Virtual University

INTRODUCTION TO CYBER SOCIETY ,CYBER CULTURE AND CYBER SPACE

Lesson # 1

Topics

- Main Objective
- Cyber Society
- Cyber Culture
- Cyber Culture Components
- Cyber Space Concept
- Cyber Space Communities
- The Cultures of Computing
- Effects of Cyber Culture on Society
- Outcomes

Main Objective

- Positive Online Environment of Internet users and a healthy cyber culture for the Internet community.
- A recognition of the power of the Internet to benefit oneself and the community at large .
- To **reflect** on how to become a responsible user of social networking sites and a commitment towards building a healthy cyber culture .

CYBER SOCIETY

Cyber Society

- **Cyber Society :**Focuses on the construction, maintenance and facilitation of community in electronic networks and computer-mediated communication.

CYBER CULTURE

Cyber Culture

Introduction:

- **World Wide web** is the collection of electronic documents.
- Each electronic document on the web is called a web page. Which can contain text, graphics, audio and video.
- The use of World Wide Web by a people or a group of people for the exchange of social expectations, custom, history and language is called cyber culture.

Cyber Culture

- Like every culture has its own language, the cyber culture is not the exception to this rule.
- It converts the human written language or symbols to machine language and reconverts to human understandable language so the people on the destination can understand.
- Now a day's specially in online chatting the cyber language is creates of new codes which affects our daily spoken language.

CYBER CULTURE COMPONENTS

Cyber Culture Components

- Internet
- Website
- E-Mail
- Blog
- Online Chat
- E-Commerce
- Social Networks

THE INTERNET

Cyber Culture Components

The Internet

- The network formed by the co-operative interconnection of a large number of computer networks.
- No one owns the Internet.
- There is no central administration to the internet.
- Main goal of the internet is to connect several computers together for the exchange of messages and share the information etc.
- Community of people.
- Collection of resources.

WEBSITE

Cyber Culture Components

Website

- A location connected to the Internet that maintains one or more web pages.
- Web pages are the building blocks of the website.
- Web pages includes documents like texts and multimedia contents etc.
- A web sites may be accessible through a public Internet Protocol (IP) network, such as the Internet, or a private local area network (LAN), by referencing a uniform resource locator (URL) that identifies the site.

E-MAIL

Cyber Culture Components

E-mail (Electronic Mail)

- **Electronic mail**, most commonly called **email.**
- E-mail is the Most widely used application on the internet.
- Messages that are sent electronically from one computer to another is an e-mail message.

BLOG

Cyber Culture Components

Blog:

- A **blog** is a discussion or informational site published on the World Wide Web consisting of discrete entries ("posts").
- A regularly updated website or web page, typically , runs by an individual or a small group.

ONLINE CHAT

Cyber Culture Components

Online Chat

- Any kind of communication over the **Internet** that offers a real-time transmission of text messages from sender to receiver is called online chat.

- Online chat may address point-to-point communications as well as multicast communications from one sender to many receivers

  and video chat, or may be a feature of a web conferencing service**.**

- Any direct text-based or video-based (webcams), one-on-one chat or one-to-many group chat by using tools such as instant messengers,

  Internet Relay Chat (IRC) etc**.**

E-COMMERCE

Cyber Culture Components

E-Commerce

- **Electronic commerce**, commonly written as **e-commerce**, is the trading or facilitation of trading in products or services using computer networks, such as the Internet.
- Commercial transactions conducted electronically on the Internet. E.g.
- Online shopping.
- Online market places.
- Business to business buying & selling.
- Online newsletter for marketing prospective.

SOCIAL NETWORKS

Cyber Culture Components

Social Networks

- A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images , videos are referred to as social networks. For example networks like
- Face book.
- Linked in.
- Twitter.

CYBER SPACE

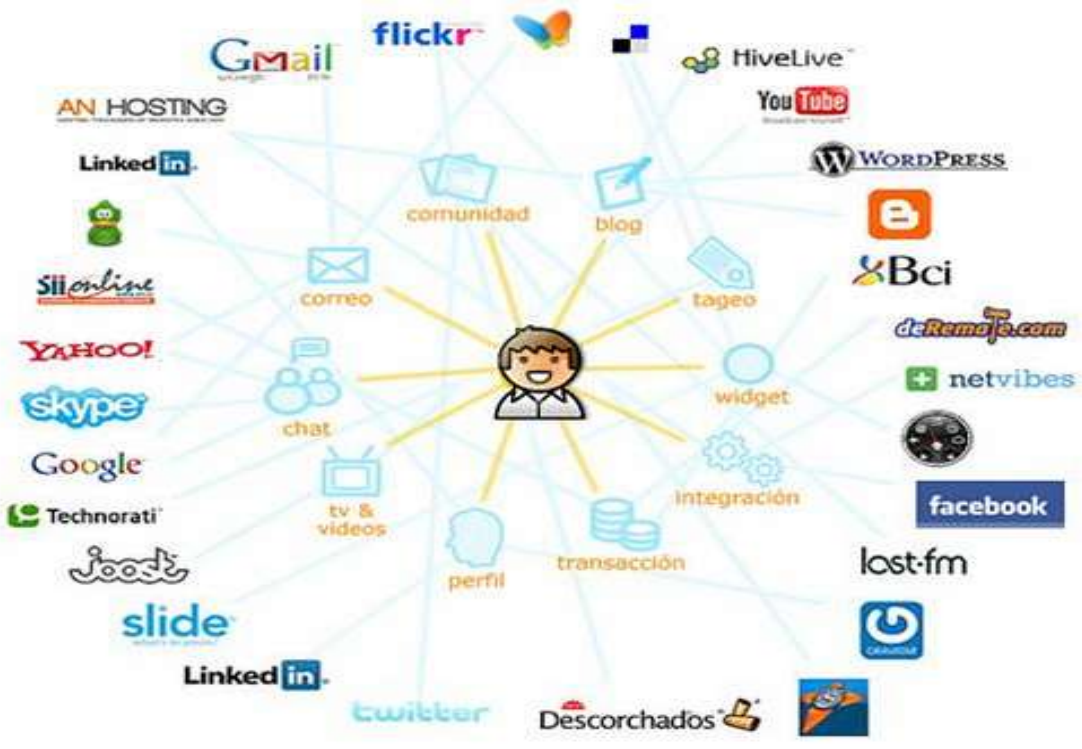
Concept of Cyber Space

- The cyberspace is a term used to describe the space created through the union of electronic communications networks such as the internet, which enables computer facilitated communication between any numbers of people who may geographically dispersed around the globe.
- Cyberspace is a public space where individuals can meet, exchange ideas, share information, provide social support, conduct business etc.

Concept of Cyber Space

The human interaction does not require physical connection to communicate, but is rather characterized by the interconnection of millions of people throughout the world through chat room, email, Facebook etc.

Concept of Cyber Space



Cyber Space Communities

- Due to worldwide use of computer network, people are now able to get together and form cyber communities that can exchange messages easily through cyberspace.
- Physically meeting has been reduced due to introduction of cyber culture.

The Culture of Computing

- Culture is an important process in computer related contexts. The processes that create meaning in actions.
- Cyber culture is indicated to break down borders and barriers, not only between nations but also between groups and individuals separated from each other due to some reasons.
- If cyber culture grows then those who are cut off from cyber culture will feel more isolated from society and will not be properly updates about latest development and fast change.

Effects of Cyber Culture on Society

Effects of Cyber Culture on Society

- The cyber culture has brought great impact on human individual's life.
- In education the style of teaching learning has changed. The student teacher interactivity can be formed online.
- The cyber culture has great influence in the business world.
- The use of internet for emails and other social networks is our participation in the cyber culture.

Effects of Cyber Culture on Society

- Cyber culture reduced the gap between groups and individuals separated from each other due to some reasons.
- Now days there are many social networking sites like Face book, MySpace and Twitter, which all serve to provide links to many friends to maintain their relationship.
- These social networks are means of interactivity between people around world.

Effects of Cyber Culture on Society

- Face to face communication is becoming weak due to emerging of these social networks.
- The People who don't have the ability to communicate face to face they can exchange their views, through these social network.
- Business decision can be made through video conferences.

Out Come

- The cyber culture is developing and we need to know the values and believes of this culture.
- Cyber culture has great influence on human culture and in way new uniform global culture is developing.

References

- https://en.wikipedia.org/wiki/Cyberculture
- https://sites.google.com/site/inhainternetlanguage/random/what-is-cyberculture
- http://sociologyindex.com/cyberculture.htm
- http://www.slideshare.net/wowox/cyberculture-27445734

THANK YOU

FUNDAMENTALS OF E- COMMERCE

Lesson # 2

Overview of the Lesson

- Main Objective
- Basic of E-Commerce.
- Types of E-Commerce.
- Process of E-Commerce
- Advantages of E-Commerce
- Disadvantages of E-Commerce
- E-Shopping Safety Tips
- Outcomes

Main Objective

- Basic knowledge about E- Commerce environment.
- Identify the main business and market place models for electronic communication and trading.
- Understanding of different transactions mechanisms available through online services.

E-COMMERCE

E-Commerce Basics

- Process of buying, selling or exchanging products, services and information through computer networks.
- It refers to the use of the Internet and the Web to manage business between and among organizations and individuals.

Domains of E –commerce

1. Physical Domain
2. Digital Domain

E-Commerce Basics

Traditional E- Commerce

- All the dimensions are physical in nature
- Perform all business transactions off-line.
- Buy and sell products through physical agents and representatives.

Pure E- commerce

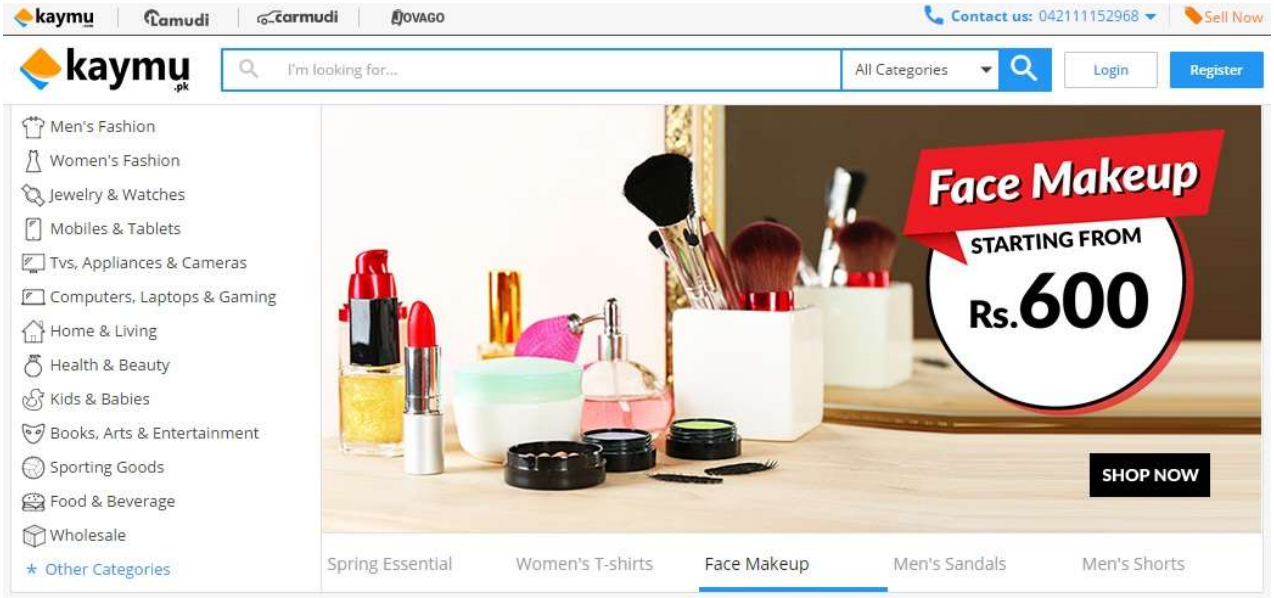
- All the dimensions are digital in nature.
- Pure online (virtual) organizations.
- Buy and sell products online.

E-Commerce Basics

Hybrid Approach

- A combination of physical and digital dimensions
- Primary business carried out in the physical world.
- Provide some services on line.

E- Commerce Example



E-COMMERCE TYPES

Types of E-Commerce Models

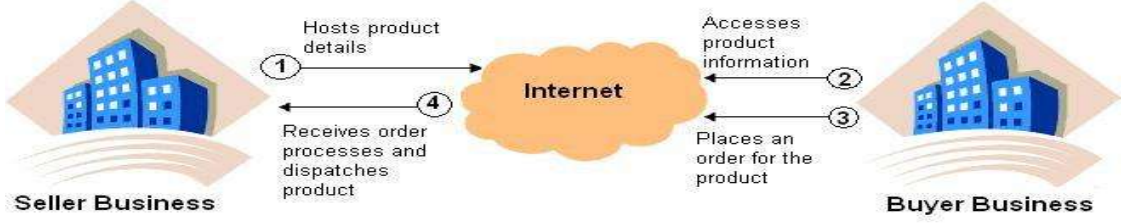
Four Major Domain on which E-Commerce Works

- **Business-to-Business (B2B) Model**
- **Business-to-Consumer (B2C) Model**
- **Consumer –to-Business (C2B) Model**
- **Consumer-to-Consumer (C2C) Model**

Business-to-Business (B2B) Model

B2B Model describes commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.

Example: Dell deals computers and other associated accessories online but it does not manufacture all those products. So, in govern to deal those products, first step is to purchases them from unlike businesses i.e. the producers of those products.

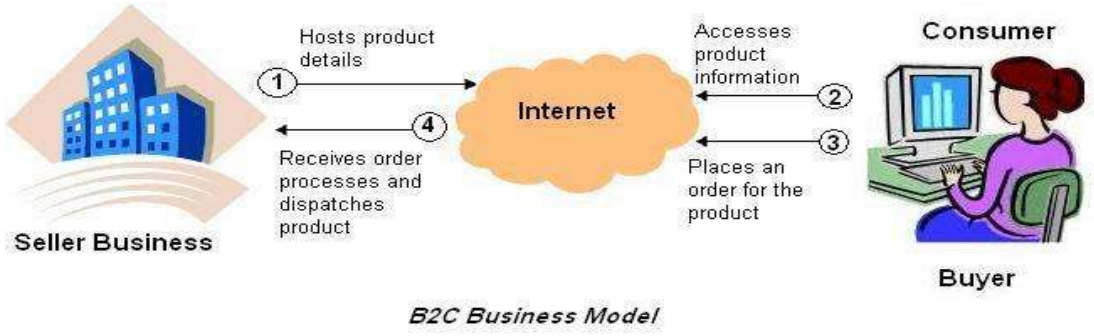


B2B Business Model

Business-to-Consumer (B2C) Model

The B2C model involves transactions between business organizations and consumers. It applies to any business organization that sells its products or services to consumers over the Internet. These sites display product information in an online catalog and store it in a database. The B2C model also includes services online banking, travel services, and health information.

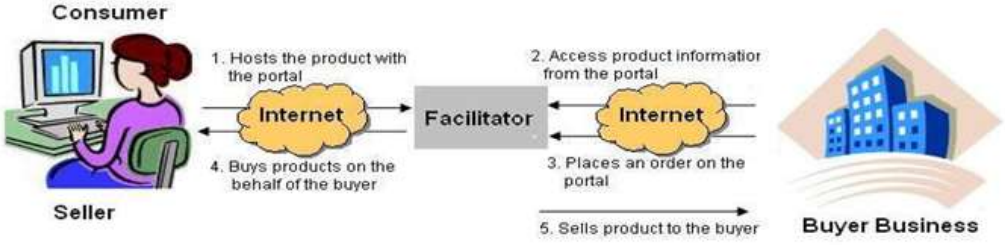
Example: www.daraz.pk, www.amazon.com etc….



B2C Business Model

Consumer-to-Business (C2B) Model

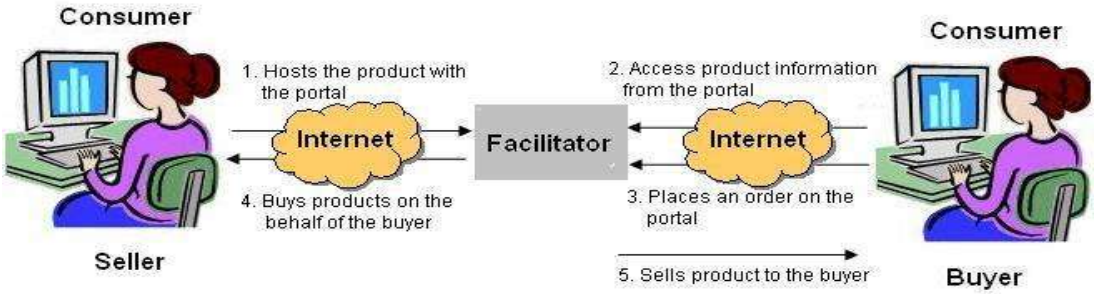
- A C2B model, is a type of commerce where a consumer or end user provides a product or service to an organization.
- An example is Priceline.com, where the customer names a product and the desired price, and Priceline tries to find a supplier to fulfill the stated need



Consumer-to-Consumer (C2C) Model

The C2C model involves transaction between consumers. Here, a consumer sells directly to another consumer.

eBay.com, olx.com, etc… are common examples of online auction web sites that provide a consumer to advertise and sell their products online to another consumer.



C2C Business Model

PROCESS OF E-COMMERCE

Process of E-commerce

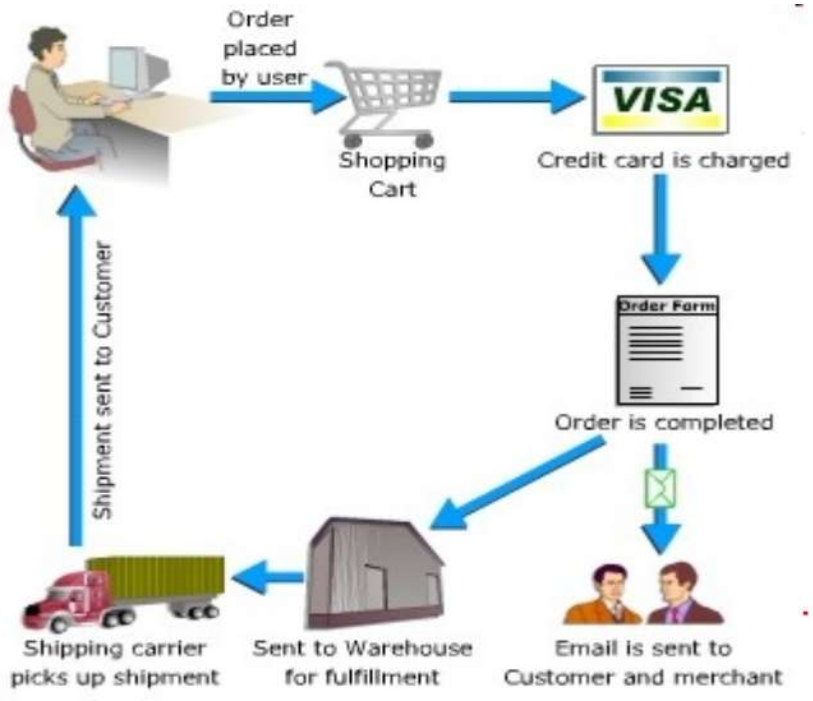
- A consumer uses Web browser to connect to the home page of a merchant's Web site on the Internet.
- The consumer browses the catalog of products featured on the site and selects items to purchase.
- The selected items are placed in the electronic equivalent of a shopping cart.
- When the consumer is ready to complete the purchase of selected items, He/she provides a bill-to and ship-to address for purchase and delivery .

Process of E-commerce

- When the payment method is identified and the order is completed at the Commerce Server site, the merchant's site displays a receipt confirming the customer's purchase.
- The Commerce Server site then forwards the order to a Processing Network for payment processing and fulfilment.

These are some common steps of online transactions.

Process of E-commerce



ADVANTAGES AND DISADVANTAGES OF E-COMMERCE

Advantages of E- Commerce

- Faster buying/selling procedure, as well as easy to find products.
- Buying/selling 24/7.
- You can shop anywhere in the world.
- Low operational costs and better quality of services.
- No need of physical company set-ups.
- Easy to start and manage a business.
- Customers can easily select products from different providers without moving around physically.
- Communication improvement.

Disadvantages of E- Commerce

- Unable to examine products personally.
- Not everyone is connected to the Internet.
- There is the possibility of credit card number theft.
- Mechanical failures can cause unpredictable effects on the total processes.

E-Shopping Safety Tips

E-Shopping Safety Tips

- **Check out sellers**: Conduct independent research before you buy from a seller you have never done business with. Some attackers try to trick you by creating malicious websites that appear real, so you should verify the site before supplying any information.

- **Make sure the site is genuine**: Before you enter your personal and financial information to make an online transaction, look for signs that the site is secure.

E-Shopping Safety Tips

- **Protect your personal information**: Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.

- **Turn your computer off when you're finished shopping**: Many people leave their computers running and connected to the Internet all day and night. This gives scammers 24/7 access to your computer to install malware and commit cyber-crimes.

Outcomes

Have the concepts and processes that comprise the technical infrastructure of e-commerce sites and be able to solve problems about online transactions.

References

- http://www.slideshare.net/siddhesh130995/e-commerce-31086645?qid=71930f23-5bfd-4e6a-b9e0-910bfa64cac3&v=&b=&from_search=2
- http://www.slideshare.net/munishsingla71/e-commerce-ppt-10713485?qid=689adfcf-df44-45d5-a4d2-663b93e2d9ae&v=&b=&from_search=6
- http://www.slideshare.net/jsm268/e-commerce-3717853?qid=695c2245-7ed4-4a9c-aadc-1b753036a56e&v=&b=&from_search=7
- http://www.slideshare.net/m8817/security-in-ecommerce?qid=695c2245-7ed4-4a9c-aadc-1b753036a56e&v=&b=&from_search=10
- http://www.slideshare.net/Tylerjd/e-commerce-presentation?qid=e4e4876e-c158-4f8d-8390-72a305bf1826&v=&b=&from_search=21
- https://www.youtube.com/watch?v=FAyit_s9eY0
- https://www.youtube.com/watch?v=xKJjyn8DaAw&nohtml5=False

THANK YOU

Virtual University

INTRODUCTION TO CYBER CRIMES

Overview of the Lesson

- Main Objective
- Introduction to Cyber Crime
- Categories Of Cyber Crime
- Types of Cyber Crimes
- Safety Tips
- Outcomes

Main Objective

- To explore about cybercrime.
- To create basic awareness about cyber crime .
- To gain more knowledge about cyber crime.
- Understanding of the risks of harmful online behavior.

CYBER CRIMES

Introduction to Cyber Crime

Cyber Crime:

- Computer crime or cybercrime, refers to any crime that involves a computer , Mobile and a network.
- Computer may be used as a weapon for crime or as a target.

The Computer as a Target : Using a computer to attack other computers.

The computer as a weapon: Using a computer to commit real world crimes.

Cyber Criminals:

- Those who are doing crimes by using the computer as a target or an object.

What is Cyber Crime? Simple Theory

- When you purchase a home it comes with a door and a lock. You always ensure that the door/lock exist and working properly. You may even purchase security systems.
- Likewise, Your Computer System is your home and security tools are your door/lock .
- So if someone breaches into your computer System, accesses all your personal accounts and tampers your data, is the criminal who is committing the crime.
- And committed crime is known as cyber-crime.

CATEGORIES OF CYBER CRIME

Categories Of Cyber Crime

Cyber Crime Against Individual

- This type of cyber crime can be in the form of hacking, identity theft, cyber bullying, cyber stalking etc.

Cyber Crime Against Property

- Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing.
  - In this case, they can steal a person's bank details and misuse the credit card to make purchases online.

Categories Of Cyber Crime

Cyber Crime Against Government

- Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism.
  - In this category, criminals hack government websites, military websites or circulate propaganda.

TYPES OF CYBER CRIMES

Types of Cyber Crimes

There are numerous types. Some of which are:

- **Hacking:** Hacking in simple terms means illegal access into a computer system without the permission of the computer owner/user.
- **Software Piracy:** This crime occurs when a person violates copyrights and unauthorized copying of software.
- **Cyber Stalking:** The crime in which the attacker harasses or threaten a victim using electronic communication, such as e-mail, instant messaging (IM), or messages posted to a Web site or on social networking sites.

Types of Cyber Crimes

- **Malicious Software:** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software and hardware. (virus, worms, Trojan Horse, web jacking, e-mail bombing etc.)
- **Identity Theft:** A criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information.
- **Cyber Bullying:** Cyber bullying is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner. This could be done via, text messages or images, personal remarks posted online, hate speeches and posting false statements in order to humiliate or embarrass another person.

Types of Cyber Crimes

- **Denial-of-service attack:** This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.

- **E-mail Spamming & Spoofing**: Email spoofing refers to email that appears to have been originated from one source and it was actually sent from another source. Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

- **Computer Vandalism**: Damaging or destroying data rather than stealing or misusing them is called cyber vandalism. These are program that attach themselves to a file and then circulate.

SAFETY TIPS

Safety Tips

- Use antivirus software's .
- Insert firewalls .
- uninstall unnecessary software .
- Maintain backup .
- Never send your credit card number to any site that is not secured.
- Avoid sending any photograph online particularly to strangers.
- Do not open mails from strangers. This prevents your system from unwanted attacks.

Safety Tips

- Don't respond to harassing or negative messages.
- Learn more about Internet privacy.
- Keep your operating system up to date.
- Change passwords frequently and Use hard-to-guess passwords.
- Don't share access to your computers with strangers .
- If you have a Wi-Fi network, password protect it.
- Disconnect from the Internet when not in use.

Outcomes

As internet technology advances so does the threat of cyber crime. In times likes these we must protect ourselves from cyber crime. Antivirus software, firewalls and security patches are just the beginning. Never open suspicious emails and only navigate to trusted sites.

References

- http://www.slideshare.net/tusharmalhot/cyber-crime-12320892?qid=769158d0-e1e2-47aa-bc34-c8d9fa89d727&v=&b=&from_search=13
- http://www.slideshare.net/aritraranjan/cyber-crime-32802194?qid=769158d0-e1e2-47aa-bc34-c8d9fa89d727&v=&b=&from_search=17
- http://www.slideshare.net/Binupjayan/cyber-crime-technology?qid=769158d0-e1e2-47aa-bc34-c8d9fa89d727&v=&b=&from_search=21
- http://www.slideshare.net/rajurmr22/cyber-crime-29238299?qid=769158d0-e1e2-47aa-bc34-c8d9fa89d727&v=&b=&from_search=20
- http://www.slideshare.net/soreingam/cyber-crime-28351567?qid=769158d0-e1e2-47aa-bc34-c8d9fa89d727&v=&b=&from_search=22

Virtual University

CYBER SECURITY

Topics

- Main Objective
- What is cyber security
- Need of Cyber Security
- Major Security Problems and Solutions
- Security Measures
- Advantages of cyber security
- Outcomes

Main Objective

- The objective is to educate and create awareness amongst the students community on use of technology, internet media and its implication on possible cyber crimes.

- Some of the possible prevention measures . One can take to avoid getting victimized for a cyber crime.

CYBER SECURITY

What is Cyber Security

- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access and attacks delivered through the Internet by cyber criminals.

- Protecting computer system and information from unauthorized access or destruction / abuse.

What is Cyber Security

Security deal with three primary issues, called the CIA triad.

1. **Confidentiality** :Assurance that only authorized user may access a resource.
2. **Integrity**: Assurance that resources has not been modified.
3. **Availability** : Assurance that authorized user may access a resource when requested.

Need of Cyber Security

- Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
- Security measures provides full security services to balance the needs of providing information to those who need it with taking action to mitigate the dynamic threats posed by cyber thieves and cyber terrorists.

Need of Cyber Security

Home Computer Security

- Your home computer is the popular target for intruders.
- They look for credit card numbers, bank account information.
- Use your computers to attack other computers on the internet.

Why Intruder attack home computers?

- Not very secure
- Easy to break into

How do they attack your computers?

- They send you E- mail with a virus
- They often install new programs that let them continue to use your computer (Back door).
- Trojan horses are such programs which are used as the back doors.

SECURITY PROBLEMS AND SOLUTIONS

Major Security Problems and Solutions

- **Virus and Worms**
- **Hacker**
- **Malware**
- **Trojan Horses**
- **Password Cracking**

Major Security Problems and Solutions

Virus and Worms:

- A Virus is a “program” that is loaded onto your computer without your knowledge and runs against your wishes.

Virus can reach to your computer in may ways

- CD- Rom
- E-mails
- Websites
- Downloaded Files

Check each of the above for viruses before using it.

Major Security Problems and Solutions

Solution:

- Install a security suite that protects the computer against threats such as viruses and worms.
- Handle E- mail attachments carefully.

Major Security Problems and Solutions

Hackers:

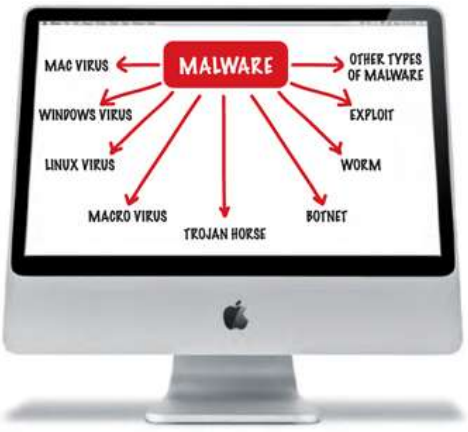
- A person who secretly gets access to a computer system in order to get information, cause damage, etc.
- Hackers attack where they see weakness. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.

Solution:

- It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.
- Regularly update your operating system
- Install Anti virus software's.

Major Security Problems and Solutions

Malware:



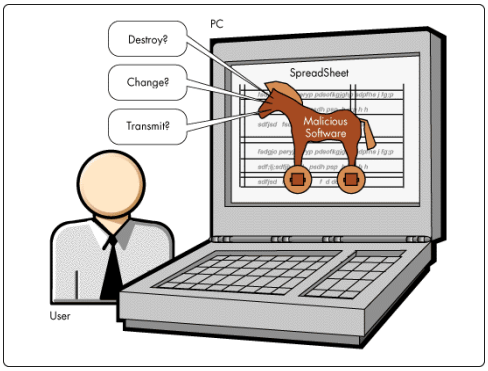
- The word "malware" comes from the term "Malicious software."
- Malware is any software that infects and damages a computer system without the owner's knowledge or permission.

Solution:

- Download an anti-malware program that also helps prevent infections.
- Activate Network Threat Protection, Firewall, Antivirus.

Major Security Problems and Solutions

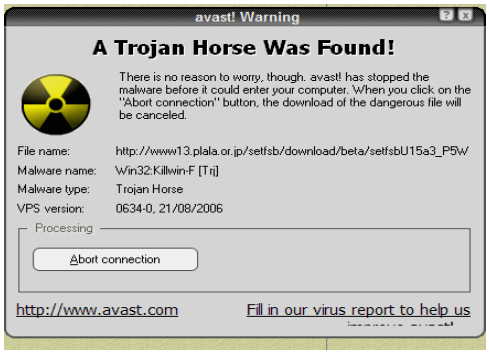
Trojan Horse:



- Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
- These viruses are the most serious threats to computers

Solution:

- Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.



Major Security Problems and Solutions

Password Cracking:

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

Solution:

- Use always Strong password.
- Never use same password for two different sites.

SECURITY MEASURES

Things to do for Protecting your Computer

- Use security software.
- Maintain current software and updates.
- Never share passwords .
- Do not click random links.
- Do not download unfamiliar software off the Internet.
- Log out or lock your computer.
- Remove unnecessary programs or services.
- Frequently back up important documents and files.

ADVANTAGES OF CYBER SECURITY

Advantages of Cyber Security

1. Protects system against viruses, worms, spyware and other unwanted programs.
2. Protection against data from theft.
3. Protects the computer from being hacked.
4. Minimizes computer freezing and crashes.
5. Gives privacy to users.

Outcomes

Improve the knowledge about cyber security and to overcome several security loopholes , Also it helps to spread awareness among normal people about emerging security threats. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.

CRYPTOGRAPHY

Lesson # 5

Introduction of Cryptography

- The method of hiding plaintext in such a way as to hide its substance is called encryption.
- Encrypting plaintext results in unreadable gibberish called cipher text

Origin

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

Caesar's Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

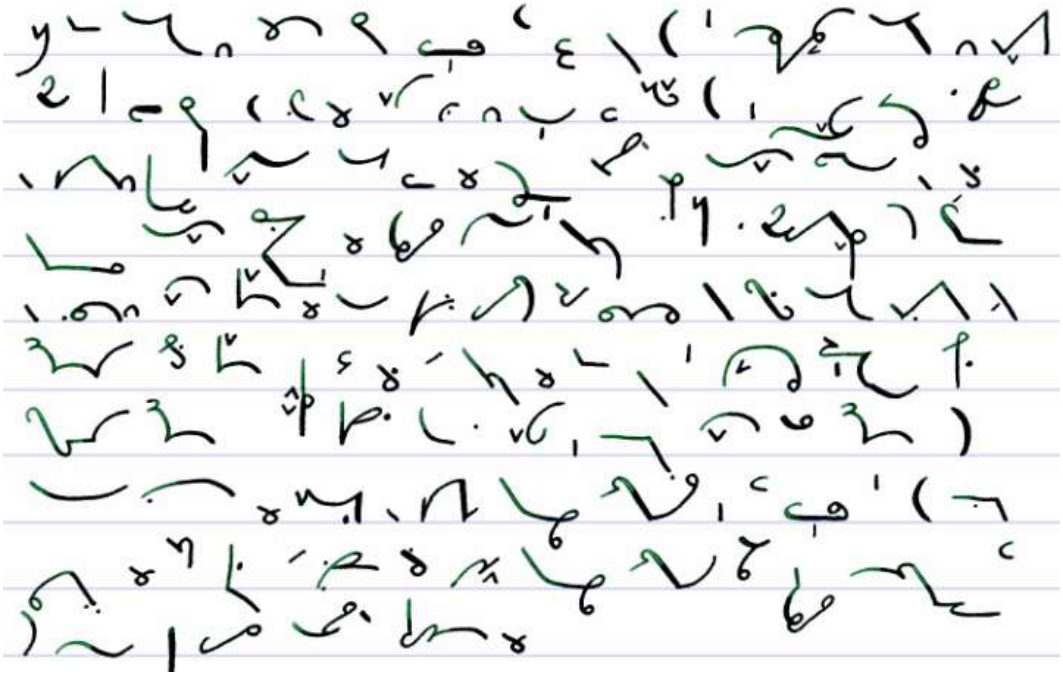
and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

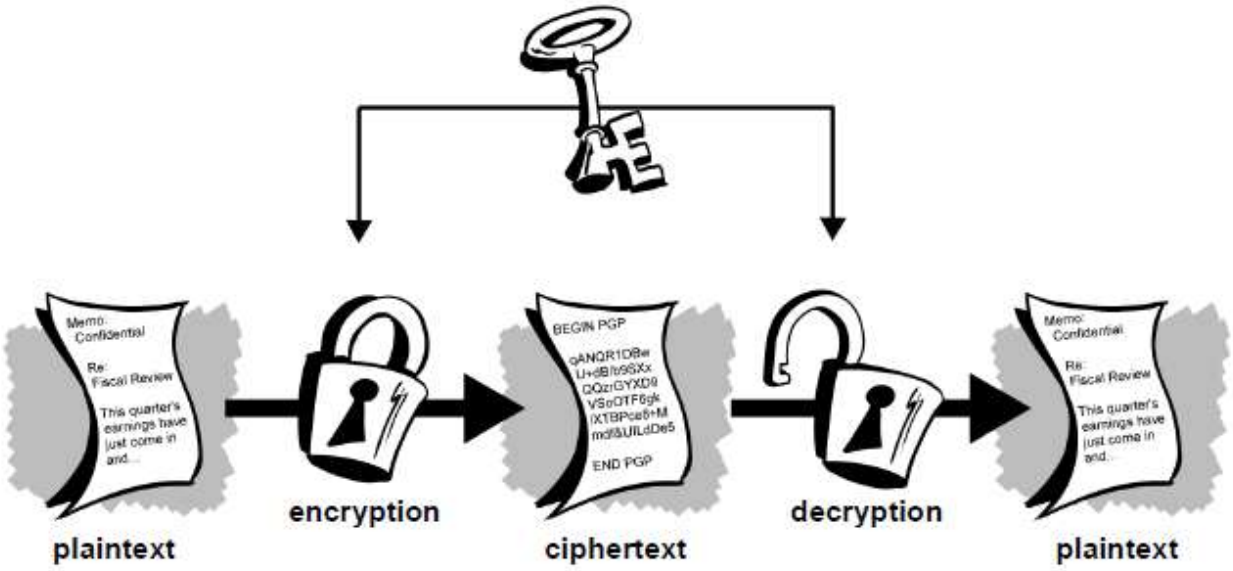
"SECRET" encrypts as "VHFUHW

Examples



CONVENTIONAL CRYPTOGRAPHY

Conventional cryptography



Conventional cryptography

- It is very fast. It is especially useful for encrypting data that is not going anywhere.

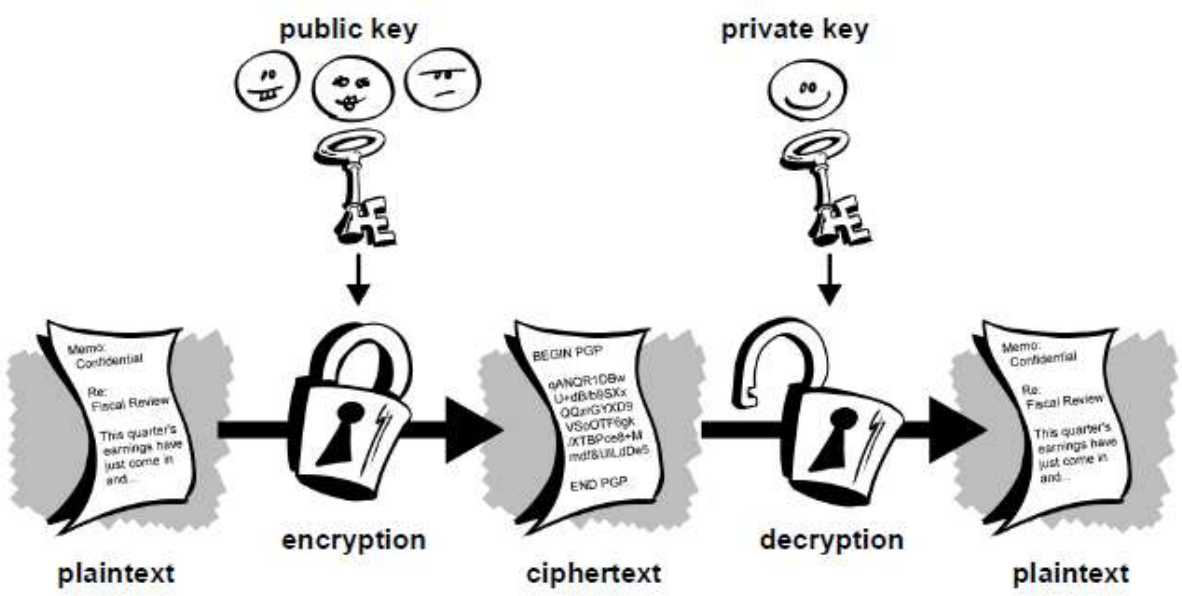
BUT

Key Management

- Both ends must agree upon a key and keep it secret between themselves.
- Being on different physical locations, they must trust a courier (secure communication medium) to prevent the disclosure of the secret key.
- Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key

PUBLIC KEY CRYPTOGRAPHY

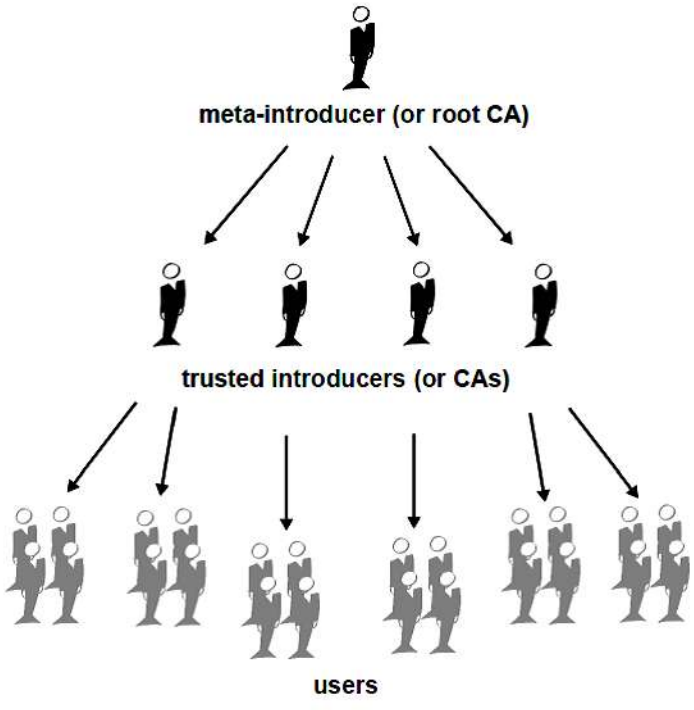
Public key cryptography



Certificate Management and Distribution

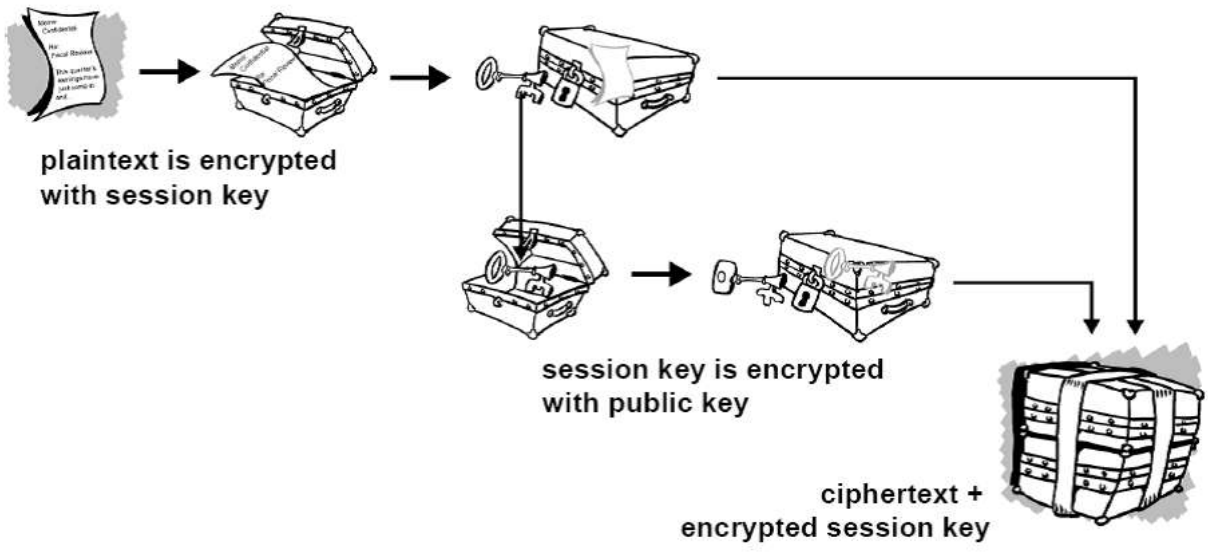
- Public Key Infrastructures
- Certification Authority, or CA
  - CA is authorized to issue certificates to its computer users. (ACA's role is analogous to a country's government's Passport Office.)

Certificate Management and Distribution

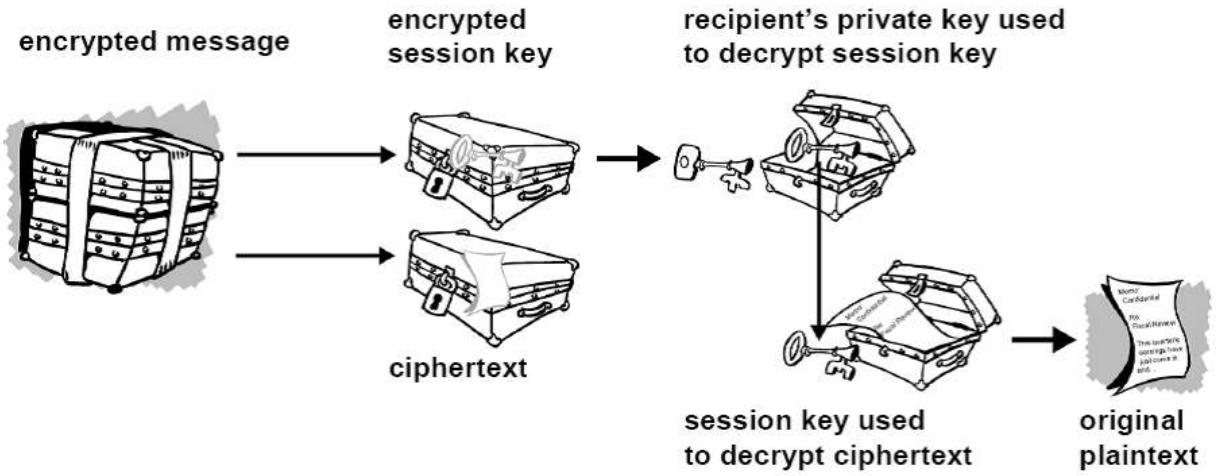


HYBRID APPROACH

Hybrid Approach



Hybrid Approach



Virtual University

Introduction to Cyber Law

Lesson # 6

Definition

The term “Cyber Law” Refers to all the legal and regulatory aspects of the Internet and its users

NEED OF CYBER LAW

Need of Cyber Law

Cyber Murder

A hacker changed the value of insulin in a patient's online prescription who was admitted in a hospital the nurse injected that quantity and patient expired.

Need of Cyber Law

- E-commerce penetrates into every corner of the modern business
- Regulatory Issues
- Emails
- Social Media
- Video Streaming

Need of Cyber Law

- Email spoofing
- Financial crimes
- Online gambling
- Sale of illegal articles
- Forgery
- Cyber Defamation
- Cyber stalking

Need of Cyber Law

- Denial of Service attack
- Trojan attacks
- Worms and Viruses
- Data diddling
- Intellectual Property crimes
- Cyber Disputes
- Unauthorized access to computer systems
- Salami attacks

THE ROLE OF LAW AND LAWYERS

The role of law and lawyers

The 1st rule of management is delegation. Don't try and do everything yourself because you can't.

The role of law and lawyers

- Consultancy
- The Subject matter Expert
- A blend of Law and Technology

CYBER REGULATION'S EVOLUTION

Cyber Regulation's Evolution

- UNCITRAL 1966
- Model Law on
  - E-Commerce 1996
  - E-Signatures 1996
- Wipo Copy Rights Rules 1996
- Wipo Performance and Phonograms Treaty Rules 1996

Cyber Regulation's Evolution

- ICANN Uniform Domain Name Disputes Resolution Policy 1998
- DMCA 1998
- EUCD 2001
- ITA 2000

Cyber Regulations in Pakistan

- The Electronic Transaction Ordinance 2002
- Prevention of Electronic Crime Ordinance 2008

CYBER LAWS IN PAKISTAN

Lesson # 7

Cyber Laws in Pakistan

- There are different laws, promulgated in Pakistan.
- These laws not only deal with crime of Internet
- These deal with all dimensions related to computer & networks.
- Two of them are most known.
- They are:
  - Electronic Transaction Ordinance 2002
  - Electronic / Cyber Crime Bill 2007

Electronic Transaction Ordinance 2002

Electronic Transaction Ordinance 2002

Overview

- The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers.
- Protection for Pakistani e-Commerce locally and globally.
- Protect Pakistan's critical infrastructure
- It is heavily taken from foreign law related to cyber crime.

Pre-ETO 2002

- No recognition of electronic documentation
- No recognition of electronic records
- No recognition of evidential basis of documents/records
- Failure to authenticate or identify digital or electronic signatures or forms of authentication
- No online transaction system on legal basis.
- Electronic Data & Forensic Evidence not covered.
- No Rules for all of these …

POST ETO 2002

Post ETO 2002

- Electronic Documentation & Records recognized
- Electronic & Digital forms of authentication & identification
- Messages through email, fax, mobile phones, Plastic Cards, Online recognized.

ETO 2002

Sections

- There are 43 sections in this ordinance
- It deals with following 8 main areas relating to e-Commerce.
  - Recognition of Electronic Documents
  - Electronic Communications
  - Web Site
  - Digital Signatures Certification Providers
  - Stamp Duty
  - Attestation, certified copies
  - Jurisdiction
  - Offences

VIOLATION OF PRIVACY INFORMATION

36. Violation of privacy information

- Gains or attempts to gain access
- To any information system with or without any purpose
- To acquire the information unauthorized
- Imprisonment 7 years
- Fine Rs. 1 million

DAMAGE TO INFORMATION SYSTEM

37. Damage to information system

- Alter, modify, delete, remove, generate, transmit or store information
- Create hindrance in information access
- knowingly when not authorized to do so
- Imprisonment 7 years
- Fine Rs. 1 million

OFFENCES TO BE NON-BAIL ABLE

38. Offences to be non-bail able

- All offences under this Ordinance shall be non-bail able, compoundable and cognizable.

PROSECUTION AND TRAIL OF OFFENCES

39. Prosecution and trail of offences

- No Court inferior to the Court of Sessions shall try any offence under this Ordinance.

Electronic/Cyber Crime Bill 2007

Overview

- “Prevention of Electronic Crimes Ordinance, 2007” is in force now
- It was promulgated by the President of Pakistan on the 31st December 2007
- The bill deals with the electronic crimes included:
  - Cyber terrorism
  - Data damage
  - Electronic fraud
  - Electronic forgery
  - Unauthorized access to code
  - Cyber stalking
  - Cyber Spamming/spoofing

Electronic/Cyber Crime Bill 2007

- It will apply to every person who commits an offence, irrespective of his nationality or citizenship.
- It gives exclusive powers to the Federal Investigation Agency (FIA) to investigate and charge cases against such crimes.

Electronic/Cyber Crime Bill 2007

Punishments

- Every respective offence under this law has its distinctive punishment which can be imprisonment or/and fine.

Sections

Data Damage:

- Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.

Punishment:

- 3 years
- 3 Lac

Electronic/Cyber Crime Bill 2007

Electronic fraud:

- People for illegal gain get in the way or use any data, electronic system or device or with intent to deceive any person, which act or omissions is likely to cause damage or harm.

Punishment:

- 7 years
- 7 Lac

Electronic/Cyber Crime Bill 2007

Electronic Forgery:

- Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic

Punishment:

- 7years
- 7 Lac

Electronic/Cyber Crime Bill 2007

Malicious code:

- Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or device, with intent to cause harm to any electronic system or resulting in the theft or loss of data commits the offence of malicious code.

Punishment:

- 5 years
- 5 Lac

Electronic/Cyber Crime Bill 2007

Cyber stalking:

- Whoever with intent to harass any person uses computer, computer network, internet, or any other similar means of communication to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image.
- Threaten any illegal or immoral act
- Take or distribute pictures or photographs of any person without his knowledge
- Commits the offence of cyber stalking.

Punishment:

- 3 Years
- 3 Lac

Electronic/Cyber Crime Bill 2007

Spamming:

- Illegal electronic messages to any person without the permission of the recipient.

Punishment:

- 6 month
- 50,000

Electronic/Cyber Crime Bill 2007

Spoofing:

- Whoever establishes a website, or sends an electronic message with a fake source intended to be believed by the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information

Punishment:

- 3 Years
- 3 Lac

Offence	Imprisonment (years)	Fine
Criminal Access	3	3 Lac
Criminal Data Access	3	3 Lac
Data Damage	3	3 Lac
System Damage	3	3 Lac
Electronic Fraud	7	7 Lac
Electronic Forgery	7	7 Lac
Misuse of Device	3	3 Lac
Unauthorized access to code	3	3 Lac
Malicious code	5	5 Lac
Defamation	5	5 Lac
Cyber stalking	3	3 Lac
Cyber Spamming	6 months	50,000
Spoofing	3	3 Lac
Pornography	10	-----
Cyber terrorism	Life	10 Million

CRITICISM

Criticism

- There are seemingly 21 ‘cyber’ issues covered in this Bill
- It may seem to cover all aspects of the new digital era.
- But detailed look shows quite the contrary.
- Practically in all issues the government has gone the extra mile to reinvent a new definition, significantly deviating from the internationally accepted norms.

Criticism

- There seems to be an elaborate play of words within the document
- allow room for the regulating body (FIA) to confuse and entrap the innocent people
- The FIA, has been given complete and unrestricted control to arrest and confiscate material as they feel necessary
- A very dangerous supposition
- Safeguards and Protection

Criticism

- **One example of the hideous nature of the bill:**
  - The Government has literally attempted to insert a new word in the English language.
  - The word TERRORISTIC is without doubt a figment of their imagination vocabulary
  - Hence they attempt to define the word, quite literally compounding the problem at hand
  - They have actually defined what real-life terrorism might be
  - But fail to explain what they mean by the word Cyber in cyber terrorism.
  - the concern is that there happens to be no clear-cut explanation on how a Cyber Terrorism crime is committed.

Why we must know Cyber Laws?

- Which specific laws apply to Organization.
- By law, which information assets need to be protected?
- Organizational Policies and Rules

Virtual University

CONCEPT OF CYBER SPACE JURISDICTION AND OTHER PRINCIPAL OF JURISDICTION

LESSON # 8

JURISDICTION

JURISDICTION

The right, power, or authority to administer justice by hearing and determining controversies.

- Territorial Jurisdiction
- Extra Territorial Jurisdiction
- Cyber Jurisdiction

TERRITORIAL JURISDICTION

TERRITORIAL JURISDICTION

Refers to jurisdiction over cases arising in or involving persons residing within a defined territory.

EXTRA TERRITORIAL JURISDICTION

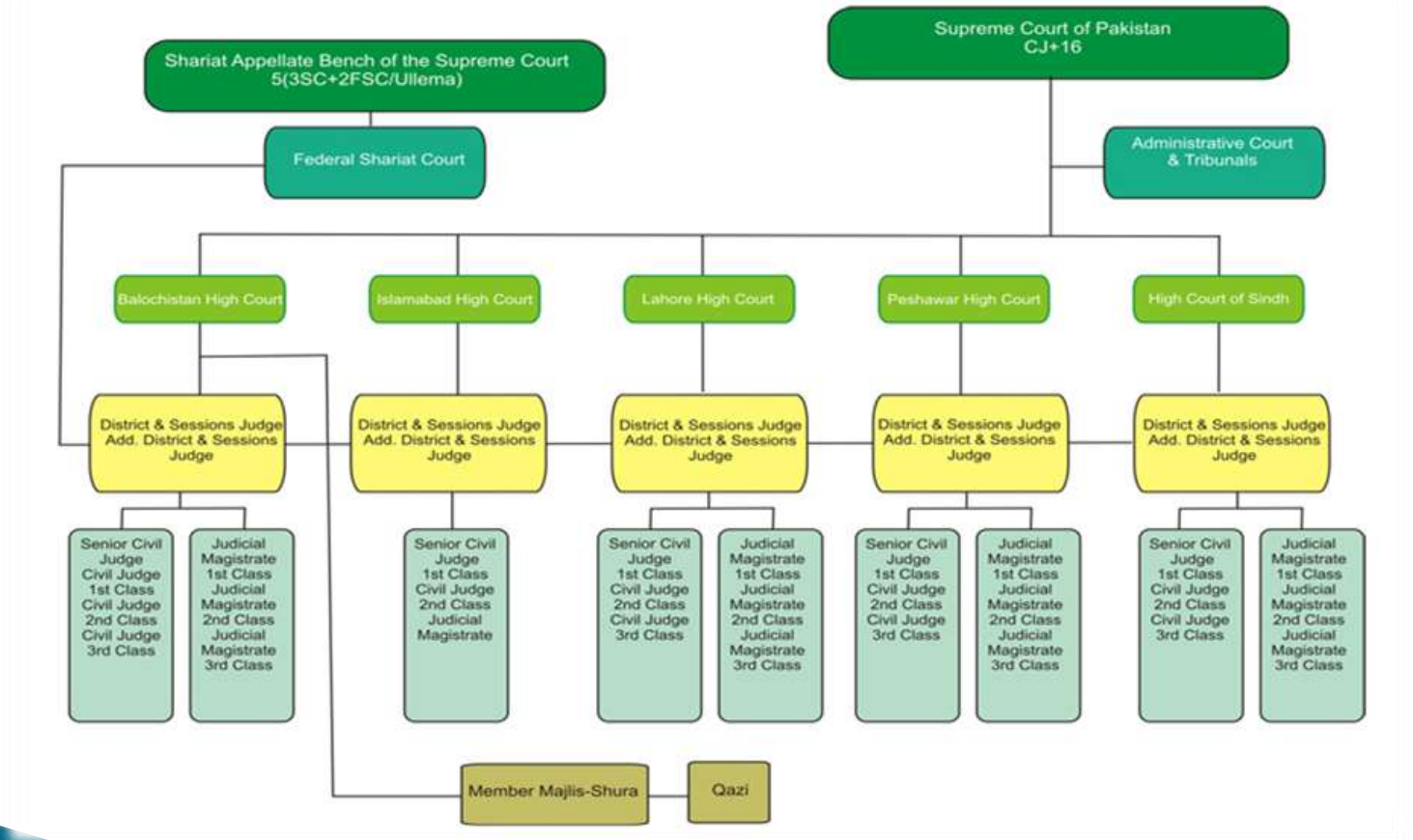
EXTRA TERRITORIAL JURISDICTION

Extra territorial Jurisdiction refers to a court's ability to exercise power beyond its territorial limits.

CYBER JURISDICTION

CYBER JURISDICTION

A virtual approach, defining the cyber world beyond the boundaries of nation states enforcement of cyber laws uniformly accepted.



CYBER DISPUTE/CONFLICT

CYBER DISPUTE/CONFLICT

A tense situation between and/or among nation-states and/or organized groups where unwelcome cyber attacks may result in retaliation