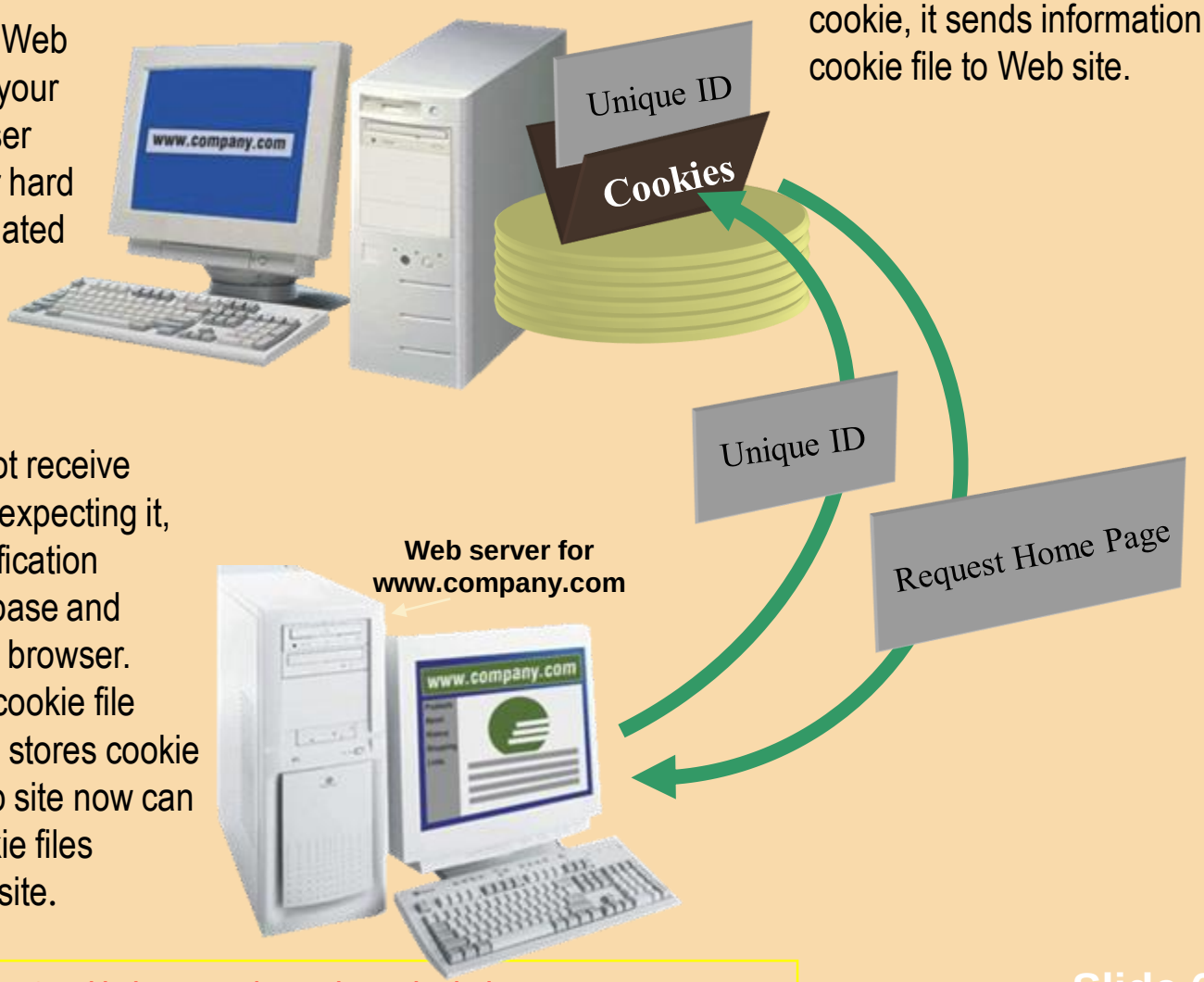
- Most Web sites use cookies to track user preferences.
- Some Web sites use cookies to store users' passwords, so that they do not need to enter it every time they log in to the Web site.
- Online shopping sites generally use a session cookie to keep track of items in a user's shopping cart. This way, users can start an order during one Web session and finish it on another day in
- another session. Session cookies usually expire after a certain time, such as a week or a month.
- Some Web sites use cookies to track how often users visit a site and the Web pages they visit while at the site.
- Web sites may use cookies to target advertisements. These sites store a user's interests and browsing habits in the cookie.

c. Information privacy

- How do cookies work?

Step 1. When you type Web address of Web site in your browser window, browser program searches your hard disk for a cookie associated with Web site.

Step 2. If browser finds a cookie, it sends information in cookie file to Web site.



Step 3. If Web site does not receive cookie information, and is expecting it, Web site creates an identification number for you in its database and sends that number to your browser. Browser in turn creates a cookie file based on that number and stores cookie file on your hard disk. Web site now can update information in cookie files whenever you access the site.

p. 369 Fig. 10-18

c. Information privacy

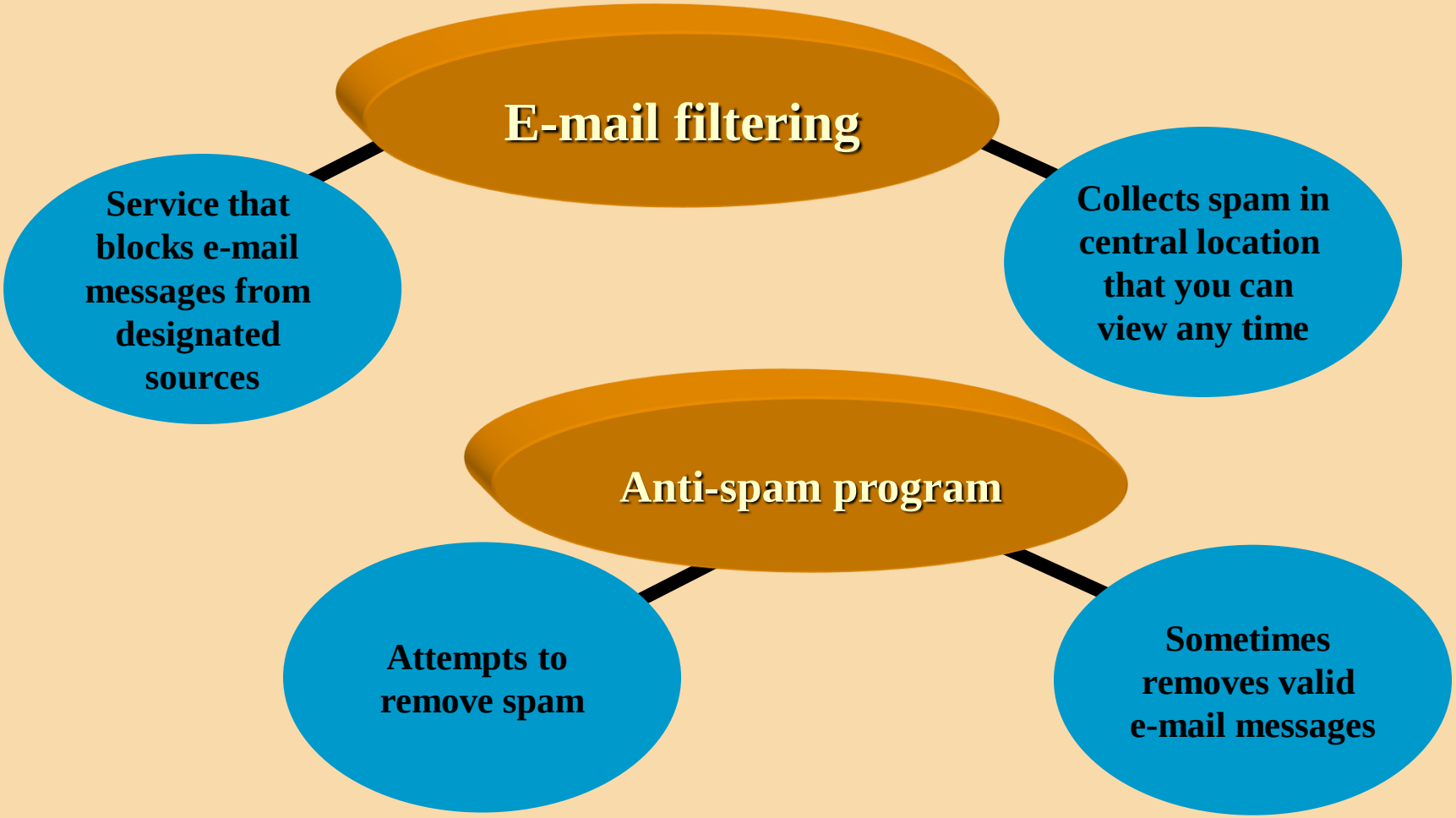
- For privacy purposes, You can set a browser to accept **cookies** automatically, prompt you if you want to accept a cookie, or disable cookie use altogether.
- Keep in mind if you disable cookie use, you will not be able to use many of the e-commerce Web sites.

c. Information privacy

- **What are spyware and spam?**
  - **Spyware is program placed on computer without user's knowledge which Secretly collects information about the user**
  - **Spam is unsolicited e-mail message sent to many recipients**

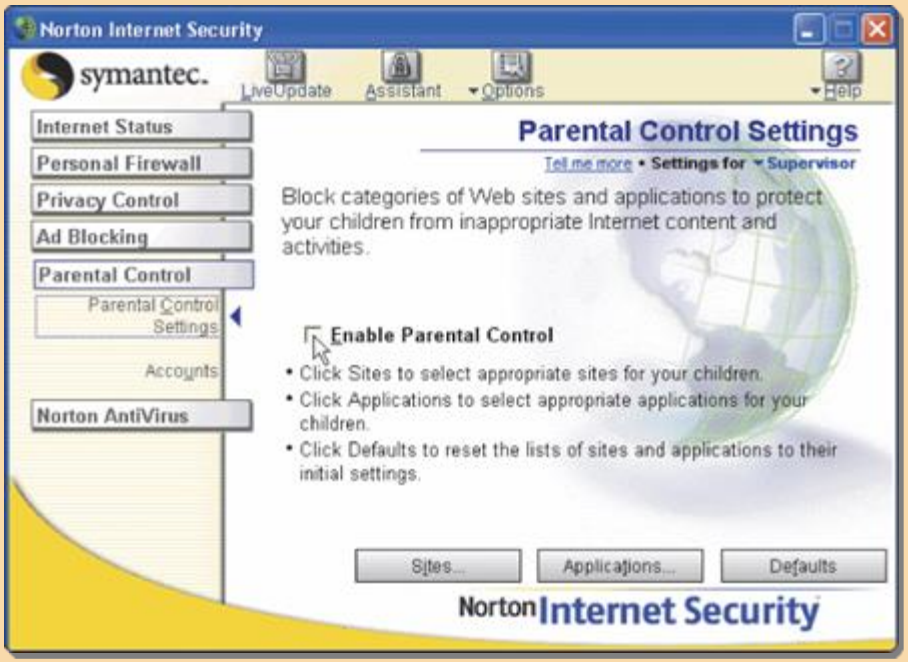
c. Information privacy

- **How can you control spam?**



c. Information privacy

- **What is content filtering?**
  - **Process of restricting access to certain material**
  - **Internet Content Rating Association (ICRA) provides rating system of Web content**
  - **Web filtering software restricts access to specified sites**



c. Information privacy

What is Phishing?

- Phishing is a scam in which a perpetrator sends an official looking e-mail message that attempts to obtain your personal or financial information. Some phishing e-mail messages ask you to reply with your information; others direct you to a deceptive Web site, or a pop-up window that looks like a legitimate Web site, that may request you to update credit card numbers, Social Security numbers, bank account numbers, passwords, or other private information. Always don't click a link in an e-mail message; instead retype the Web address in your browser.
- A **phishing filter** is a program that warns or blocks you from potentially fraudulent or suspicious Web sites. Some Web browsers include phishing filters.

c. Information privacy

What is Pharming?

- Pharming is a scam, similar to phishing, where a perpetrator attempts to obtain your personal and financial information, except they do so via spoofing. That is, when you type a Web address in the Web browser, you are redirected to a phony Web site that looks legitimate.

What is Clickjacking?

- **Clickjacking** is yet another similar scam. With clickjacking, an object that can be clicked on a Web site, such as a button, image, or link, contains a malicious program. When users click the disguised object, for example, they may be redirected to a phony Web site that requests personal information, or a virus may download to their computer

c. Information privacy

What is Social Engineering?

- As related to the use of computers, social engineering is defined as obtaining confidential information by taking advantage of the trusting human nature of some victims. Some social engineers trick their victims into revealing confidential information such as user names and passwords on the telephone, in person, or on the Internet.
- Techniques they use include pretending to be an administrator or other authoritative figure, feigning an emergency situation, or impersonating an acquaintance. Social engineers also obtain information from users who do not destroy or conceal information properly. These perpetrators sift through company dumpsters, watch or film people dialling telephone numbers or using ATMs, and snoop around computers looking for openly displayed confidential information.

c. Information privacy

Employee Monitoring:

- Employee monitoring involves the use of computers to observe, record, and review an employee's use of a computer, including communications such as e-mail messages, keyboard activity (used to measure productivity), and Web sites visited. Many programs exist that easily allow employers to monitor employees.
- A frequently debated issue is whether an employer has the right to read employee e-mail messages. Actual policies vary widely. Some companies declare that they will review e-mail messages regularly, and others state that e-mail is private. Several lawsuits have been filed against employers because many believe that such internal communications should be private. Another controversial issue relates to the use of cameras to monitor employees, customers, and the public. Many people feel that this use of video cameras is a violation of privacy.

c. Information privacy

Content Filtering

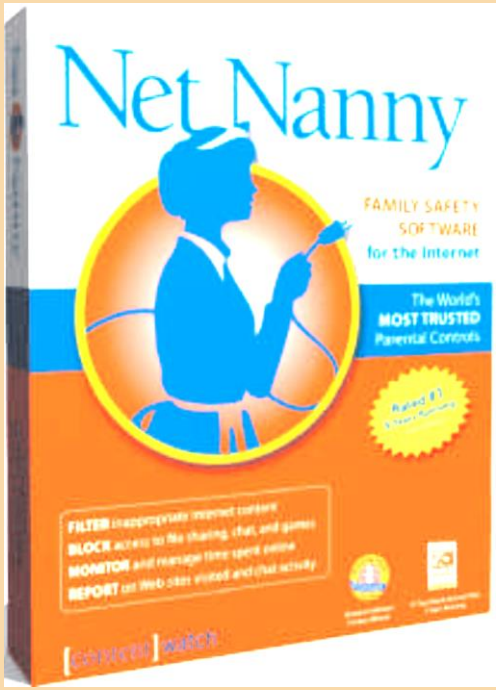
One of the more controversial issues that surround the Internet is its widespread availability of objectionable material, such as racist literature, violence, and pornography. Content filtering is the process of restricting access to certain material on the Web.

•Many businesses use content filtering to limit employees' Web access. These businesses argue that employees are unproductive when visiting inappropriate or objectionable Web sites. Some schools, libraries, and parents use content filtering to restrict access to minors.

•Some countries like China also do content filtering though banning some websites like Facebook. Content filtering opponents argue that banning any materials violates constitutional guarantees of free speech and personal rights.

c. Information privacy

- **Web filtering** software is a program that restricts access to specified Web sites.
- Some also filter sites that use specific words. Others allow you to filter e-mail messages, chat rooms, and programs. An example of a web filtering program in Net Nanny.
- Many Internet security programs include a firewall, antivirus program, and filtering capabilities combined.



Sub Topic 3. Emerging Technologies

Sub topic Objectives:

a. Emerging technologies

- *explain the concept of emerging technologies (artificial intelligence, digital forensics, among others).*

b. Application areas of specific emerging technologies

- *explain how specific technologies are applied in problem-solving in society.*

c. Implications of emerging technologies

- *explain advantages and disadvantages.*

Emerging technologies

- Definition: **Emerging technologies** are those that are currently being developed or will be developed in the next 5 to 10 years, and which will alter the business and social environment.
- ICT is always improving and changing and new technologies are being developed all of the time. Developments in technology will, by nature, impact on our everyday lives and these include:
  - **Artificial Intelligence (AI)**
  - **Digital forensics**
  - **Biometrics**
  - **Robotics**
  - **Quantum Cryptography**
  - **Computer Assisted Translation (CAT)**
  - **3D and Holographic Imaging (aka holograms)**
  - **Virtual Reality**

Application areas and impacts of some emerging technologies

Artificial Intelligence (AI)

- This is a computer science that is focused on creating computer systems that simulate human intelligence. The term was first used in 1956 by a computer scientist at the Massachusetts Institute of Technology (MIT) who was focused on trying to make computers behave like humans.

AI is being developed in the following application areas:

- **Expert Systems** - These are computers that have been programmed to make decisions based on information they are given. For example: Medical expert systems can diagnose patient's illnesses based on symptoms entered.
- **Languages** - This type of AI involves computers that can understand different human languages as they are spoken to them.
- **Robotics** - Robotic artificial intelligence is where machines are programmed to imitate a human.
- **Game Playing** - Computers developed to play games against human players. For example: In 1997 a computer named 'Deep-Blue' defeated a world champion in the game of chess.

Application areas and impacts of some emerging technologies

Impacts of AI on everyday life:

- **Accurate prediction of weather** - AI software will soon be used to sift through weather data more accurately that humans can and will be used to predict approaching storms and automatically issue warnings.
- **Increased leisure time** - Robotic vacuum cleaners are becoming more and more popular. These can detect walls and other objects in order to vacuum around them. People can leave them running whilst they enjoy extra spare time.
- **Safer transport** – Self driving cars already exist will drastically reduce road accidents. Driverless trains too already exist in some countries!
- **Increased Personal safety** - Modern home alarm systems use artificial intelligence software that can tell the difference between the home owners and intruders. The software automatically alerts the police when intruders are detected.
- **Improved medical care** - Robotic surgery assistants are being used to quickly and accurately pass the correct surgical tools to doctors. The few seconds saved in getting the correct tool to the doctor can save patient's lives.

Application areas and impacts of some emerging technologies

- **Digital forensics**
- Digital forensics, also called computer forensics, network forensics, or cyberforensics, is the discovery, collection, and analysis of evidence found on computers and networks. Digital forensics involves the examination of computer media, programs, data and log files on computers, servers, and networks.

  Many areas use digital forensics, including
  - law enforcement,
  - criminal prosecutors,
  - military intelligence,
  - insurance agencies,
  - Tax investigations and
  - information security departments in the private sector.

Application areas and impacts of some emerging technologies

- **Impact of Digital Forensics on everyday life:**
- Forensics has led to increased legal use of digital evidence. Digital evidence is information found on a wide range of electronic devices that is useful in court because of its probative value.
- Technology changes evidence. There is still a vigorous debate in the legal world over the usage and reliability of DNA evidence, for example. This is now being mirrored in more recent court challenges over the use of digital evidence.
- Digital evidence tendered in court often fails to meet the same high standards expected of more established forensics practices, particularly in ensuring the evidence is what it purports to be. It is increasingly common for criminal trials to rely on digital evidence. And, regrettably, it is common for innocents to be convicted and guilty people acquitted because of digital evidence.

Application areas and impacts of some emerging technologies

Biometrics

Biometrics is where parts of a person's body are used for identification purposes. Examples include:

- **Fingerprints** - These are impressions embedded at the end of human fingers and thumbs. Fingerprints kept in a database can be matched to those left at crime-scenes to help identify the culprit.
- **Eye recognition** - Eye scans analyse the iris which is the coloured ring that surrounds the pupil.
- **Face recognition** - This is where the shapes of individual's faces are analysed.
- **Voice recognition** - Pitch, tone and frequency of voices are unique and can be analysed to identify people.
- All of these parts of the human body are unique from person to person and can be used to authenticate identity. Even identical twins have slightly different fingerprints and voices etc.

Application areas and impacts of some emerging technologies

- **Impacts of Biometrics on everyday life:**
- **Better airport security** - Iris recognition is already in use in some airports. Travellers have their eyes and iris scanned into a system and this data is later matched up when the person is performing airport checks.
- **Increased building security** - Fingerprint access to buildings have been replacing the older methods of locks and keys. This method ensures that only authorised people can enter restricted buildings or rooms.
- **Reduced car theft** - Cars already exist that use fingerprints to only unlock their doors or start the engine for the fingerprint that is registered. This means that the doors will not unlock for a print that is not recognised and makes the car harder to steal.
- **More secure mobile phones** - Mobile phones contain our lives. We used our phones for everything from social media to shopping online. They need to be as secure as possible in order to protect the valuable data that they contain. Apple recently released an iPhone model that uses a fingerprint reader to identify the true owner of the phone. It will not unlock for a fingerprint that it does not recognise.

Application areas and impacts of some emerging technologies

- Robotics

- Robots are increasingly being used in manufacturing due to their proven increase in productivity. Think about it! Robots can work 24/7 and never need to take breaks. They also do not require wages like humans do. This means that robots can produce more at a lower cost. They are either automated (controlled by a computer chip) or manually controlled by a human.

Some more typical tasks that robots can be used for are described in the table below:

- **Dangerous jobs -** E.g. disposing of bombs, spray painting or cleaning up nuclear waste. Note: these are all jobs that could harm or kill a human.
- **Exploring extreme environments-** E.g. inside volcanoes, planets or the depths of the ocean. Note: humans cannot visit these environments due to lack of oxygen and high pressure / heat levels.
- **Repetitive manufacturing jobs -** E.g. production lines, packing and welding etc.
- Note: these jobs can also be performed by humans but robots can do them much faster and more efficiently.
- **Moving heavy objects -** E.g. installing large engines, moving pallets of items etc.

Application areas and impacts of some emerging technologies

Impacts of Robotics on everyday life:

- **Increased personal time** - If robots can carry out domestic chores, this frees up more time for us to spend as we wish.
- This could mean more time spent at work or for more enjoyable activities such as socialising.
- **More efficient manufacturing** Robots can manufacturer products such as cars much faster and cheaper than humans can. This means that companies can make more products at less cost and this means greater business profits.
- **Loss of jobs** Due to higher and cheaper productivity, robots are taking over the manufacturing jobs that used to be carried out by humans. This means that humans are missing out on employment on assembly lines and factory work.
- **Safer working environments** - Robots can safely carry out tasks that are too dangerous for humans. For example: spraying cars with toxic paint, defusing bombs on battlefields and search and rescue operations in buildings destroyed by earthquakes

Application areas and impacts of some emerging technologies

Quantum Cryptography

- Quantum cryptography (encryption) is an emerging technology that allows messages and data to be sent with complete privacy.
- Note: Encryption is where digital data and files are scrambled so that only authorised people are allowed to read it.
- Unauthorised people attempting to read the data would see illegible nonsense instead of the real information. Older methods of encryption were based around mathematics but quantum cryptography uses physics instead.
- This makes the encryption impossible to break.
- In quantum cryptography, messages are encrypted using photons. Photons are tiny packets of light.

Application areas and impacts of some emerging technologies

Impacts of Quantum Encryption on everyday life:

- **Completely secure voting** Citizens of countries have the right to vote-in new governments but history is littered with examples of where these votes have been tampered with in order to influence election outcomes. Securing votes with quantum encryption methods ensures that they cannot be tampered with or changed.
- **Completely secure communication -** Messages sent by the military often include the locations of squadrons or special op's teams. If enemy forces intercepted these messages it could have severe consequences. Using quantum cryptography to secure the messages would eliminate the risk of them being read or heard by unauthorised ears.
- **Completely secure bank transfers -** Any electronic transfer of money, such as at ATM's or buying goods online, will be completely secure. Some banks are already using quantum cryptography for the purposes of securing money transfers.
- **Completely secure personal information -** Health records, bank details and other types of personal information will be absolutely secure from hackers and other people wishing to commit identity theft crimes.

Application areas and impacts of some emerging technologies

- **Computer Assisted Translation (CAT)**
- CAT is where a human translator uses computer software to help in the translation process. CAT software can reduce the amount of time that the translation takes. Current CAT tools are not always 100% accurate. They need a human to check for errors.

Examples of different types of CAT tools include:

- **Spell checkers** - These are usually built-into word processing software and can automatically flag-up spelling errors and suggest translations of miss-spelt words. NOTE: Most word-processors now allow the user to select the language in which to spell-check.
- **Translation memory software** -Translation memory software are databases which store translated text as the human translator works through it in order to be reused in the future. Translated text is built-up in the database's memory and can be accessed by other translators in order to speed up their translation jobs.
- **Language search-engine software** - These are Internet based systems which allow translators to enter any text that they want translating and also to select which language they want the text translating into. The software will then search through a large collection of translation memory databases to try and find a match with the text entered into the search engine. If a match is found, translated text will be shown on-screen.

Application areas and impacts of some emerging technologies

Impacts of Computer Aided Translation on everyday life:

- **More accurate documents** Spell checkers can quickly scan your word processed documents and automatically find spelling errors. Miss-spelt words can be quickly corrected to produce an error-free document.
- **A more multilingual society** Anyone with an Internet connection can access tools such as Google Translate and the vast collection of language databases that the tools can search through. This makes accessing other languages much easier than in the past and makes it easier for people to learn these new languages.
- NOTE: Google's new 'Voice Search' facility allows users to actually speak into a tablet or mobile phone and Google will automatically translate (and speak) the words or phrase in almost any language.
- **Quicker and more efficient translations** Foreign visitors to countries can be communicated with much easier through these CAT tools. They are especially useful in places like embassies where a wide-range of foreign visitors may need to communicate with local officials about problems or ask for advice etc.

Application areas and impacts of some emerging technologies

3D and Holographic Imaging (aka holograms)

- This is a technique where images are made to appear three-dimensional and to actually have depth. Holograms work by taking two regular two-dimensional images of the same object and laying one on top of the other.

- The two-dimentional images need to have been shot at different angles.
- Two different types of laser beams are used to record the two-dimensional images onto a single photographic plate. This creates one single image that incorporates the angles of the original two-dimensional images. This produces a 3D effect. When viewing the image, human eyes see it from slightly different angles. The brain combines them into a three-dimensional image.

Application areas and impacts of some emerging technologies

Impacts of 3D imaging on everyday life:

- **Improved security** - Credit cards, ID cards, software and some bank notes include holograms as a way of trying to prevent forged duplicates being created. NOTE: Forgeries don't usually include a hologram as they are difficult and expensive to reproduce.
- **Better movie experiences** -Hollywood have been using 3D imaging within the production of movies for many years. These provide the viewer with a much more immersive experience. NOTE: 3D movies require the viewer to wear special glasses for the effect to take place. The glasses project two images shot at different angles (one in each eye) and your brain puts them together as one 3D image.
- **Greater data storage** - It is thought that the technology behind holograms will eventually be used to provide the means to store large amounts of data. Companies have already produced discs that use holographic layers that each have the potential to hold a massive 3.9 terabytes. NOTE: This is the equivalent of over 150 standard Blu-ray discs.

Application areas and impacts of some emerging technologies

- **Virtual Reality**
- Virtual reality is where computers are used to create an artificial environment that users can interact with as if it were real. Virtual reality is not really meant for gaming purposes. It is used for more serious purposes such as:
- Allowing architects to walk around a virtual version of their design (this gives a better idea of what the finished building will look like)
- Training soldiers in combat (flight simulation, battlefield simulation)
- Training surgeons (virtual patients can be operated on to provide experience to trainee surgeons).

As they walk around the virtual environment users will experience things in a similar way to the real world. For example:

- Objects get smaller as you walk away from them (and bigger as you move closer)
- The direction of sounds change as you move around
- Objects in the virtual world appear the same dimensions as they would in the real world (for example dogs are smaller than us but elephants are bigger).

Application areas and impacts of some emerging technologies

- **Virtual Reality**
- Virtual reality is where computers are used to create an artificial environment that users can interact with as if it were real. Virtual reality is not really meant for gaming purposes. It is used for more serious purposes such as:
- Allowing architects to walk around a virtual version of their design (this gives a better idea of what the finished building will look like)
- Training soldiers in combat (flight simulation, battlefield simulation)
- Training surgeons (virtual patients can be operated on to provide experience to trainee surgeons).

As they walk around the virtual environment users will experience things in a similar way to the real world. For example:

- Objects get smaller as you walk away from them (and bigger as you move closer)
- The direction of sounds change as you move around
- Objects in the virtual world appear the same dimensions as they would in the real world (for example dogs are smaller than us but elephants are bigger).

Application areas and impacts of some emerging technologies

- **Impacts of Virtual Reality on everyday life:**
- **Improved medical surgeons** - Surgeons can be trained using virtual patients. This allows them to practice over and over until they have perfected a particular surgery without risk to a real patient.
- **Safer and stronger buildings** - Virtual buildings allow architects to walk around to experience what the building would look like when completed and check for potential errors before the actual building is constructed. This allows architects to modify designs quickly and cheaply and will, potentially, allow for the development of much larger and safer buildings than we currently have.
- **More effective treatment of phobias** - VR is being used to help patients overcome phobias and anxieties. People can experience a tame, controlled version of what they are afraid of. Slowly the person becomes used to the situation and can relax.
- **Training in dangerous situations** - VR can be used for training in dangerous situations where it is impossible to practice the real thing. For example: A large fire in an office building could never be set up in reality, but it could in a virtual environment. This will allow workers to practice emergency evacuation in a safe environment.
- **More realistic education -** VR can give students the opportunity to learn in a much more interactive way. For example: Astronomy students can learn about the solar system by engaging with the objects in the virtual environment.

Sub Topic 4. ICT Industry

Sub topic Objectives:

- Careers in the ICT industry
  - *explain the meaning of careers in the ICT industry.*
  - *appreciate careers in the ICT industry.*
- ICT in SMEs
  - *identify the potential of ICTs for earning.*

Careers in the ICT industry

- **ICT industry**
- Information and communication technology (ICT) has created new job titles such as computer operators, computer technicians, system analyst, computer programmers, software engineer, information systems manager, data base administrator, computer trainer, web administrator, computer graphics designers, system administrators and network administrator.

Meaning of careers in the ICT industry

- **System analyst**
- This a person who is responsible for analyzing a company's needs or problems then designs and develops a computer based information system.
- **Some of the responsibilities of a system analyst include:**
- Reviewing the current manual or redundant information system and making recommendations on how to replace it with a more efficient one.
- Working with programmers to construct and test the system.
- Coordinating training for users of the new system.

Meaning of careers in the ICT industry

- **A good system analyst is one who has at least the following attributes;**
- Good problem solving skills and creativity, ie. Must have wide experience in solving problems.
- Good communication skills: The analyst must be able to communicate clearly and precisely both in writing and in speech. He/she must be able to talk to different groups of people e.g managers, operators, attendant and general public.
- Must have business knowledge: the analyst must clearly understand the environment for which the system is being developed.
- Technical knowledge: A system analyst must be well trained in relevant areas of computer science such as hardware, software programing knowledge.

Meaning of careers in the ICT industry

- **Computer operator**
- Some of the responsibilities of a computer operator include;
- Entering data into the computer for processing.
- Keeping up-to-date records (log files) of all information processing activities.
- **Computer technician**
- Given that computers require regular maintenance, upgrading as well as emergency repairs, demand for computer technicians continues to grow as more people computerize their workplaces and homes.
- Some of the responsibilities of a computer technician are;
  - Troubleshooting computer hardware and software related problems.
  - Assembling and upgrading computers and their components.
  - Ensuring that all computer related accessories such as printers modems, storage media devices are in good working condition.

Meaning of careers in the ICT industry cont

- **Computer engineer**
- Computer and electronic engineers are coming up with new and more efficient technologies in information and communication technology almost daily. Since computers are electronic devices, hardware designers must be good in electronic engineering in order to be able to:
- Design and develop computer components such as storage devices, motherboards and other electronic components.
- Determine the electrical power requirement of each component.
- Re-engineer computer components to enhance its functionality and efficiency.
- Design and develop engineering and manufacturing computer controlled devices such as robots.

Meaning of careers in the ICT industry

- **Computer programmer**
- Large organizations such as insurance companies, banks, manufacturing firms and government agents hire programmers to work together with system analysts in order to:
- Develop in house application programs or system programs.
- Customize commercial application packages to suite the organization needs.
- Install, test, debug, and maintain programs developed or customized for the organization.

Meaning of careers in the ICT industry

- **Web administrator/webmaster**
- **A web administrator is responsible for:**
- Developing and testing websites.
- Maintaining, updating and modifying information on the website to meet new demands by the users.
- **Software engineers:** Most Software engineers analyses user needs and create application software. Software engineers usually have experience in programming, but focus on the design and development of programs using the principles of mathematics and engineering.
- **Computer Trainers:** Computer trainers typically teach new users how to use the computer software and hardware.

Meaning of careers in the ICT industry

- **Network administrator**
- A network administrator is a specialist whose responsibilities are to:
- Set-up a computer network.
- Maintain and enforce security measures on the network.
- Monitor the use of network resources.
- Maintain and troubleshoot network related problems.
- **Graphic designers:** A graphic designer is a professional within the graphic design and graphic arts industry who assembles together images, typography, or motion graphics to create a piece of design.

Meaning of careers in the ICT industry

- **System Administrators**
- *A system administrator, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.*
  Other responsibilities of an information system administrator include;
  The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.
- A system administrator may acquire, install, or upgrade computer components and software; provide routine automation; maintain security policies; troubleshoot; train or supervise staff; or offer technical support for projects.

ICT in SMEs

- Small and medium enterprises (SMEs) are independent firms and companies which tend to have fewer employees and lower sales volume compared to large firms and companies. Different definitions are given from different organizations and countries. For example, the Organisation for European Economic Cooperation (OECD) and European Union (EU) designate the upper limit of employees for SME as 200 employees.
- Researchers have increasingly focused on the adoption and use of ICT by small and medium enterprises (SMEs) as the economic development of a country is largely dependent on them. Following the success of ICT utilisation in SMEs in developed countries, many developing countries are looking to utilise the potential of the technology to develop SMEs

ICT in SMEs

- **Role of ICT in SMEs**
- **Innovation and productivity.** ICT assists businesses to be more responsive to innovation opportunities and provides significant efficiency gains.
- **Open and closed innovation.** SMEs survive the competitive environment based on the innovation driven by ICT.
- **Economic role**. ICT in economics plays two important tasks, which are strategic management and cost reduction.
- **Entrepreneurship role.** ICT enables closer links between businesses, suppliers, customers and collaborative partners.

ICT in SMEs

Policies regarding adoption of ICT in SMEs

- The organisations should consider these factors for adoption of ICT in SMEs.
- **E-commerce / E-business:** Shift to a wider view of e-commerce integration of internal and external processes.
- **Staff ICT training**. Training programmes for SME managers and employees focussing on both ICT and managerial skills need to be provided in cooperation with business and sector organisations, training institution and commercial training services.
- **Privacy issues.** Address security, trust and confidence through broad policy frameworks, regulatory and self-regulatory tools, trustworthy technologies and affordable redress mechanisms.
- **E-governance**. Use e-government initiatives to provide incentives for SMEs to go on-line by simplifying administrative procedures, reducing costs and allowing them to enter new markets.
- **Growth analysis.** Expand collection and analysis of increasingly available statistics on e-business and e-commerce to monitor progress and improve cross-country analysis.
-

ICT in SMEs

Challenges of ICT adoption

- **Technical Support challenges.** In developing countries like Uganda, SMEs often lack the human technological resources needed for ICT implementation. Without internal technological capabilities, utilisation of ICT applications might be difficult and sometimes dangerous in terms of system maintenance and failures. The opposite is to seek advice and support from IT professionals, but most SMEs do not simply afford to do that because of the relatively high cost.
- **Lack of awareness-** uncertainty of ICT benefits, set-up costs and pricing issues and security concerns are the most visible barriers to ICT
- **Managerial challenges**. From managerial perspective, SMEs may also lack the managerial understanding and skills. ICT adoption projects are complex in nature and cannot be successfully implemented without relevant skills and a visionary mindset.
- **Administrative challenges.** The decision-making process of the managers is rather intuitive, based on instinctive decisions and is less dependent on formal models of decision making. They tend not to pass on information and do not delegate decision-making powers to their inferiors.

ICT in SMEs

Case Study: SMEs in Uganda

- In Uganda SMEs account for a significant share of production and employment and are therefore directly connected to poverty alleviation. While in many respects the Ugandan economy is different to that of other countries in the continent, for the poor population in the rural areas SMEs are also very relevant for employment and as an income source. Especially in developing countries like Uganda, SMEs are challenged by the globalisation of production and the shift in the importance of the various determinants of competitiveness.

Why government encourages SME access to and use of ICTS:

- The SME play a key role in national economic development strategies by facilitating flows of information, capital, ideas, people and products.

ICT in SMEs

- **The problem at hand in Uganda**
- Most SMEs in Uganda, do not appreciate the importance of using ICTs and e-business in the performance of their businesses. There is therefore need to establish the factors that have led to this reluctance towards the application of ICTs in the business processes of SMEs in order to exploit the benefits of these modern technologies which can be easily implemented for improved performance, cost reduction, competitive advantage and many others.

- Comparatively, medium-sized enterprises have made attempts to put ICT strategies in place. The medium-sized enterprises attach great value to information compared to small-sized enterprises perhaps because they have significant investments

ICT in SMEs

- **ICTs commonly used by SMEs in Uganda**
- The ICTs most commonly used by SMEs in Uganda include:
- Microsoft Office applications;
- computers;
- internet access;
- e-mail communications;
- telephones;
- photocopiers;
- printers; and
- Websites.

- However, unlike SMEs in developed countries, those in Uganda are not fully exploiting the potential of ICT to compete effectively in the international markets.

This is because of the following factors:

- lack of e-business / e-commerce infrastructure;
- lack of skills to develop and maintain interactive websites; and
- the use of obsolete technologies.
- high cost of internet connectivity;
- security issues concerning payments; and Shortage of skills.

ICT in SMEs

Sources of information used by SMEs

- SMEs in general obtain information from various sources, including:
- the internet;
- head offices;
- heads of department;
- brochures;
- other ICT companies;
- consultants;
- training seminars;
- trade catalogues;
- visits to relevant offices.

ICT in SMEs

Means of disseminating information by SMEs

SMEs disseminate information through a combination of methods, such as:

- e-mail;
- memos;
- staff meetings;
- departmental heads;
- newsletters;
- annual reports;
- websites;
- intranets;
- workshops;
- trade catalogues; and
- personal visits.

Information sharing among SMEs

Some of the SMEs have LANs, suggesting that they recognise the importance of information sharing. However, most applications implemented on the LANs are basic, such as e-mail applications, small databases, Microsoft applications, and product information that are largely for in-house use.

ICT in SMEs

- **Compliance by SMEs with information security procedures**
- Both small and medium-sized enterprises employ mainly antivirus programmes and regular backups to ensure the security of information. However, medium-sized enterprises in addition use sophisticated information security measures such as:
- firewalls;
- regular software updates;
- offsite storage;
- authentication;
- encryption; and
- audit trails for diagnostics.

ICT in SMEs

Barriers to adoption of ICTs by SMEs in Uganda

- Most of the current and potential clients for SMES in Uganda are not connected to the internet, largely because of high costs and a lack of awareness.
- The government has not put in place an e-commerce friendly environment, which would build consumer trust and business confidence.
- Moreover, the ICT market is not yet mature and people are yet to develop confidence in using ICTs. For example some people still tend to prefer going to the teller in the bank instead of querying and accessing their accounts through internet or mobile banking.
- Furthermore, telecommunication cost is high, quality sometimes poor and a barrier to transacting business on the web.

- PTO for more

ICT in SMEs

Barriers to adoption of ICTs by SMEs in Uganda

- Other barriers include:
  - limited and poor-quality bandwidth;
  - lack of security guarantees;
  - inadequate legislative framework;
  - frequent internet downtime;
  - slow internet access;
  - high taxation; and
  - inadequate technical support.

ICT in SMEs

Potential of ICTS for earning

Past exam Qn: Mention ways in which you will use the subsidiary ICT knowledge and skills you've acquired to earn income during your S6 vacation. (*5 mks)*

Possible Answers:

- Typesetting documents and printing business
- Taking on Data Entry jobs
- CD/ DVD writing and selling
- Provision of internet services
- Networking computers for organizations
- Desktop Publishing
- Computer Software Installation
- Computer Hardware Maintenance
- Image editing and graphic design
- Web page or website development
- Blogging
- Social Media marketing
- Computer Training, etc.