Details of Curriculum for Class XI

Lesson 1: Computer Security

Objective: Students will able to

- *Understand computer security and its policies, procedure and tools that are necessary to protect computer system.*
- *Define malicious programs and its effects*
- *List various ways to protect computer system*
- *Differentiate between authentication and identification*

Computer security refers to the protection given to computers and information contained in them from unauthorised access.

1.1 Why Computer Security?

- We need to protect
  - Our data
  - Our ability to use our computers (denial of service attacks)
  - Our reputation with DOE, Congress and the general public

Major sources of danger

- Running malicious code on your machine due to system or application vulnerabilities or improper user actions
- Carrying infected machines (laptops) in from off site

The practice of computer security also includes polices procedures hardware and software tools that are necessary to protect the computer systems.

Security properties

- ***Confidentiality***
  - Information about system or its users cannot be learned by an attacker. Strict controls must be implemented to ensure that only those people who need access to certain information have that access. The most common form of access control is the use of password and keeping password confidential is one of the most fundamental principles of computer security.
- ***Integrity***
  - The system continues to operate properly, only reaching states that would occur if there were no attacker

  Integrity ensures that information cannot be modified in unexpected ways as loss of integrity could result from human errors, intentional tampering or even catastrophic events. The consequences using inaccurate information can be disastrous therefore an effort must be made to ensure the accuracy and

integrity of data at all times. For this encryption process is used which transforms information into some secret form to prevent unautharised individual from accessing the data

- ***Availability***
  - Actions by an attacker do not prevent users from having access to use of the system. Availability prevents resources from being deleted or becoming inaccessible. This applies not only to information but also to the machines on the network and other aspects of the technology infrastructure. This inability to access the required resources is called ‘ denial of service ‘ .

1.2. Common Security Threats

- ***Errors and omission***

  Users, system operators and programmers frequently make unintentional errors, which contributes security problems directly and indirectly resulting in system crashes. Many programs, especially those designed by users for personal computers lack quality control measures. However, even most sophisticated programs cannot detect all types if input errors or omission. A sound awareness and training program can help an organization reduce the number and severity of errors and omission.

- ***Fraud and theft***

  Information technology is increasingly being used to commit fraudulent and theft activity. Computer system are exploited in numerous ways both by automating traditional methods of fraud and by using new methods. For examples individual may use a computer to steal money from a large number of financial accounts thus generating a significant sum for their own use. Financial systems are not only institution facing fraudulent activity, systems, which control access to any resources are targets, such as time and attendance system, Inventory system, school grading systems, or long distance telephone systems.

  The majority of fraud uncovered on computer system is committed by insiders who are autharised users of a system.

- ***Loss of physical and infrastructural support***

  The infrastructural support includes power failures, loss of communications, water outages and leaks, lack of transportation service, natural calamity and so forth. Recent study has shown that

more loss is associated with fires and floods than with viruses and other more widely publicized threats.

- ***Hackers and crackers***
  The term hackers refer to a person who breaks into computer without autharisation. They enter corporate and government computers using stolen passwords and security loopholes and steal in formations, transfers money to their accounts, and do lot of other criminal activity. They do lot of malicious activities like changing passwords, shutting down or crippling the system. A growing numbers of hackers are part of the electronic crimes rings internet on stealing credit card numbers and other sensitive information and this kind of theft is difficult to detect because criminal usually leave behind no evidence of their visits. Cracker is an individual who attempts to access computer system without authorization. This individual are opposite to hackers destroy the data once into another computer system.

1.3. *Malicious programs*

It is often seen that users opens up certain files (such as game ,utility and so on) on the internet. On opening of such files , a users begins to face unusual activities from the computer, such as malfunctioning of the application or inefficient running of hardware resources and so on. Such unusual activity is the result of malicious programs which penetrate with the useful file. This malicious program are often called virus, worms, Trojan horse, logic bomb, spyware etc.

1. Virus

A computer virus is a type of malware that is intentionally written to gain entry into your computer, without your knowledge or permission. It has the capacity to modify or replicate itself, in which case it will continue spreading. There are varying different types of computer viruses and their effects also vary widely.

- **Boot Sector viruses:** This virus infects the hard disk's or floppy drive's boot sector. This would make the computer unable to boot. These viruses can, however, be avoided by ensuring that the hard drive is well protected. Never start the computer using an unknown disk drive Boot sector Virus .Examples are Brain, Joshi, BDF

- **File infecting Virus:** This virus infects executable files or programs. On running the programs, the virus would be activated, then be able to carry out its damaging effects. Most of the existing viruses are in this category.eg Raindrop, Jerusalem
- **Polymorphic Virus:** This virus gets copied from file to file as its propagates. Such virus is difficult to detect because each copy it generates appears different from other one.
- **Stealth Virus**: This types of virus attempts to conceal its presence from users
- **Multipartite Virus**: This virus infects both boot sector and executable files and uses both mechanisms to spread.eg one-half virus

2. ***Malicious codes and software***

Malicious codes are the software programs that generate threats to the computer system and precious data. The code can be in the form of worms, Trojan horses, logic bombs and other 'uninvited' virus.

- **Worm: Worm** is also a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped
  Eg code red

- **Trojan Horses: Trojan Horse** is a destructive program. It usually pretends as computer games or application software. These program enters into a computer through an e-mail or free program downloaded from internet If executed, computer system will be damaged.eg back orifice

- **Logic bomb**: A **logical bomb** is a destructive program that performs an activity when a certain action has occurred. It is program or portion of program piece which lies dormant until specific piece of program logic is activated. The most common activator of logic bomb is date. For example the well known logic bomb is Michelangelo which has a trigger set for Michelangelo's birth date, it causes system crash or data loss or other unexpected interaction with existing code.

1.4.***Affecting computer system***

How virus spreads:

- Virus is designed to proliferate and propagate in computer network. This means any contact between two or computers is an opportunity for infection.
- Unauthorised users break into a computer system and easily cause destruction by planting virus in the most sensitive locations of the computer.
- Virus can be spread through infected software transmitted from disk, network, e-mail, or other storage devices.

Protecting Computer system

- **A**lways update your anti-virus software at least weekly.
- **B**ack up your important files and ensure that they can be restored.
- **C**hange the computer's boot sequence to always start the PC from its hard drive
- **D**on't share Drive C: without a password and without read-only restrictions.
- **E**mpty floppy drives of diskettes before turning on computers, especially laptops
- **F**orget opening unexpected e-mail attachments, even if they're from friends
- **G**et trained on your computer's anti-virus software and use it.
- **H**ave multiple backups of important files. This lowers the chance that all are infected.
- **I**nstall security updates for your operating system and programs as soon as possible
- .**J**ump at the chance to learn more about your computer. This will help you spot viruses

1.5. **Users Identification and authentication**

Identification and authentication (I&A) is another line of defense against the unauthorised people from entering into a computer system. I&A is a building block of computer security as it forms the basis for the most types of access controls and for establishing user's accountability. Such access control often requires a system to identify and differentiate among different users. *Identification* is the means through which user provides a claimed identity to the system. *Authentication refers to establishing value of the claim.* Computer system uses the data authentication for recognizing people.

There are three ways of authenticating users' identity. These can be done using alone or in combination with others.

1. User Requirements (Password, PIN, Cryptographic key)
2. Users Possessions (ATM card, Smart Card)
3. Users Biometric (Voice pattern, handwriting dynamics, fingerprints)

1. **User Requirements**

   The most common form of information and authentication is the combination of user ID and password. Password system works by requiring the user to enter a user ID and password (personal identification number).The system compares the previously stored password for the user ID . If there is a match, the user is authenticated and granted access. These types of security access have been successfully providing security to a computer system for a long time. However this techniques dependent upon keeping password secrets. Unfortunately there are many ways that the secret key may be divulged.

- ✓ **Finding passwords**

  If the user creates a password, he may tend to make it easy to remember. On other hand, assigned password may be difficult to remember, so users are more likely to write them down. In both cases s to finding of password unauthorise users become more easier.

- ✓ **Giving Passwords**

  Users may share their password with others for sharing files. In addition people can be trickle into divulging their passwords.

- ✓ **Electronic Monitoring**

When passwords are transmitted to a computer system, they can be electronically monitored. This can happen on the network used to transmit the passwords on the computer system itself

2. **Users Possessions**

- ✓ **Memory tokens**

  Memory tokens are meant for storing information. The most common types of memory tokens are credit cards. A common application of memory tokens for authentication to computer system is the automatic teller machine (ATM) Card.

  Memory tokens when used with PIN provide significantly more security than passwords. A hacker must have both valid token and corresponding PIN to pretend someone else. This is much more difficult than obtaining valid password and user ID combination. However this method also has certain limitation, although

sophisticated technical attacks are possible against memory tokens system.

- ✓ **Smart tokens**
  A smart token requires the user to provide something the user to provide something the user know (PIN or password) in order to unlock the smart token for use. `

3. Biometric Technique

Biometric authentication Technologies uses the unique characteristics of an individual to authenticate the person's identity. This includes physiological attributes (such as fingerprints, hand geometry or retina patter) or behavioural pattern (such as voice pattern and hand written signature)

(Ref E-book Am introduction to computer security: NIST Handbook)

Lesson2: The internet and Privacy

Objective: Students will able to

- ***Define various terms related to internet and privacy***
- ***Name the various parts in URL***
- ***Differentiate between legal and illegal post on internet***
- ***Know to tag ,share and forwarding***

2.1. Terms used in internet

Apps and Applets
Apps and applets are small software applications. They are designed to be much smaller than regular computer software, but still provide very useful functions. Lately, apps are very popular with cellphone and mobile platforms; specifically: with the Apple iPhone and the Google Android phone.
Examples of apps: rangefinder GPS for golfing, song identification software, restaurant reviews, pocket video games, language translators for traveling.

Blog - A blog is information that is instantly published to a Web site. Blog scripting allows someone to automatically post information to a Web site. The information first goes to a blogger Web site. Then the information is automatically inserted into a template tailored for your Web site.

Bookmark - a way of storing your favorite sites on the Internet. Browsers like Netscape or Internet Explorer let you to categorize your bookmarks into folders.

Browser - A software program that allows users to access the Internet.
Examples: ***Non-graphical:*** a user interface for computers which allows you to read plain text, not pictures, sound, or video, on the Internet. It is strictly text based, non-Windows, and does not place high memory demands on your computer. An example is **lynx**

Graphical: a user interface for computers which enables people to see color, graphics, and hear sound and see video, available on Internet sites. These features are usually designated by underlined text, a change of color, or other distinguishing feature; sometimes the link is not obvious, for example, a picture with no designated characteristic. Examples
are **Netscape** and **Internet Explorer**.

Chat - real-time, synchronous, text-based communication via computer.

Clickbait-is a term describing web content that is aimed at generating online advertising revenue, especially at the expense of quality or accuracy, relying on sensationalist headlines or eye-catching thumbnail pictures to attract click-throughs and to encourage forwarding of the material over online social networks. Clickbait headlines typically aim to exploit the "curiosity gap", providing just enough information to make the reader curious, but not enough to satisfy their curiosity without clicking through to the linked content.

Cookie - Information (in this case URLs, Web addresses) created by a Web server and stored on a user's computer. This information lets Web sites the user visits to keep of a user's browsing pattterns and preferences. People can set up their browsers to accept or not accept cookies.

Cloud Computing-Cloud computing is a fancy term to describe that your software is online and 'borrowed', instead of purchased and actually installed on your computer. Web-based email is the most prevalent example of cloud computing: the users' email is all stored and accessed 'in the cloud' of the Internet, and not actually on their own computers.

E-commerce

E-commerce is 'electronic commerce': the transacting of business selling and buying online

Firewall - The name "firewall" derives from the term for a barrier that prevents fires from spreading. A computer "firewall" is a barrier between your computer and the outside world. Just like a fire is most likely to spread through open doors in a building, your computer is most vulnerable at its ports (the doors). Without ports you could not go on the Internet or let Internet traffic enter your computer.
An effective software firewall isolates your computer from the Internet using a code that sets up a blockade to inspect each packet of data, from or to your computer — to determine whether it should be allowed to pass or be blocked.

Flash - Animation software used to develop interactive graphics for Web sites as well as desktop presentations and games (Windows and Mac) by the company Macromedia. Flash on the Web is displayed by a browser plug-in. Non-Web presentations are run by a Flash player, included on a floppy or CD-ROM. Flashcan be used to create vector-based graphics in one or more timelines that provide a sequential path for actions.

FTP - Using file transfer protocol software to receive from upl**oad) or send to (download) files (text, pictures, spreadsheets, etc.) from** one computer/server to another.

HTML - A type of text code in Hypertext Markup Language which, when embedded in a document, allows that document to be read and distributed across the Internet.

HTTP - The hypertext transfer protocol (http) that enables html documents to be read on the Internet.

Hypertext - Text that is non-sequential, produced by writing in HTML (**H**yper**t**ext **M**arkup **L**anguage) language. This HTML coding allows the information (text, graphics, sound, video) to be accessed using HTTP (Hypertext Transfer Protocol).

Hyperlink - Text, images, graphics that, when clicked with a mouse (or activated by keystrokes) will connect the user to a new Web site. The link is usually obvious, such as underlined text or a "button" of some type, but not always.

Instant Messaging (IM) - a text-based computer conference over the Internet between two or more people who must be online at the same time. When you send an IM the receiver is instantly notified that she/he has a message.

IP Address - IP (Internet Protocol) address is the number or name of the computer from which you send and receive information on the Internet.

Your computer's 'internet protocol' address is a four-part or eight-part electronic serial number. An IP address can look something like '202.3.104.55' or like '21DA:D3:0:2F3B:2AA:FF:FE28:9C5A', complete with dot or colon separators. Every computer, cell phone, and device that accesses the Internet is assigned at least one IP address for tracking purposes. Wherever you browse, whenever you send an email or instant message, and whenever you download a file, your IP address acts like a type of automobile license plate to enforce accountability and traceability

Portal - A Web site "gateway" that provides multiple services, which could include Web searching capability, news, free-email, discussion groups, online shopping, references and other services. A more recent trend is to use the same term for sites that offer services to customers of particular industries, such as a Web-based bank "portal," on which customers can access their checking, savings and investment accounts.

WWW-The **World Wide Web** (**WWW**) is an information space where documents and other web resources are identified by URLs, interlinked by hypertext links, and can be accessed via the Internet

2.2. URL

URL - A universal resource locator (a computer address) that identifies the location and type of resource on the Web. A URL generally starts with "http." URL's, or 'uniform resource locators', are the web browser addresses of internet pages and files. A URL works together with IP addresses to help us name, locate, and bookmark specific pages and files for our web browsers The format of URL has four parts: Protocol, server(domain name and domain type), path and file name. Here is an example,

https://www.bankofamerica.com/login/password.htm

- **Protocol**: http
- **Host Computer Name:** www
- **Domain Name:** bankofamerica
- **Domain Type:** com
- **Path:**/login
- **File Name:** Password.htm

  The first part of the address, the part before colon, is the access method. Apart from http (hyper text transfer protocol) you could also find other protocol such as ftp (file transfer protocol),news (news server), mailto(mail server) and telnet(for accessing remote computers) The protocol is separated by colons and slashes. After slashes ,the host computer 's name is displayed that is, an indicator such as www, which stands for world wide web. Next comes the domain name ,it is the unique and case sensitive human readable name for a host on the internet.Domain type such as .com represents type of the organization or country to which the host belongs

  Domain Types

- .**gov** - Government agencies
- . **edu** - Educational institutions
- . **org** - Organizations (nonprofit)
- . **mil** - Military
- .**com** - commercial business
- .**net** - Network organizations
- **ca** - Canada
- .**th** - Thailand

- http://forums.about.com/ab-guitar/?msg61989.1

- ftp://files.microsoft.com/public/eBookreader.msi
- telnet://freenet.edmonton.ca/main

2.3. Terms used in internet privacy

- **Cyberbullying** :
  cyberbullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass, threaten or intimidate someone.
- ***Digital footprints***
  There are two main classifications for digital footprints: passive and active. A passive digital footprint is created when data is collected without the owner knowing, whereas active digital footprints are created when personal data is released deliberately by a user for the purpose of sharing information about oneself by means of websites or social media.

- ***Cyberstalking****(online stalking)*
  It has been defined as the use of technology, particularly the Internet, to harass someone. Common characteristics include false accusations, monitoring, threats, identity theft, and data destruction or manipulation. Cyberstalking also includes exploitation of minors, be it sexual or otherwise.

- ***Spamming***
  Electronic spamming is the use of electronic messaging systems to send unsolicited messages (**spam**), especially advertising, as well as sending messages repeatedly on the same site.

- ***Phishing***
  Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.
  Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page

- **Spoofing**

Spoofing is a type of scam where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user. The main purpose is to trick the user into releasing sensitive information in order to gain access to one's bank account, computer system or to steal personal information, such as passwords.

- ***door Back***
  Hidden software or hardware mechanism used to circumvent security controls and gain entry into an information system mostly with malicious interest.

- Card Skimmer
  An illegal electronic device that can capture all of the personal information from credit card or debit card

Information and privacy – 2 sides of the same coin
Privacy means to keep to yourself information about you and your closest friends and families. Information like – Age, Full Name, Address, Phone Number, Name of School, Password Information (even to friends), Images (At this age, kids get into social networking and will be sharing images via cell phones and digital cameras.)

Situations where the right to privacy is being violated or is likely to be violated.

Provide simple scenarios where the right to privacy is being misused. Students must say whether or not the right to privacy is being misused. For example:
1. Radhika has a FB friend Maya. Maya wants Radhika's friend's History notes and requests her to share her friend's phone number. Radhika hands it over to Maya immediately. (Y or N)
2. Pratap's uncle comes home to visit them. His uncle wants the link of the site from where he can purchase cheap spare parts for his motor bike. Pratap e-mails the link to his uncle. (Y or N)

● 5 Questions to consider before posting anything
a. Is it violating my or someone else's right privacy
b. Is this absolutely necessary to post this?
c. How will it help me and/or others?
d. Is this saying something bad about others?
e. Is this hurting another individual?

Use of the five questions while posting which question is being disregarded by a certain post. For example:
a. Neeta posts a picture of herself and her best friend who had gone for a picnic. (Question a)
b. Asif tweets about how Amit got scolded by the Math teacher. (Question e, d)

2.4. *Protecting What Is Yours*

- ***Password***
  Password is a set of secret characters or words utilized to gain access to computer ,web, network resources or data.

  Strong password and weak password
  Strong password
  Term used to describe a password that is an effective password that would be difficult to break often.
- Use strong passwords Be creative: use a hobby:
  - Watching Sci Fi: SciFicTV
  - Better variation: Sc2F3c&TV ; longer = better
  - Use acronyms rather than dictionary words: CKKBKBP, which means for music students “Chodo kal Ki Bate Kal Ki Baat Purani”
  - Use 6 to 16 characters – a minimum of 8 is best – that includes at least one number and one special character, such as % or &.

Weak Password
A password that is not effective password because it is easy to remember and break. Examples of weak password are name, birth date, phone number or easy guessable words.

Things to remember

- *Always* change the password provided by a vendor or other system provider
- Change your password frequently – at least once every three to six months
- If you think your password has been compromised, *change it immediately*
- Protect your security codes and passwords by keeping them secret. Do not write them down or store them on your computer!
- **Lock your computer when you leave your desk.**

Lab Session

Tagging

What is tagging and how does it work?

When you tag someone, you create a link to their profile. The post you tag the person in may also be added to that person's Timeline. For example, you can tag a photo to show who's in the photo or post a status update and say who you're with. If you tag a friend in your status update, anyone who sees that update can click on your friend's name and go to their profile. Your status update may also show up on that friend's Timeline

How do I tag myself or my friends in photos?

To tag yourself or your friends in a photo:

1. Click the photo to expand it
2. Hover over the photo and click **Tag Photo** at the bottom
3. Click the person in the photo and start typing their name
4. Choose the full name of the person you want to tag when it appears
5. Click **Done Tagging**

If you want to tag friends in multiple photos in an album at once:

1. Go to the album
2. Click **Tag** at the top right of the page
3. Enter the name of a friend or page to tag
4. Click each photo you want to tag with that name
5. Click **Save Tags** when you're finished
6. Repeat this process for each friend or page you'd like to tag

Keep in mind that when you tag someone in a photo, that person's friends may also see, like or comment on the photo. Also, if you tag a photo that was not uploaded by a friend, the person who uploaded the photo will need to approve the tag.

How do I remove a tag from a photo or post I'm tagged in?

To remove a tag from a post you've been tagged in, click ⌄ in the top right of the post and select **Remove Tag**.

You can also remove tags from multiple posts at once:

1. Go to your activity log
2. Click **Photos** in the left column
3. Click to check the box to the left of the posts you'd like to remove a tag from
4. Click **Report/Remove Tags** at the top of the page
5. Click **Untag Photos** to confirm

Removed tags will no longer appear on the post or photo, but the post or photo is still visible to the audience it's shared with. People may be able to view the post or photo in places like News Feed or search results. To fully remove it from Facebook, ask the person who posted it to take it down

- **Sharing (online file , photographs, pictures documents etc)**
- **Forwarding (E-mails, messages etc)**
- **Reply / Reply All / Bcc (E-mail)**
- **Re-tweeting (tweeter etc)**

A *Retweet* is a re-posting of a Tweet. Twitter's *Retweet* feature helps you and others quickly share that Tweet with all of your followers. You can *Retweet* your own Tweets or Tweets from someone else. Sometimes people type RT at the beginning of a Tweet to indicate that they are re-posting someone else's content.

● I***nstagramming***

Instagram is an online mobile photo-sharing, video-sharing, and social networking service that enables its users to take pictures and videos, and share them either publicly or privately on the app, as well as through a variety of other social networking platforms, such as Facebook, Twitter, Tumblr, and Flickr.

Ref: http://netforbeginners.about.com

Wikipedia, the free encyclopedia

https://en.wikipedia.org/wiki/Password_strength

http://www.webopedia.com

Lesson 3: Social Media

Objective: Students will able to
Know the characteristics of Social media
Understand various ways in which social media impacts society
Recall qualities of being good digital citizen

3.1. *Ease of expressing yourself in social media*

Social media is the electronic communication through which users creates online communities to share information, ideas, personal messages and other content such as audio, video, pictures etc.

Characteristics of Social media

1. Web Space
   The website should provide the users free web spaces to upload content.
2. Web address
   The users are given a unique web ad dress that becomes their web identity. They can post and share all their content on this web address.
3. Build profiles
   Users are asked to enter personal details like name, address, date of birth education, professional etc. The site then mines the personal data to connect individuals.
4. Upload content in real time
   Users are provided with tools to post content in real time. The last post comes first giving the site freshness.
5. Enable conversation
   Members are given right to comment on posts made by friends and relatives. The conversation are great social connect.
6. Post have time stamp
   All post are time stamped, making it easy to follow post.

IMPACT OF SOCIAL MEDIA ON VARIOUS FIELDS

1. Education

As per the survey of previous research, 90% of college students use social networks. Technology has shown a rapid development by introducing small communication devices and we can use these small communication devices for

accessing social networks any time anywhere, as these gadgets include pocket computers, laptops, iPads and even simple mobile phones (which support internet) etc. For the purpose of education social media has been used as an innovative way. Students should be taught to use this tool in a better way, in the educational classes' media just being used for

messaging or texting rather than they should learn to figure out how to use these media for good. Social media has increased the quality and rate of collaboration for students. With the help of social media students can easily communicate or share information quickly with each through various social sites like Facebook, Orkut, and Instagram etc. It is also important for students to do some practical work instead of doing paper work. They can also write blogs

Positive Effect of Social Media on Education

- Social media gives a way to the students to effectively reach each other in regards to class ventures, bunch assignments or for help on homework assignments
- Many of the students who do not take an interest consistently in class might feel that they can express their thoughts easily on social media.
- Teachers may post on social media about class activities, school events, homework assignments which will be very useful to them.
- It is seen that social media marketing has been emerging in career option. Social media marketing prepares young workers to become successful marketers.
- The access of social media provides the opportunity for educators to teach good digital citizenship and the use of Internet for productivity .

Negative effect of Social Media on Education

- The first concern about the negative effect comes to mind is the kind of distraction to the students present in the class. As teachers were not able to recognize who is paying attention in the classroom
- One of the biggest breakdowns of social media in education is the privacy issues like posting personal information on online sites.
- In some of the scenario there were many in appropriate information posted which may lead the students to the wrong side.
- Because of social media students lose their ability to engage themselves for face to face communication.
- Many of the bloggers and writers posts wrong information on social site which leads the education system to failure.

2. Business

Social media is the new buzz area in marketing that includes business, organizations and brands which helps to create news, make friends, make connections and make followers. Business use social media to enhance an organization's performance in various ways such as to accomplish business objectives, increasing annual sales of the

organization. Social media provides the benefit as a communication platform that facilitates two way communications between a company and their stock holders. Business can be promoted through various social networking sites. Many of the organization promotes their business by giving advertisement on the social
media in order to attract maximum users or customers.

Positive Effect of Social Media on Business

- Social Media helps to better understand their audience by their likes and dislikes
- It helps the business for promotional activities.
- Social networking sites helps to make new customers by providing useful facilities.
- Helps to enhance market insight and stretch out beyond your rivals with online networking.
- It also helps to increase awareness among brands and reach with little to no budget

Negative Effect of Social Media on Business

- In business filed social media is not entirely risk free because many of the fans and followers are free to post their opinion on a particular organization, the negative comment can lead the organization to failure.
- Many of the large organization have fallen victim to the hackers.
- The wrong online brand strategy can doom a company, and put at a huge viral social disadvantage.
- Getting involved with Social Media is very time consuming. As an organization you should assign a person to always bolster your pages and profile with significant substance.
- Most companies have difficulty measuring the results of social media advertising

3. Society

As we all are aware of social media that has an enormous impact on our society. Many of the social media sites are most popular on the web. Some social media sites have transformed the way where people communicate and socialize on the web. Social networking sites render the opportunity for people to reconnect with their old friends, colleagues and mates. It also helps people to make new friends, share content, pictures, audios, videos amongst them. Social media also changes the life style of a society.

Positive Effects of Social Media on Society

- Social Media helps to meet people they may not have met outside the social media forums.
- It also helps to share ideas beyond the geographical boundaries.
- It provides open opportunity for all writers and bloggers to connect with their clients.
- It unites people on a huge platform for the achievement of specific goals. This brings positive change in the society.
- Social media provides awareness among society like campaigns, advertisement articles, promotions which helps the society to be up to date with the current information.

Negative Effects of Social Media on Society

- it make people addicted. People spend lots of time in social networking sites which can divert and focus from the particular task.
- Social media can easily affect the kids, the reason is sometimes people shares photos, videos on media that contain violence and negative things which can affect the behavior of kids or teenagers.
- It also abuses the society by invading on people's privacy.
- Social lives like family also weaken as people spend more time connecting to new people.
- Some people use their images or videos in social sites that can encourage others to use it false fully.
-

4. ***Youngsters***

   Nowadays social media has become a new set of cool tools for involving young peoples. Many young people's day to day life are woven by the social media Youngsters are in conversation and communication with their friends and groups by using different media and devices every day. In past years it was seen that youngsters are in touch with only friends and their groups in schools and colleges. But nowadays youngsters are in contact not only with known friends but also with unknown people through social networking sites, instant messaging etc. Throughout the country teenagers frequently use the web, mobile phones, and online games to communicate and gather information with each other.

Positive Effects of Social Media on Youngsters

- Social media helps youngsters to stay connected with each other.
- Useful information can be exchanged over social networking sites.

- Social networking sites can allow teens to find support online that they may lack in traditional relationships, especially for teens.
- In a Critical Development period youngsters also go for social networking sites for advice and information.
- Youngsters can look to social media for getting the answers related to their career objectives.

Negative Effects of Social Media on Youngsters

- Today it's not clear that who the "strangers" are especially in the field of social media.
- Kidnapping, murder, robbery can be easily done by sharing details on social media.
- There are many cases registered in police station where adults target young children and lure them into meeting them.
- Mostly youngsters waste lots of time on social sites like chatting which also affects their health.
- Some useless blogs influence youth extremely that they become violent and can take some inappropriate action

The social and political impact

- Technology has played a major role in politics for the past few decades such as Digitally processed Voters' Identity Cards, use of electronic ballot Machines, Debates Interviews and discussion on the electronic media
- Canvassing trough the social media was observed in the recent elections

In that way, social media is a natural progression for a democracy such as but the tools have only come into ,The intent has always been such .India Indians are voicing their opinions wi ,With social media platforms .beingth a vengeance.

3.2, Netiquette(What does it mean to be respectful)

Good Digital Citizen Guidelines

- Protect your online privacy.
- Respect the online privacy of others.
- Respect the rules, values, and policies of your family, religion, community, and school.
- Understand the values of other cultures, religions, and communities.
- Build a positive online reputation and portfolio of work.

- Use online communications in constructive ways, doing nothing you would not do in a F2Fo (face to face) setting.
- Evaluate the accuracy of any information you find or receive online - or share online.
- Maintain a healthy balance between your online activities and relationships with your physical world activities and relationships

http://www.seochat.com/c/a/social/social-media-and-society-the-good-the-bad-and-the-ugly/
http://www.ijcat.com/archives/volume5/issue2/ijcatr05021006.pdf
https://en.wikipedia.org/wiki/Internet_troll
http://www.slideshare.net/dhruva.trivedy/role-of-social-media-in-politics

Lesson 4: Cyber Crime

Objective: Students will be able to

- *Define Cyber crime*
- *List the categories of cyber crime*
- *Know types of online harassment*
- *Understand the cyber law in India*

4.1. Cyber Crime

Any crime that involves a computer and a network is called a "Computer Crime" or "Cyber Crime".

Categories of computer crime

1. The computer as target
   The Computer as a Target :-using a computer to attack other computers.
   e.g. Hacking, Virus/Worm attacks, DOS attack etc.

2. The computer as weapon
   The computer as a weapon :-using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

4.2.Online Harassment

Technological advancements have created new possibilities for criminal activity, such as

a. Unauthorized access & Hacking:-

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. By hacking web server taking control on another person's website called as web hijacking

b. Harassment through Email

- **Email spoofing**

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

- **Email bombing**
  E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.
- **Sending threatening emails**
- **Defamatory emails**
- **Email frauds**

c. Denial of Service attacks:-
Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

- **Preventive Measures For Cyber Crimes:**
  Prevention is always better than cure. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programs by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

4.4. Cyber law of India

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offences.

Penalties: Imprisonment up to 3 years and / or
Fine: Two lakh rupees.

- **http://www.cyberlawsindia.net/**

http://deity.gov.in/content/cyber-laws-security

Refrence:
Source: http://doug-johnson.squarespace.com/blue-skunk-blog/2012/11/27/top-10-guidelines-for-digital-citizenship.html)
http://www.pewinternet.org/2014/10/22/online-harassment/)

Lesson 5: The emergence of E-commerce

Objective: Students will be able to

- *Define e-commerce*
- *Recall Basic steps in an e-commerce transaction*
- *List various apps of e- commerce*
- *Know application of e-commerce*
- *Understand safety measures while doing e-commerce transaction*
- *Use the e-commerce knowledge in day today life*

5.1 What is e-commerce

E-commerce is 'electronic commerce': the transacting of business selling and buying online

●Basic steps in an e-commerce transaction

1. Customer enters credit card information on a secure page.
2. Payment information is stored on a merchant's server and passed through the processor.
3. Credit Card account is authorized to guarantee that a payment is available.
4. All transactions are settled to the bank at the end of the day.
5. Merchant receives payment for the transactions according to the payout agreement in their merchant contract. . Customer enters credit card information on a secure page.
6. Payment information is stored on a merchant's server and passed through the processor.
7. Credit Card account is authorized to guarantee that a payment is available.
8. All transactions are settled to the bank at the end of the day.
9. Merchant receives payment for the transactions according to the payout agreement in their merchant contract.

● E-commerce and Apps

Paytm, GoDaddy, Airtel Money, Mobile Recharge, Bill, Snapdeal,etc.

5.2 Applications of e-commerce

E-commerce businesses may employ some or all of the following:

Financial services

● Banking

Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.

- Online financial exchanges for currency exchanges or trading purposes.

Things you can do

- Download Credit Card Transactions.
- Download Banking Transactions.
- Transfer Money
- Quickly Verify Bank Balances.
- Online Bill Payment.
- Open and Close accounts
- Track recent account
- Check account balances

● Retail
- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Engaging in pretail for launching new products and services

● Convenience services (bill payment/ticket booking…etc)
- Paying Electricity bill
  1. Enter your 'Consumer Id' and click on Preview to view your latest bill/Bill history/Payment details.
  2. Verify Bill Detail.
  3. Click on Proceed to make payment to pay your bill online.
  4. Enter your Credit / Debit card details and make the payment.

● Leisure and entertainment
- Gathering and using demographic data through web contacts and social media

2.3 Safety in E-Commerce Transactions

- Modes of payment
  Shopping online using credit cards is becoming increasingly popular as it makes life way and due to the diversified options available. Be it an e-commerce transaction, booking tickets online or availing a service, online transactions has its intrinsic advantages of saving time and convenience. But there is also a fear of data associated with this, as a lot of third party websites and cookies are actively stealing user information silently leading to security risks

Taking some significant steps can minimize their risk of such fraudulent transactions. Let us take a look at the top 10 tips to ensure safe online card transactions:

1) Install Latest Security Software: Prevention is better than cure and the same is true for all online transactions. The World Wide Web is full of malware, spam and spyware and the best protection to avoid your security being compromised is to use good antivirus software.

2) Use Auto Update for all Software. Web browser companies release patches as updates regularly to cover any such security glitch in the software. If you find it hard to manually check and update their software, the best way is to keep the auto update option enabled for all software in your computer.
3) Look for Encryption Signs: Before entering any confidential information or sensitive data on any webpage, check if the website using proper encryption. Encryption is a security measure that helps protect data while travelling over the various networks on the internet. The basic sighs of encryption include an internet protocol or url address starting with https (where s stands or security) as well as a sign displayed a closed padlock located in the right corner of the screen.
4) Use Different Passwords: A recent study has revealed that majority of the people use common passwords for a number of transactions including sensitive transactions like net banking and credit cards for the convenience of recollecting. Using the same password makes you at high risk, as if hackers can somehow get access to one password, they would virtually have access to all your accounts. The best way to keep you safe in the virtual world is to use unique passwords for different transactions.
5) Cash on delivery option: If any sites are offering cash on delivery option, don't hesitate to use it as it is a good safety tip at no cost. Many sites give this option, but many of us ignore it mainly because of our carelessness in going through all details.
6) Dealing with Offers: You might be getting lot of promotional mails and coupons as mails from retail companies. But while utilizing such offers, it is recommended to go directly to the seller site rather than entering details in the coupon link, which will be usually sent by third parties.
7) Check Website's Digital Certificate: Before doing any transaction from online retailers and merchant websites, make sure to check for safe digital certificates that can authenticate the website. Independent services like VeriSign for example is a popular authentication service provider which helps users to make sure that the website they are dealing with is genuine and not some fraudulent imposter.
8) Avoid Using Public Computers: Always use personal computers or electronic gadgets like phones or tablets to complete any financial transaction over the internet. Never use any public computers or your friend's mobile for such sensitive transaction as their security may have been compromised. Also make sure you always connect to the internet using a secured Wi-Fi connection which is password protected. Doing financial transactions over a public Wi-Fi connection is highly unsafe and not recommended.
9) Stay Away from Phishing Emails Seeking Confidential Information: Any promotional mails from your bank or any third party websites or vendors

seeking your sensitive banking information must be ignored as spam. A lot of innocent people have been trapped by such phishing websites and emails in the past coming in the name of banks, RBI, IT department etc. Any mail seeking your banking information by offering lucrative lottery or content winnings must never be encouraged.

10) Buy From Reputed Merchants: Doing online transaction from reputed merchant websites and e-commerce platforms make sure your security is not compromised. A lot of small vendors may not have adequate security mechanisms in place that could lead to compromise of all user sensitive information in the future. Also check for a confirmations email once you complete any financial transaction to make sure the money you have paid has reached the merchant. Also do check the seller's privacy policy as some retail companies use to resell personal information like contact numbers with market research companies, which can cause leakage of secure data if not handled with care.

Lab Session

- Simulating or carrying out an e-transaction
  - Teachers show how to buy a online products using different online shopping app
  - How to pay bill online (electricity bills, Phone bills etc)
  - How to book a tickets (Railway, bus, air)

References:

https://www.google.co.in/#q=Safety+in+E-Commerce+Transactions

http://articles.economictimes.indiatimes.com/2014-03-05/news/47933708_1_transactions-software-firefox

References:

https://www.google.co.in/#q=Safety+in+E-Commerce+Transactions

http://articles.economictimes.indiatimes.com/2014-03-05/news/47933708_1_transactions-software-firefox

Lesson 6: Being Future Ready

Describe three ways in which e-commerce will impact the way we will study and work in the near future.This is an open ended exploratory question which needs to be in a discussion format. Allow students to imagine ways in which e-commerce will shape their future. Have them discuss how they will need to be ready for it. Link this discussion to the various guidelines – beginning with username password, all the way to the guidelines of being a good digital citizen and cyber laws.