UNIT-4 (ICT-SEM-IV)
Effects Of Using IT

Software Copyright

Software copyright is the relatively recent extension of copyright law to machine-readable software. It is used by proprietary software companies to prevent the unauthorized copying of their software.

Software copyright, the relatively recent extension of copyright law to software, allowed a market for proprietary software to flourish for some time. Some proponents of free software use software copyrights in order to ensure that the software they write will remain free, using licenses such as the GNU General Public License

software copyright Until the late 1990s the only way of obtaining legal protection for software was by copyright. This was easy as no formal procedures were required since the copyright existed as soon as the software was created. However, copyright is a weak safeguard compared with a patent where ownership can be proved relatively easily and it is possible to sue without having to prove that copying has taken place. Unfortunately, getting a patent for software was a very difficult process. However, the late 1990s saw a liberalization of American practice and a number of computer programs and business processes have won patents.

HACKING

Hacking is unauthorized use of computer and network resources. (The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. Since the word "hack" has long been used to describe someone who is incompetent at his/her profession, some hackers claim this term is offensive and fails to give appropriate recognition to their skills.

Computer hacking is most common among teenagers and young adults, although there are many older hackers as well. Many hackers are true technology buffs who enjoy learning more about how computers work and consider computer hacking an "art" form. They often enjoy programming and have expert-level skills in one particular program. For these individuals, computer hacking is a real life application of their problem-solving skills. It's a chance to demonstrate their abilities, not an opportunity to harm others.

Hacking is a felony in the United States and most other countries. When it is done by request and under a contract between an ethical hacker and an organization, it's OK. The key difference is that the ethical hacker has authorization to probe the target. We work with IBM Consulting and its customers to design and execute thorough

evaluations of their computer and network security. Depending on the evaluation they request (ranging from Web server probes to all-out attacks), we gather as much information as we can about the target from publicly available sources. As we learn more about the target, its subsidiaries and network connectivity, we begin to probe for weaknesses.

Examples of weaknesses include poor configuration of Web servers, old or unpatched software, disabled security controls, and poorly chosen or default passwords. As we find and exploit vulnerabilities, we document if and how we gained access, as well as if anyone at the organization noticed. (In nearly all the cases, the Information Syhstems department is not informed of these planned attacks.) Then we work with the customer to address the issues we've discovered.

The number of really gifted hackers in the world is very small, but there are lots of wannabes.... When we do an ethical hack, we could be holding the keys to that company once we gain access. It's too great a risk for our customers to be put in a compromising position. With access to so many systems and so much information, the temptation for a former hacker could be too great -- like a kid in an unattended candy store.

VIRUS

Computer viruses are programs written by "mean" people. These virus programs are placed into a commonly used program so that program will run the attached virus program as it boots, therefore, it is said that the virus "infects" the executable file or program. Executable files include Macintosh "system files" [such as system extensions, INITs and control panels] and application programs [such as word processing programs and spreadsheet programs.] Viruses work the same ways in Windows or DOS machines by infecting zip or exe files.

A virus is inactive until you execute an infected program or application OR start your computer from a disk that has infected system files. Once a virus is active, it loads into your computer's memory and may save itself to your hard drive or copies itself to applications or system files on disks you use.

Some viruses are programmed specifically to damage the data on your computer by corrupting programs, deleting files, or even erasing your entire hard drive. Many viruses do nothing more than display a message or make sounds / verbal comments at a certain time or a programming event after replicating themselves to be picked up by other users one way or another. Other viruses make your computer's system behave erratically or crash frequently. Sadly many people who have problems or frequent crashes using their computers do not realize that they have a virus and live with the inconveniences.

Definitions of computer virus

Virus: a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer; "a true virus cannot spread to another computer without human assistance"

A computer virus is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. ...: A program which can be transmitted between computers via networks (especially the Internet) or removable storage such as CDs, USB drives, floppy disks, etc., generally without the knowledge or consent of the recipient. ... What are computer viruses, and where can I find more information?

A computer virus is a piece of code that is secretly introduced into a system in order to corrupt it or destroy data. Often viruses are hidden in other programs or documents and when opened, the virus is let loose.Virus is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

A computer program with the characteristic feature of being able to generate copies of itself, and thereby spreading. It is usually known as a dangerous program which is able to perform some harmful tasks. Harmful software that can damage a computer, sometimes beyond repair. Programming code created as a prank or as a malicious action that secretly affects other programs and causes unwanted consequences.

A virus is a software program designed to infect, destroy or interfere with a computer or software program.

Actions that are need to be taken to protect against hacking and Virus

Load only software from original disks or CD's. Pirated or copied software is always a risk for a virus.

Execute only programs of which you are familiar as to their origin. Programs sent by email should always be suspicious.

Computer uploads and "system configuration" changes should always be performed by the person who is responsible for the computer. Password protection should be employed.

Check all shareware and free programs downloaded from on-line services with a virus checking program.

Purchase a virus program that runs as you boot or work your computer. Up-date it frequently.

Virtual data still requires physical security. This could mean keeping your server in a locked room, removing disk drives from workstations that don't need them, and installing an alarm system in your office. All the security software in the world won't stop someone from breaking into your office and carting off your computers.

Beware of bugs**.** Most computer viruses are just a nuisance, but it takes only one malevolent virus to bring your network to its knees. Install reliable antivirus software, keep it updated, and train your employees to use it. Think about other protective measures, such as installing only shrink-wrapped commercial software on your computers.

Network security is a daily job. Stay on top of changes that could affect the security of your LAN. Keep your operating system updated with the latest security patches and bug fixes. Assign access to directories and other network resources on a need-to-have basis, and remove a user's account immediately when they leave your company. Use network logging and security tests to check your network for security holes and possible break-ins.

Pay attention to passwords**.** One bad password can compromise your entire network. Avoid passwords that contain dictionary words or personal information, and require users to change their passwords regularly. When an employee leaves the company, disable their password immediately as part of the termination process.

You must know that whether or not your PC will be hacked will depend very much on your actions as well. For example, downloading files from warez sites and poor habits of opening up strange email attachments, is as good as inviting hackers to break your door. So avoiding these type of activity can also prevent you from hacking and viruses

Stay alert for unusual activity on your accounts. If you have trouble logging into any of your accounts and you sure the username and password is correct – alert your ISP right away and send the account name with logins.

DO NOT use duplicate passwords, i.e. use different passwords for your affiliate accounts and server access. For your best defense against bruteforce password attacks, be sure your passwords are comprised of numbers as well as uppercase and lowercase letters and change your passwords regularly.

Last but not least, backup your sites' data! Although they probably do, it is not enough to count on your ISP to back up your site regularly. You can generate your own full site backups manually from cPanel.

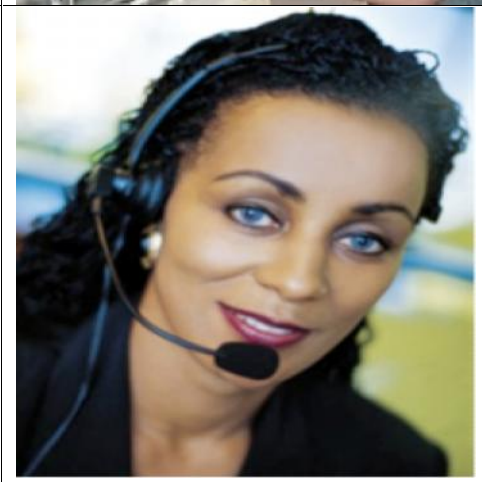
A alternative that may be preferable however, is to install software that does **automated backups** and has a quick and easy **restore process** such as Affiliate Backup. At the time of the hacker attack,

Although there is no way to completely eliminate hacker attacks, there is plenty you can do to prevent them from gaining access to your site. DO make the time and effort to protect yourself, because doing so after the fact takes 100 times more time and effort.

Effect of ICT on Patterns of Employment

The personal computer (PC) was developed in the early 1980s. Before this date, computers were huge, expensive machines that only a few, large businesses owned. Now PCs are found on almost every desk in every office, all over the world. Because companies now have access to so much cheap, reliable computing power, they have changed the way they are **organised** and the way they **operate**. As a result, many people's jobs have changed...

Areas of Increased employment

IT Technicians All of the computers in a business need to be maintained: **hardware fixed**, **software installed**, etc. **IT technicians** do this work.	
Computer Programmers All of the **software** that is now used by businesses has to be created by computer **programmers**. Hundreds of thousands of people are now employed in the '**software industry**'	
Web Designers Much of modern business is conducted **on-line**, and company **websites** are very important. Company websites need to be **designed** and built which is the role of **web designers**.	

Help-Desk Staff

People often need **help** using **computers**, and **software** applications.

Computer and software company have **help-desks** staffed by trained operators who can give **advice**.

Areas of Increased Unemployment

Some jobs have been lost as a result of computers being used to do the same work that people used to do.
Some examples of areas have suffered job losses

Manufacturing

Many factories now have **fully automated production lines**. Instead of using people to build things, **computer-controlled robots** are used.

Robots can run **day and night**, never needing a break, and **don't need to be paid**! (Although the robots **cost a lot to purchase**, in the long-term the factory saves money.)

Secretarial Work

Offices used to employee many **secretaries** to produce the **documents** required for the business to run.

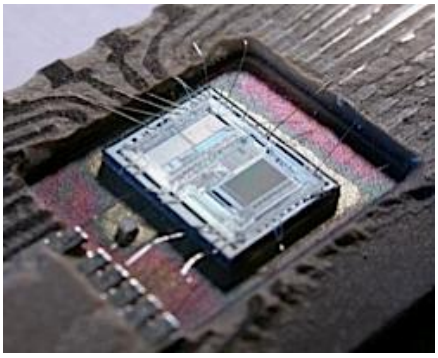
Now people have personal computers, they tend to **type and print their own documents**.

Accounting Clerks Companies once had large departments full of people whose job it was to do **calculations** (e.g. profit, loss, billing, etc.) A personal computer running a **spreadsheet** can now do the same work.	
Newspaper Printing It used to take a team of **highly skilled printers** to typeset (layout) a newspaper page and to then print thousands of newspapers. The same task can now be performed far more **quickly** using computers with **DTP** software and **computer-controlled printing presses**.	

The effects of microprocessor-controlled devices in the home

What is a Microprocessor?

A microprocessor is a **small CPU** built into a single '**chip**' (see below).



In a single 'chip', a microcontroller contains:

A **CPU**

Some **RAM**

Some **ROM** (Used for storing the devices **software**)

Examples of Microprocessor-Controlled Devices :

Many of the electronic devices that we use contain a microprocessor...

Some devices are used for **entertainment**:

Games consoles

DVD players

MP3 players

Some devices help to make our lives easier (**labor-saving devices**):

Programmable **microwave ovens**

Programmable **washing machines**

Home **security systems**

Mobile telephones

The effects on **leisure time** - microprocessor controlled domestic appliances such as washing machines, cookers, heating systems etc. do not need direct human control because they have timers, operating programs and safety checks built in. This means the user can leave them to complete their tasks so they have more leisure time.

The effects on **the need to leave the home** - computers linked to the Internet have greatly reduced the need for people to leave the home.

Entertainment - music and games can be downloaded. Movies can be downloaded and this, along with Interactive digital television, means there is no need to go to the cinema or video rental shop.

Goods - these can be easily ordered from online stores and delivered to the home.

Food - takeaway food and groceries can be ordered online and delivered directly to the door.

Services - banking, ordering insurance and many other services can be carried out over the telephone or the Internet.

The effects on **social interaction** - from the comfort of the home people can communicate in many more ways than the traditional telephone and postal service.

Email allows fast efficient communication with the ability to send files as attachments and email many people at the same time.

Online messaging allows users to sent text, images and files in real time, as well as communicate via voice and video.

Wireless phones and **mobile phones** allow interaction by telephone conversations from any room or the garden.

SMS (Short Messaging Service) text messages, images and video clips to be sent between mobile phones and computers.

Answer machines allow messages to be left for users who cannot answer the telephone.

Social interaction websites allow users to interact by leaving messages and adding comments to blogs. Users can also upload and share image and video files.

Capabilities of IT

Repetitive Processing – Computers can carry out the same or similar tasks (e.g. mailmerge, payroll) over and over very quickly and with a high level of accuracy.

Speed of Processing – A computer system can process raw data very quickly to produce information.

Data Storage Capacity – Traditionally, a company's information would be stored on paper in filing cabinets which takes up expensive storage space. A computer system can store the same amount of data in a fraction of the space. Other advantages include the ability to backup data easily and increase security by password protection or encryption.

Speed of Searching – Another big advantage of a computerised data storage system over a paper based system is that searches are virtually instantaneous.

Speed of Data Communications – Data can be sent from one side of the world to the other in a matter of seconds via the internet (e-mail) compared to days using traditional post ('snail mail').

The Ability to Produce Different Output Formats – Information can be output from a computer system, either on-screen or printed, in the form of graphs, charts, reports, pictures, sound etc.

Limitation of IT

Input (GIGO) – Even the most advanced data processing system will give inaccurate information if the data input is not accurate.

Hardware – The system must incorporate suitable hardware for the system to work efficiently (e.g. a barcode scanner in a shop or library, a plotter in architect's office or a powerful processor and graphics card in a CAD/CAM system.

Suitability of the Operating System – The right choice of operating system is vital for a system to work efficiently (e.g. a real time control system for air traffic control, a real time transaction for ticket sales or a batch processing system for payroll or billing)

Software – There are a number of problems that may arise when selecting appropriate software especially if the software is to be developed for a specific purpose:

- Possible changes in circumstances during development
- Time taken to implement the software
- Compatibility of the new software with current hardware and data
- Financial Costs
- Insufficient testing resulting in 'bugs'
- Poor communications with the user – the solution may not meet the user's requirements

ISSUES RELATED TO INFORMATION ON INTERNET

The Internet and World Wide Web are a fantastic **resource** for finding and sharing information. The Web contains literally billions of web pages containing information about every topic imaginable.

However we need to **take care** when using the Internet to **look for information**, or to **send information**...

Reliability of Information

The Internet and Web are **not regulated** - there is no organization that controls who can create web pages or what those pages can contain. **Anyone can create web pages** and say anything they want to.

In many ways this is a **good thing**. It means that corrupt organizations or governments, who have always been able to hide details of their activities, are no longer able to do so. When bad things happen, people write about it on the Web and the world gets to know, and hopefully do something about it. But it's also a **bad thing**. It means that people or organizations can easily **spread lies and hatred**. There are thousands of websites containing **bigoted viewpoints**, and thousands more that are full of information that is **biased**, **inaccurate**, or just plain **wrong**.

So... how do you know which web pages to believe, which information to trust?

Check **several sources** of information (go to lots of different websites). If they all say them same thing, it is likely to be true

Stick to websites that belong to **trusted organisations**. If the website address ends in **.gov.uk** (the UK government site) it is more likely to be reliable than one like www.tomiscool.net

Look at the **spelling and grammar** used. Reliable websites are usually checked for errors. Too many spelling errors mean it's probably not to be trusted.

Undesirable Information

Avoiding this type of material can be tricky. Many organisations such as **schools**, some **governments** (e.g. for religious reasons), and also many **parents**, make use of **web page filtering software**. This software attempts to prevent offensive and illegal material being accessed.

Even if filtering software is not installed on a computer, you can still take steps to help you avoid these types of sites:

Use the '**safe search**' feature on search engines such as Google.

Don't click the links that are shown in junk email (spam)

Think carefully about the **keywords** that you use to search with

Security of Data Transferred Using the Internet

As has been discussed already, you should always consider **encrypting** any **sensitive or personal data** that is sent or accessed over a public network such as The Internet.

Many websites, especially **online shopping** or **online banking** sites, require you to enter personal information, such as **credit card numbers**, social security **IDs**, etc. To make sure your data is safe, these websites use **encryption** - they are called **secure websites**. You should always make sure that a website is **secure** before giving personal information The website URL (address) should begin with **https**://... (normal, unsecure sites have addresses that start with http://...)

Your web browser should show a **closed padlock icon**

Potential Health Problem Related to Constant Use Of ICT

If we use a computer for many hours (as people often do at work), there are some health issues that might affect us...

Eye-Strain

One health issue that can occur after using computers for a long time is **eye-strain** (tiredness of the eyes). This is caused by looking at a **monitor** which is a **constant distance** away. The muscles that focus your eyes do not move, and so get **tired** and **painful**. Eye-strain can also cause **headaches**. This problem can be solved: **Look away** from the monitor at **regular intervals** – re-focus on distant or close objects to exercise the muscles in the eye. **Take regular breaks**. Use an **anti-glare filter** in front of the monitor to cut down on screen reflections that can also tire the eyes.	

Back and Neck Ache

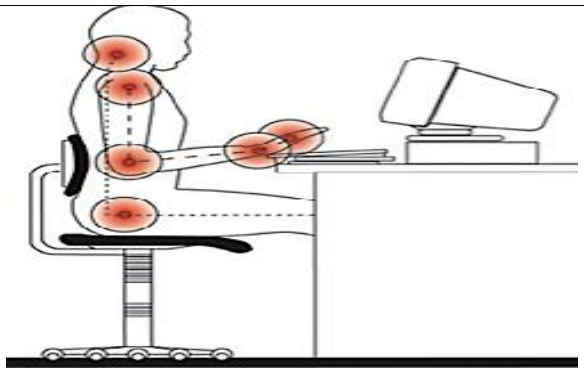
Many people suffer from **back and neck pain** after working at a computer for a long time. This is usually due to them having a **bad sitting posture**.

This problem can be solved:

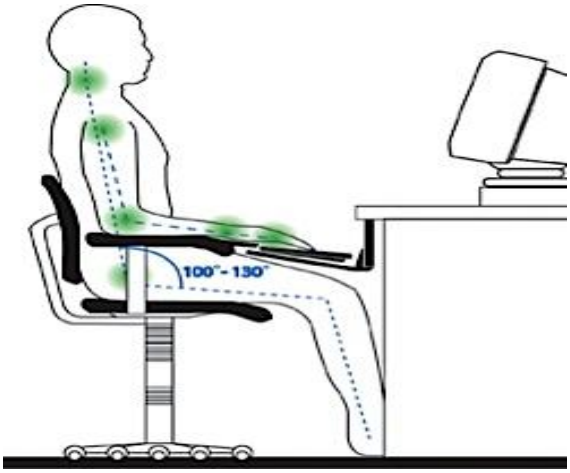
Use an **adjustable, ergonomic chair**, and take the time to s**et it up properly**.

The computer **keyboard** and **monitor** should be at the **correct height** for the seated person (keyboard lower than the elbow, top of monitor at eye level).

Take regular breaks: get up, walk around, stretch your muscles



Bad Position



Good Position

Repetitive Strain Injury (RSI) in Wrists and Hands

Any **repetitive** movement (same movement over and over again) can result in a health problem called **repetitive strain injury** (RSI).

In particular, **typing** and using a **mouse** for long periods are common causes of **RSI** in the **wrist** (it is often called carpal-tunnel syndrome).

his problem can be solved:

Use a **wrist-rest** to support the wrists while typing and when using the mouse.

Take regular breaks from typing or using the mouse.

MCQ

1.Software copyright is used by proprietary software companies to prevent the
a) Authority for copying software b) **unauthorized copying of their software.**
c) Both a and b d) None of these

2.Freeware Softwares are using
a) **GNU General Public License** b) software copyright
c) Both and a and b d) none of these

3. A _____ is inactive until you execute infected program or start your computer from infected hard disk
a) **Virus** b) Pen drive
b) Antivirus d) Spam

4. Hacking is
a) Authority for viewing software b) Authority for copying software
c) **unauthorized use of computer and network resources.** d) None of these

5. Computer hacking is the practice of _____to accomplish a goal outside of the creator's original purpose.
a) Adding computer software b) Adding computer hardware
c) **modifying computer hardware and software** d) Install software

6. The people who do computer hacking activities are often called
a) Master b) **hackers.**
c) experts d) All of these

7. Hackers have_____ in one particular program.
a) **expert-level skills** b) Masters
c) Low level skills d) Knoladge

8. Causes of hacking
a) old or unmatched software b) poorly chosen or default passwords.
c) disabled security controls d) **All of the above**

9. Virus is used to
a) To damage the data on your computer b) erasing your entire hard drive.
c) **All of the above** d) None of the above

10. Virus is
a) **A software program capable of reproducing itself and usually capable of causing great harm to files or other programs.**
b) A hardware capable of reproducing itself and usually capable of causing great harm to files or other programs
c) Both a and b d) None of these

11. A computer virus is a computer program that can
a) pest itself and infect a computer b) cut itself and infect a computer
c) **copy itself and infect a computer.** d) undo itself and infect a computer

12. Actions that are need to be taken to protect against and hacking and Virus is
a) Load only software from original disks or CD's. Pirated or copied software is always a risk for a virus
b) Execute only programs of which you are familiar as to their origin. Programs sent by email should always be suspicious.
c) Computer uploads and "system configuration" changes should always be performed by the person who is responsible for the computer. Password protection should be employed.
d) **All of the above**

13.Alternatives that may be preferable against virus
a) **backups and restore process** b) Format the software
c) A & B d) None of these

14. Following are the Leisure-Time microprocessor controlled devices using at home
a) Washing machine b) Microwave Owen
c) Heating system d) All of above

15. All of the computers in a business need to be maintained by
a) hardware fixed b) software installed
c) **Both of these** d) None of this

16.Computer programmers are the one
a) **Who develop the program** b) who design the software
c) Both of these d) None of these

17. Web designers are the one
a) Who design the company software b) **Who design websites**
c) Who installed software d) B & C

18. Computer and software company have _____ staffed by trained operators who can give **advice**.
a) Secretarial Work b) Manufacturing
c) **help-desks** d) None of these

19. Many factories have _____ to build things automatically
a) Computer b) Chip
c) Men d) **computer-controlled robots**

20._____ employee to produce the documents required for the business to run.
a)**secretaries** b) Accounting Clerks
c) Manager d) Director

21. Companies once had large departments full of people whose job it was to do calculations
a) Secretaries b) Manager
c) **Accounting Clerks** d) Director

22. Newspaper Printing used to take a team of _____to typeset (layout) a newspaper page and to then print thousands of newspapers.
a) Dot Matrix Printer b) Inkjet printer
c) Colored printer d) **highly skilled printers**

23. A microprocessor is a
a) RAM b) **small CPU in a single chip**
c) ROM d) Electronic devices

24. Examples of Microprocessor-Controlled Devices
a) Games consoles b) DVD players
c) MP3 players d) **All of the above**

25. SMS means
a) Short massage sending b) sending message service
c) **Short Messaging Service** d) sending message shortly

26**.** Mobile phones are used for
a) Email b) SMS
c) Entertainment d) **All of the these**

27._____ allows fast efficient communication with the ability to send files as attachments.
a) **Email** b) SMS
c) Entertainment d) All of the above

28. The telephone or the Internet provide the serves like
a) Online banking b) Online ordering insurance
c) None of this d) **Both of this**

29. _____allow messages to be left for users who cannot answer the telephone.
a) **Answer machines** b) voice machines
c) Email machines d) transport machines

30. Following are the characteristic or advantages of using computer
a)Accuracy b) Speed
b)Data Storage d) **All of above**

31.Following are the drawbacks of IT
a) GIGO b) Failure of hardware

c) lack of suitable software d) **All of above**

31. Which of the following is the issues related to information on internet
a) Speed processing b) **Undesirable information**
c) Data storage d) None of these

32. The information which is bad or not provided by any authorized organization found on internet is called
a) **Unreliable information** b) Undesirable information
c) Both a amd b d) None of these

33. If the web site address ends with **.gov.in ,** it belongs to
a) **Indian government site** b) Indian site
c) UK government site d) Indonesia government site

34. The information which user does not want or require while surfing on internet is called
a) **Undesirable information** b) Reliable information
b) Unreliable information d) Desirable information

35. To make the data secure following process is done
a) Decryption b) **Encryption**
b) Filtering d) All of above

36. Which of the following health problem can be occurred due to constant use of IT
a) Eye strain b) Back and Neck Ache
b) RSI d) **All of these**

37. The website begin with name “https:\” is
a) **Secure website** b) Unsecure website
b) Both a and b d) None of these

38. The website begin with name “http:\” is
a) **Secure website** b) **Unsecure website**
b) Both a and b d) None of these