Unit-7
Security and Ethical Consideration in ICT
Computer virus

A computer virus is a program or malicious software that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also duplicate themselves. After entering a computer, a virus attaches itself to another program. All computer viruses are man-made.

A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Some people distinguish between general viruses and *worms.* A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Virus Protection

Virus Protection is integral (essential)to internet security and security of a system or network. It is nothing but securing a system or network against viruses, worms, Trojans and all kinds of malware using different technologies. It offers(provides) a blend (balance) of technologies like antivirus, anti-spyware, firewalls etc.

Basic Measures of Virus Protection

- Use of Antivirus
- Use of Firewall
- Keep Your Anti-Virus Software Up to Date.
- Download only trusted programs
- Avoid pirated software
- Be cautious (careful) about Phishing and Social Engineering
- Be wise with Passwords
- **Be careful what you download**
- Be careful if you share files
- Shop safely online
- Think Before You Click
- Do not open an email attachment unless you were expecting it and know whom it's from
- Never open files with a double file extension, e.g. filename.txt.vbs. This is a typical sign of a virus program.
- . Do not open an email attachment unless you were expecting it and know whom it's from.
- Make sure that your Runbox virus filter is activated.

Cyber Security

Cyber security, computer security or IT security is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

Cyber security has never been simple. And because attacks evolve every day as attackers become more inventive, it is critical to properly define cyber security and identify what constitutes good cyber security.

Why is this so important? Because year over year, the worldwide spend for cyber security continues to grow: 71.1 billion in 2014 (7.9% over 2013), and 75 billion in 2015 (4.7% from 2014) and expected to reach 101 billion by 2018. Organizations are starting to understand that malware is a publicly available commodity that makes it easy for anyone to become a cyber attacker.

The term cyber security is used to refer to the security offered through on line services to protect your online information. With an increasing amount of people getting connected to internet, the security threats that cause massive harm are increasing also

'Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized'**Security"** is the quality or state of being secure--to be free from danger. But what are the types of security we have to be concern with?

Physical security - addresses the issues necessary to protect the physical items, objects or areas of an organization from unauthorized access and misuse.

Personal security - addresses the protection of the individual or group of individuals who are authorized to access the organization and its operations.

Operations security- protection of the details of a particular operation or series of activities.

Cybercrime/ Computer crime

Cybercrime is criminal activity done using computers and the Internet. This crime may be such as downloading illegal music files and stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offense, such as creating and **distributing viruses on other computers** or **posting confidential business (secret) information on the Internet**. Perhaps the most famous form of cybercrime is **identity theft**. In this type of crime criminals use the Internet to steal personal information from other users. Two other most common ways of doing cybercrimes are **phishing** and **pharming** . In them, the criminals **lure** users to fake (false) websites (that appear to be legitimate), where they are asked to enter personal information such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers. Then, criminals use the information to "steal" another person's identity. For this reason, it is good to always check the URL or Web address of a site to make sure it is legitimate before entering your personal information.

Classification of computer crimes

Abuses, misuses or crimes attached to computers take different and various forms. They are classified in several ways and according to more than one criterion. One such classification makes use of two categories: (1) crimes where a computer system itself is the target such as hacking, dissemination of viruses, and denial of service attacks; (2)traditional crimes like fraud, theft, and child pornography that are facilitated and enabled by a computer.

Types of computer crimes

There are many different ways of classifying computer crimes. But a typical way is activity- based classification According to this criteria these are four basic categories: theft, fraud, copyright infringement, and attacks.

Theft. Theft refers to either unauthorized removal of physical items **such as hardware or** unauthorized removal or copying of data or information**. It is well known that laptop computers are targeted at airports and restaurants. This is the example of the theft of physical items.** There are also other theft which are not physical. **For example,** any information contained in electronic form such as that stored in computer hard disks, etc. Another example of theft is **identity theft**. In it ,offenders (criminals) trick web users into disclosing social security numbers, bank account and credit card information, home addresses, and more. A common scheme is known as "email phishing."

Fraud.:It is any dishonest misrepresentation of fact which causes loss. It is dishonest trick. By means of such criminal trick, the fraud will get benefit such as:Credit card offers (offer credit cards) but they are offered only to capture personal information, to investor postings which promote a stock or investment offer to encourage investment which will benefit the person posting the information, to medical and pharmaceutical -related sites which purport to provide correct medical advice or sell altered medications.

Copyright infringement - The Internet has provided a good opportunity and environment for copyright violation. This type of computer crime includes use of software, music, books , etc. which is not appropriately bought (e.g Books). There is easy Software piracy by posting files for downloading all over the world. However, another more costly copyright infringement occurs when **trademarks and logos** of corporations are posted on non-authorized web sites. Some criminals utilize the trademarks and logos to appear to be a legitimate site to do fraud. Many corporations have employees or consulting contractors who constantly crawl the web to sniff out illegal usage of trademarks and logos.

Attacks on organizations and individuals: Attacks on organizational information systems may be either physical or logical. There are many types of cyber attacks. One very popular attack is Denial of Service Attacks (DoS) . It attacks specific web sites and servers. Some of the newsworthy examples of DoS during 2000 - 2001 have occurred at Microsoft.com, eBay.com, and Amazon.com. Web servers and connections can only handle so much traffic so Denial of Service (DoS) usually take the form of one of

two ways: – Coordinated attack (typically from unsuspecting desktops) to a particular IP address or URL requesting a page – overwhelms server and DoS occurs – Attack sends incomplete packets so that traffic gets jammed with requests for re-send.

Computer crime (detail description)

Hacking: It is gaining access illegally to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism) are committed.(**Unauthorized Access)**

Theft : Theft of any information contained in electronic form such as that stored in computer hard disks, removal storage media, etc. It Can extend to identity theft.

Identity Theft : Offenders trick online shoppers and other web users into disclosing social security numbers, bank account and credit card information, home addresses, and more. A common scheme is known as "email phishing." It is done by sending victims an email containing a link to a website that the victims use regularly. The email asks victims to update their account information on the website, but when victims click on the link within the email, they are taken to a **copycat website** that secretly captures the information they enter.

Denial of Service Attacks: In a denial of service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle. In a distributed denial of service attack, hundreds of computers (known as a zombies) are compromised, loaded with DOS attack software and then remotely activated by the hacker.

Email Spoofing : A spoofed email is one that appears to originate from one source but actually has been sent from another source.

Cyber/ Child Pornography: Child pornography crimes include both the transmission of media that exploits children, as well as solicitation to commit sexual crimes against minors. A number of sexual offenses are also committed using computers. The trafficking of child pornography is one example.

Cyber Defamation : This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about another on a website.

Intellectual Property(IP) Crimes: Software Piracy; Copyright Infringement; Trademarks Violations; Theft of Computer Source Code.

Virus/worm : Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Cyber-Terrorism : Cyber terrorism is a relatively new phenomenon. These crimes involve politically-motivated attacks to targets such as government websites or commercial networks. Such attacks are designed to be large in scale, and to produce fear and panic among the victim population. With financial markets now trading over the internet and so many other transactions taking place online, the danger of cyber terrorism has received a great deal of attention. However, actual instances of this type of crime are rare. Like conventional terrorism, `e-terrorism' is utilizes hacking to cause violence against persons or property, or at least cause enough harm to generate fear.

Phishing and **pharming** : Both of these methods **lure** users to fake websites (that appear to be legitimate), where they are asked to enter personal information. Phishing attacks are designed to steal a person's login and password. For instance, the phisher can access the victims' bank accounts or assume control of their social network. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions. The e-mails state that your information needs to be updated or validated and ask that you enter your username and password, after clicking a link included in the e-mail. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to you account.

Financial Crimes : Credit Card Frauds; Money Laundering

Online Gambling : Millions of websites, all hosted on servers abroad, offer online gambling.

Salami Attacks : It is an insignificant attack. These attacks are often used in committing financial crime and are based on the idea that an alteration, so insignificant, would go completely unnoticed in a single case. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount

of money (say 5 cents a month) from the account of every customer. This unauthorized debt is likely to go unnoticed by an account holder.

Take a test before opening e-mail attachment . Is the email from someone that you know?

ii. Have you received email from this sender before?

iii. Were you expecting email with an attachment from this sender?

Make your computer secure :

Prevention is better than cure. So, one of the best suggestions is to prevent your computer form unauthorized use (stop unauthorized users (also known as intruders) from accessing any part of your computer system.

3. Use strong password

For each computer and service you use (e-mail, chatting, online purchasing, for example) , you should have a strong password.

4. Protect your website

Stay informed and be in touch with security related news

5. Protect your personal computer

Use the latest version of a good anti-virus software package which allows updating from the internet. Do not give out identifying information such as name, home address, and school name or telephone number in a chat room. This is particularly useful for the children and women.

Introduction of Ethics

Ethics studies morals and values . It is a branch of philosophy that deals with what is considered to be right and wrong. Ethics regulates human behavior in doing something. By ethics we know whether someone is doing the right thing or wrong thing. In determining whether someone doing is true or not, ethic is more concerned to the acceptability by his social environment. In this sense, ethics are social centric. An individual cannot properly claim that his action is right ethically, unless their social environment consider it correct. It is concerned with human conduct, more specifically the behavior of individuals in society.

computer ethics(Ethics in using digital documents)

There are several applied ethics, such as environment ethics, media ethics, etc. Several applied ethics that related to computer science world is computer ethics, information ethics and cyber ethics.

Computer ethics is closely related to the use of computers by humans. There are two things in the computer ethics that can be observed, i.e. whether the computer is used to do the right thing or the computers are used correctly.

Computer ethics is a standard for computer use, such as the reproduction of software, invasion (attack) of privacy, and circulation of objectionable material. Computer ethics is also used to refer to professional ethics for computer professionals such as ethical codes of conduct that can be used as guidelines for an ethical case.

A general rule of computer ethics is respect. Here are some guidelines to follow when dealing with computers in your academic life:

I. Respect yourself

- Do not give out your passwords
- Don't say or do anything that could damage your reputation, even if you think it's impossible for someone to find it or know it was you
- Protect your identity
- Log out of portals
- Don't leave copies of your printed pages in a common printer

II. Respect others

- Don't harass or threaten anyone using a computer
- Don't abuse your access to resources like storage space

III. Respect academic integrity

- Cite any information copied from the Internet
- Ask permission to copy or modify software unless it is in the public domain .

The Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure considerat

ICT use and communication

Using technology in communicationhas become a necessity. It's now part of our lives. People communicate through emails, faxes, Mobile phones, texting services, video conferences, video chat rooms and social media channels. As time goes on, more emerging technologies will change the way we communicate and it will be up to us to embrace(hold) them or not. Let's look at the impact or **use of technology in communication** both to individuals and businesses.

The impact of technology in communication to a business:
Today, every business uses technology in its own way to reach the media and targeted consumers. , Businesses have also embraced technology by easing communication within companies and among investors and suppliers. **Below are a few uses of technology in communication to a business.**

EasyProduct Launch: During the past, companies and small business used to face a lot difficulty in informing their consumers about a new product. A company had to pay for expensive door to door marketing which could even take a lot of time to yield results. Nowadays, things have become simple, through email subscriptions, companies will have data for most consumers. So, if they introduce a new item or service, the company will draft one email with details about a new service or product and that message will be delivered to all consumers in a minute. A good example is '**.**'**MailChimp**'''. With their massive mail submission, all your clients will receive the same message in a minute via email.

Product or service surveys: Before the invention of the internet, it was so difficult to conduct a survey.Most companies would pay money to magazines and place survey forms and offer gifts to users who filled those surveys and mailed them back to the company. Taking a survey is very important to a business because that is how you will know what your clients want and know areas of improvement. Nowadays, a business can conduct a survey using **social networks**and provide users with incentives like ''gift cards''. This produces a quick response and saves the company's money and time.

Social interaction with consumers: With the recent invention of social networks like **facebook and twitter**, a business can create business pages then get followers for these pages. The process is so simple and free. For some business, they set a budget for building a fun base for their pages, so they use these pages to update and communicate with their followers. A good example is ''**Nordstrom**'' this is one of the largest fashion retail businesses in America. Nordstrom used its facebook page to update followers about new items and discounts. As of today, its facebook page has over **1,667,162 likes. See page facebook.com/Nordstrom**

Video Conferencing In the past, you had to wait for your boss to be in the meeting to start a presentation. New technology enables your boss to be in the business meeting while in a hotel in Hawaii preparing for a partnership or investors meeting. This has been made possible by the invention of video conferencing.

.

Use of digital networks''Phones and printers are all digitized, not like before when communication was hindered by telephone lines. During bad weather, most the lines would go off. Now with satellite and broadband transmissions, you can communicate with anyone at work or off work via their mobile phones. You can also send a file to a printer while you are at home and someone in the office gets the printout.

The impact of technology in communication to individuals.

Technology has changed the way we interact and communicate with other. With the increased use of social based networks, people can create new relationships and also discover old friends. With technology, parents can communicate and keep track of their children. So communication has become easier and cheaper. Below are a few uses of technology towards individuals.

Text messaging services: Keeping in touch with friends is very important, so text messaging services have solved this problem by creating mobile phone apps. This enables you to text your buddies on instant for free. A good example is **ebuddy**. The buddy chat service will allow you to chat with your close friends via text for free.

Social networking platforms: These social interaction networks have helped individuals discover old school friends and also get new friends based on interests and region. Before this technology, it would be next to impossible for you to find all your old friends and interact with them on an instant, share life and your past on instant. It would even be difficult to get new friends from other countries. But now that barrier has been removed by social networks like **facebook.com**

Parental security apps: Gone are the days when you had to lie your parents about your location. Now with GPS tracking mobile apps, your parent will install this GPS-enabled app, and they can see where you are. These apps, also have maps which indicate red zones, so you can tell if your child is in that area. When something wrong is detected, the App will notify the parent that their child might be in danger. See an example of such App. SecuraTrac

Free internet calls: Friends can call each other for free using free internet call centers. A good example is SKYPE. With Skype software installed on my laptop, I can communicate with my friends for free if they also have Skype on their laptops. This software can also be installed on smartphones. Get this software from Skype

Use of emails: Even though social networks are trying to replace email communication; there is certain information which users cannot exchange via social networks. So email services like yahoo mail, Hotmail, and Gmail have eased communication. It's now very rare to find a person writing a letter because that will involve posting it to a postal office and paying delivery fees, which is not the case when you use electronic mail.

In conclusion, technology has transformed the way we communicate; it has created a big impact in how businesses interact with consumers and how friends interact with each other.