_____ is designed to protect the organizational resources on the network. **Password Policy**

Universities to group together to promote cyber security education under the umbrella of the _____? **HEC**

.name gTLD is use for? **for personal names**

_____ is the anticipation of unauthorized access or break to computers or data by means of wireless networks is called? **Wireless security**

The Basic purpose of cyber offences defined in Pakistan Ordinance No. LXXII or 2007 to make provision for _____? **prevention of the electronic / cyber crimes**

.biz gTLD is use for? **Business**

_____is of what can be accessed, published, or viewed on the Internet. **Cyber censorship**

Defacing the government's websites by the hackers of enemy countries is called _____. **Uncontrolled hacktivism**

Issues such as protection of critical infrastructure & response to computer emergencies fall under _____ strategy. **National Cyber**

Independent group of hackers with colorful names _____ an Indian or Pakistani website. **Defaces**

There are about _____cyber offences defined in Pakistan Ordinance No. **LXXII or 2007 to make provision for prevention of the electronic / cyber-crimes? 19**

The policy that deals with "how to react to various kinds of attacks" is _____. **Defense Policy**

Password policy is designed to protect the _____ resources on the network. **Organizational**

International Consensus Principles create a predictable legal Environment as to remove _____ barriers to electronic authentication. **Legal**

Download copy, extract data from an open system done fraudulently is treated as _____ **Cyber crime**

_____ is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise. Email security

United Nations Commission on International Trade Law (UNCITRAL) is a core legal body of _____? **United Nations**

In addition to the basic gTLDs new gTLDs were added on _____. **Nov 16, 2000**

The percentage of Intentional attack by external hackers, criminals, terrorists or activists is ___? **49%**

In dealing with cyber security issues there is no bilateral or regional cooperation in _____ region. **South Asia**

It is critically important to explore factors delaying investigation and _____ ? **prosecution of cyber-crime offending**

An impediment to Evidence Discovery and Analysis is the one factor which is responsible for?

The gTLD used for professionals is _____. **Pro**

The Convention on Cyber-crime is also known as? **Budapest Convention**

The total number of ccTLDs reflected in the database of the Internet Assigned Numbers Authority (IANA) is _____ **252**

In addition to the basic gTLDs new gTLDs were added by _____ Organization. **ICANN**

Find out, select & uninstall all _____ programs from your computer. **Unwanted**

2 Cyber Criminals were arrested by FIA in _____ on 13-sept-2012. **Bahawalpur**

The gTLD used for the entire aviation community is _____. **Aero**

Policy for delegates attending the GGE conferences at the UN, internet governance conferences & international seminars comes under _____. **Foreign Policy**

National cyber security forum does not perform the _____. **Educate old peoples**

Cs-204

Mcq's

1) World Wide web is the collection of **electronic documents.**
2) Each electronic document on the web is called a **web page** that can contain text, graphics, audio and video**.**
3) **Cyber Culture** converts the human written language or symbols to machine language and reconverts to human understandable language so the people on the destination can understand.
4) Now a day's especially in online chatting cyber language is created of new codes which affect our daily **spoken language**.
5) There are **Seven** components of cyber culture.
6) Internet, email, blog, chat, e-commerce, social networks and website are components of **cyber culture.**
7) **Internet** is The network formed by the co-operative interconnection of a large number of computer networks.
8) **Main goal** of the internet is to connect several computers together for the exchange of messages and share the information etc.
9) **Website** is a location connected to the Internet that maintains one or more web pages.
10) Web pages are the **building** blocks of the website

11) 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.

12) Email stands for **Electronic mail.**

13) There is no central **administration** and owner to the internet.

14) Messages that are sent electronically from one computer to another is an e-mail **message.**

15) A **blog** is a discussion or informational site.

16) Blog is published on the World Wide Web and consists of **discrete entries** ("posts").

17) A regularly updated website or web page is run by an **individual or group of individuals.**

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

19) Online chat may address **point-to-point communications** as well as **multicast communications.**

20) Chat can be from one sender to many receivers and video chat, or may be a **feature** of a web conferencing service.

21) A chat may **be direct text-based or video-based (webcams**)

22) E- commerce stands for **Electronic Commerce.**

23) **E-commerce** is the trading or facilitation of trading in products or services using computer networks, such as the Internet.

24) Online shopping, online market places, Business to business buying & selling, online newsletter for marketing prospective are **Commercial transactions** on internet**.**

25) 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.**

26) Facebook, Linkedin, Twitter are examples of **Social network.**

27) 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.

28) Cyberspace is a **public space** where individuals can meet, exchange ideas, share information, provide social support and conduct business.

29) "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" is the concept of **Cyber space**.

30) Due to **worldwide** use of computer network, people are now able to get together and form **cyber communities** that can exchange messages easily through cyber space.

31) Physically meeting has been reduced due to introduction of **cyber culture**.

32) **Culture** is an **important** process in computer related contexts. The processes that create meaning in actions.

33) 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.

34) 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.

35) The **cyber culture** has brought great impact on human individual'slife.

36) In education the style of teaching learning has changed. The student teacher **interactivity** can be formed **online**.

37) The cyber culture has great influence in the **business world**.

38) The use of internet for emails and other social networks is our **participation in the cyber culture.**

39) Cyber culture **reduced** the gap between groups and individuals separated from each other due to some reasons.

40) 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.

41) Face to face communication is becoming weak due to **emerging of social networks.**

42) The People who **don't have the ability to communicate face to face** they can exchange their views, through these social network.

43) The cyber culture is **developing** and we **need** to know the values and believes of this culture.

44) Cyber culture has great influence on human culture and in way **new uniform global culture is developing.**

45) In traditional E-commerce all the dimensions are **physical** in nature.

46) In Pure E- commerce all the dimensions are **digital** in nature.

47) **Hacking** in simple terms means illegal access into a computer system without the permission of the computer owner/user.

48) Damaging or destroying data rather than stealing or misusing them is called **cyber vandalism**.

49) A **Virus** is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.

50) **Trojan horses** are email viruses that can duplicate themselves, steal information, or harm the computer system.

51) The method of hiding plaintext in such a way as to hide its substance is called **encryption**.

52) The term **"Cyber Law"** Refers to all the legal and regulatory aspects of the Internet and its users.

53) The 1st rule of management is **delegation**.

54) The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by **national lawmakers**.

55) A **patent** is a government authority or license conferring a right or title for a set period, especially the sole right to exclude others from making, using, or selling an invention.

56) There are about **19** cyber offences defined in Pakistan Ordinance No. **LXXII or 2007** to make provision for prevention of the electronic / cyber crimes.

57) Awareness learning needs to enter the **21st** Century.

58) A **gTLD** is a generic top level domain.

59) A **ccTLD** is a country code top-level domain, for example: .mx for Mexico.

60) There are currently **252** ccTLDs reflected in the database of the Internet Assigned Numbers Authority (IANA).

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

62) The **B2C** model involves transactions between business organizations and **consumers**.

63) A **C2B** model, is a type of commerce where a consumer or **end user** provides a product or service to an organization.

64) Computer may be used as a **weapon** for crime or as a target.

65) **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.

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

67) **Malware** is any software that infects and damages a computer system without the owner's knowledge or permission.

68) **Trojan horses** are email viruses that can **duplicate** themselves, steal information, or harm the computer system.

69) The method of hiding plaintext in such a way as to hide its substance is called **encryption**.

70) **Encrypting** plaintext results in unreadable gibberish **called cipher text.**

71) The term **Cyber Law** Refers to all the legal and regulatory aspects of the Internet and its users.

72) There are **43** sections in the ordinance **ETO 2002**. It deals with the **8** main areas relating to e-Commerce.

73) Illegal electronic messages to any person without the permission of the recipient is called, **Spamming**

74) A tense situation between and/or among nation-states and/or organized groups where unwelcome cyber attacks may result in retaliation is, **Cyber dispute / conflict**

75) A virtual approach, defining the cyber world beyond the boundaries of nation states enforcement of cyber laws uniformly accepted, **Cyber Jurisdiction**

76) There are_____ domains of E-commerce.

- **2**
- **3**
- **4**

- **5**

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

78) How many sections are included in Electronic Transaction Ordinance 2002?

- **43**
- 10
- 53
- 23

79) Public key encryption uses multiple keys. One key is used to encrypt data, while another is used to decrypt data. The key used to encrypt data is called the _____ key, while the key used to decrypt data is called the _____ key.

- Encryption, decryption
- Private, public
- Encryption, public
- **Public, private**

80) What is an encryption system that uses two keys: a public key that everyone can have and a private key for only the recipient?

- Encryption

- **Public key encryption**
- Intrusion-detection software
- Security-auditing software

81) The term Cyber Law is refer to as the legal and regulatory aspects of the _____ and its _____.

- Users, Internet
- **Internet, Users**
- Digital data, Generators
- Internet Service Provider, User

82) According to Electronic Crime Bill 2007 what is the imprisonment of "Unauthorized access to code" Offense?

- 6 Years
- **3 Years**
- 3 Months
- None of the above

83) According to Electronic Crime Bill 2007 what is the imprisonment of "Electronic Fraud" Offense?

- 1 Year
- 10 Months
- **7 Years**

- 7 Months

84) What scrambles the contents of a file so you can't read it without having the right decryption key?

- **Encryption**
- Intrusion-detection software
- Security-auditing software
- All of the above

85) What is the Fine of "Cyber Terrorism" Offense according to Electronic Crime Bill 2007?

- 1 Million
- **10 Million**
- 10 Thousand
- None of the above

86) What is the fine of "Defamation" Offense according to Electronic Crime Bill 2007?

- 5000
- 50,000
- **5 Lac**
- 7 Lac

87) What is the Fine of "Cyber Spamming" Offense according to Electronic Crime Bill 2007?

- **50,000**
- 35,000
- 5 Lac
- None of the above

88) 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.

89) We can Use our computers to **attack** other computers on the internet.

90) **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.

91) **Trojan horses** are such programs which are used as the **back doors**.

92) Security suites, such as **Avast Internet Security**, will prevent you from downloading Trojan Horses.

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

94) **Cyber security** is necessary since it helps in **securing data** from threats such as data theft or misuse, also safeguards your system from **viruses.**

95) **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.

96) Your **home computer** is the popular **target** for intruders.

97) **Hackers** attack where they see **weakness**.

98) A system that hasn't been **updated** recently has flaws in it that can be taken advantage of by **hackers**.

99) The word "**malware**" comes from the term "**Malicious software**."

100) Main goal of the **internet** is to connect **several computers** together for the **exchange** of messages and share the information etc.

.....

1. When a customer of a website are unable to access it due to bombardment of fake traffic, it is known as
   - Denial of Service Attack
2. Security Procedure can
   - Reduce but not eliminate risks
3. How Many Issues are covered In Electronic Crime Bill 2007 ?
   - 21
4. A tense situation between and/or among nation-states and/or organized groups where unwelcome cyber attacks may result in retaliation termed as
   - Cyber Dispute
5. The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation that consisted of----------sections.
   - 43
6. The 1st Law related to cyber issues 1st introduced in ----------
   - 2002
7. When Plain text is converted to unreadable format, it is termed as ----------.
   - Cipher Text
8. Which of the following is an example of a cyber crime?
   - Spam Emails
9. What Floods a website with so many request for service that it slows down or crashes ?
   - Denial-of Service attack
10. Malicious software is known as
    - Malware
11. A cyber attach in which a minor fraction of priced is added and taken to some other account is called ----------.
    - Forgery
12. The First Cyber regulation was evolved in the year ----------
    - 1966
13. Jurisdiction over cases arising in or involving persons residing within a defined territory refers to ---------
    - Territorial Jurisdiction
14. All of these are suggestion for safe computing EXCEPT
    - Open all e-mail messages but open slowly
15. What is the fine of the “Cyber Spamming” Offense according to Electronic Crime Bill 2007?
    - 50,000
16. Which of the following is a goal that courts try to achieve?
    - All of the Given Options
17. ------ is defined as any crime completed through the use of computer technology
    - Computer Crime
18. Cyber Culture Language is -----
    - No specific Language
19. According to Electronic Crime Bill 2007 what is the imprisonment of “Unauthorized access to code” Offense ?
    - 3 Years
20. -------- are the building blocks of the website.
    - Web pages

21. In ---------- the dimensions are physical in nature and all transactions are Performed off-line?
    - Traditional Commerce
22. According to Electronic Crime Bill 2007 what is the imprisonment of “Criminal Access” Offense?
    - 3 Years
23. How many sections are included in Electronic Transactions Ordinance 2002?
    - 43
24. What is the most common tool used to restrict access to a computer system?
    - Passwords
25. Virus can reach to your computer in which way?
    - All of the above
26. What is the fine of “Defamation” Offence According to Electronic Crime Bill 2007?
    - 5 Lac
27. ------- is the process or mechanism used for converting ordinary plain text into garbled non-human readable text & vice versa.
    - Cryptography
28. Members of Majlis-e-Shura in Shariah Appellate bench of supreme court of Pakistan works under ?
    - Supreme Court
29. In ---------- the dimensions are digital in nature and all transactions are performed on-line
    - Pure E-commerce
30. Internet is Owned by
    - No Body owns internet
31. The term “Cyber Law” Refers to all the legal and regulatory aspects of ----the and its ----
    - Internet , users
32. Who breaks into other people’s computer systems and steals and destroy information?
    - Hackers
33. Public key cryptography is also known as ---------- Cryptography?
    - Asymmetric
34. What is “I” stands in CIA triad?
    - Integrity
35. What is short for malicious software (is a software designed to disrupt computer operations, gather sensitive information ,or gain unauthorized access to computer systems)?
    - Malware
36. The 1st l law related to digital transaction in Pakistan was introduced in--------.
    - 2002
37. Firewalls are used to protect against----------.
    - Unauthorized Access
38. Model Law on E-Commerce and E-Signatures were evolved in ----------.
    - 1996
39. The network formed by the co-operative interconnection of a large number of computers networksis called ----------.
    - Internet

40. Amazon.com comes under the following model?
    - B2C
41. The imprisonment under section for violation of privacy information is ---- with fine of ------
    - 7 years. 1 million
42. Each electronic document on the web is called a ----------
    - Web Page
43. What is hardware and/or software that protects computers from intruders?
    - Firewall
44. -------- is a discussion or informational site published on the World Wide Web consisting of discrete entries typically, runs by an individual or a small group
    - Blog
45. What is the process of making a copy of the information stored on a computer?
    - Backup
46. In a hybrid approach ----- key is used to decrypt session key and -------- key to decrypt ciphertext
    - Private, Session
47. There are ------ types of Jurisdiction
    - 3
48. Gains or attempts to gain access to any information system with or without any purpose comes under ----------
    - Violation of Privacy information
49. Which type of e-commerce focusses on consumers dealing with each other?
    - C2C
50. What is the fine of “Cyber Terrorism” Offense According to Electronic Crime Bill 2007 ?
    - 10 Million
51. Process of buying, selling or exchanging products, services and information through computer networks is called
    - E-commerce
52. E-commerce is not suitable for
    - Online Job Searching
53. An e-business that allows consumers to name their own price for product and service is following which e-commerce model
    - C2B
54. Most individuals are familiar with which form of e-commerce ?
    - B2C
55. Which Process can Prevent data from lose due to computer problems or human errors?
    - Backup
56. The ability of a court to exercise power beyond its territorial limits refers to ---------- Jurisdiction.
    - Extra Territorial Jurisdiction
57. The practice of forging a return address on an e-mail, so that the recipient is fooled into revealing private information is termed as?
    - Spoofing
58. What software detects and removes computer viruses
    - Antivirus
59. In internet terminology IP means
    - Internet Protocol

60. The right, power, or authority to administer justice by hearing and determining controversies is referred to as?
    - Jurisdiction
61. What scrambles the contents of a file so you can't read it without having the right decryption key?
    - Encryption
62. collecting personal information and effectively posing as another individual is known as
    - Identity Theft
63. The method of hiding -------in such a way as to hide its substance is called encryption
    - Palin-text
64. Territorial Jurisdiction Refers to Jurisdiction over cases arising in or involving persons residing within a ----------.
    - defined territory
65. in --- both ends must agree upon a single shared key for encryption and decryption of messages and keep the key secret between them
    - Symmetric Encryption
66. The first Cyber regulation in Pakistan was ----------.
    - Electronic Transaction Ordinance
67. What is "A" Stands for in CIA triad?
    - Availability
68. What is "C" Stands for in CIA triad?
    - Confidentiality
69. Who Protects system from external threats?
    - Firewall
70. All the legal and regulatory aspects of the Internet and its user are defined in the term
    - Cyber Law
71. A website is being accessed by referencing a ----- that identifies the site
    - Uniform resource locator (URL)
72. ---------- Cipher technique uses "shift by 3 "rule in encrypting the plain text.
    - Caesar Cipher

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

Quiz No. 02 - CYBER LAW
(FALL 2018) 19-12-2018

Question No. 01: How many sections are included in Electronic Transaction Ordinance 2002?

- **43**
- 10
- 53
- 23

Question No. 02: What is an encryption system that uses two keys: a public key that everyone can have and a private key for only the recipient?

- Encryption
- **Public key encryption**
- Intrusion-detection software
- Security-auditing software

Question No. 03: According to Electronic Crime Bill 2007 what is the imprisonment of "Unauthorized access to code" Offense?

- **6 Years**
- 3 Years
- 3 Months
- None of the above

Question No. 04: What scrambles the contents of a file so you can't read it without having the right decryption key?

- **Encryption**
- Intrusion-detection software
- Security-auditing software
- All of the above

Question No. 05: What is the fine of "Defamation" Offense according to Electronic Crime Bill 2007?

- 5000
- 50,000
- **5 Lac**
- 7 Lac

Question No. 06: Public key encryption uses multiple keys. One key is used to encrypt data, while another is used to decrypt data. The key used to encrypt data is called the _____ key, while the key used to decrypt data is called the _____ key.

- Encryption, decryption
- Private, public
- Encryption, public
- **Public, private**

Question No. 07: The term Cyber Law is refer to as the legal and regulatory aspects of the _____ and its _____.

- Users, Internet
- **Internet, Users**
- Digital data, Generators
- Internet Service Provider, User

Question No. 08: According to Electronic Crime Bill 2007 what is the imprisonment of "Electronic Fraud" Offense?

- 1 Year
- 10 Months
- **7 Years**
- 7 Months

Question No. 09: What is the Fine of "Cyber Terrorism" Offense according to Electronic Crime Bill 2007?

- 1 Million
- **10 Million**
- 10 Thousand
- None of the above

Question No. 10: What is the Fine of "Cyber Spamming" Offense according to Electronic Crime Bill 2007?

- **50,000**
- 35,000
- 5 Lac
- None of the above

****

Quize file cs204 created by Toseef
Maryam

Lecture No 4

1. 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.
2. Protecting computer system and information from unauthorized access or destruction / abuse.
3. Security deal with three primary issues, called the CIA triad.
4. Confidentiality Assurance that only authorized user may access a resource.
5. Integrity Assurance that resources has not been modified.
6. Availability Assurance that authorized user may access a resource when requested.
7. Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
8. Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
9. 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.
10. Your home computer is the popular target for intruders.
11. We can use our computers to attack other computers on the internet.
12. Intruder attacks home computer because it is not very secure and easy to break into.
13. They do attack your computers by send us a E-mail with virus.
14. Trojan horses are such programs which are used as the back doors.
15. A Virus is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.

16. Virus can reach to our computer through CD-Rom.
17. Virus can reach to our computer through E – mail.
18. Virus can reach to our computer through Websites.
19. Virus can reach to our computer through download files.
20. Install a security suite that protects the computer against threats such as viruses and worms.
21. Handle E- mail attachments carefully.
22. A person who secretly gets access to a computer system in order to get information, cause damage, etc.
23. Hackers attack where they see weakness.
24. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.
25. Regularly update your operating system.
26. Install Anti virus software's.
27. The word "malware" comes from the term "Malicious software."
28. Malware is any software that infects and damages a computer system without the owner's knowledge or permission.
29. Download an anti-malware program that also helps prevent infections.
30. Activate Network Threat Protection, Firewall, Antivirus.
31. Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
32. These viruses are the most serious threats to computers.
33. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
34. Password attacks are attacks by hackers that are able to determine passwords or find passwords

to different protected electronic areas and social network sites.

35. Maintain current software and updates.

36. Never share passwords .

37. Do not click random links.

38. Do not download unfamiliar software off the Internet.

39. Log out or lock your computer.

40. Remove unnecessary programs or services.

41. Frequently back up important documents and files.

42. Protects system against viruses, worms, spyware and other unwanted programs.

43. Protection against data from theft.

44. Protects the computer from being hacked.

45. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.

Quize file cs204 created by Toseef Maryam

Lecture No 4

1. 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.
2. Protecting computer system and information from unauthorized access or destruction / abuse.
3. Security deal with three primary issues, called the CIA triad.
4. Confidentiality Assurance that only authorized user may access a resource.
5. Integrity Assurance that resources has not been modified.
6. Availability Assurance that authorized user may access a resource when requested.
7. Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
8. Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
9. 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.
10. Your home computer is the popular target for intruders.
11. We can use our computers to attack other computers on the internet.
12. Intruder attacks home computer because it is not very secure and easy to break into.
13. They do attack your computers by send us a E-mail with virus.
14. Trojan horses are such programs which are used as the back doors.
15. A Virus is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.
16. Virus can reach to our computer through CD-Rom.
17. Virus can reach to our computer through E – mail.
18. Virus can reach to our computer through Websites.
19. Virus can reach to our computer through download files.
20. Install a security suite that protects the computer against threats such as viruses and worms.
21. Handle E- mail attachments carefully.

22. A person who secretly gets access to a computer system in order to get information, cause damage, etc.
23. Hackers attack where they see weakness.
24. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.
25. Regularly update your operating system.
26. Install Anti virus software's.
27. The word "malware" comes from the term "Malicious software."
28. Malware is any software that infects and damages a computer system without the owner's knowledge or permission.
29. Download an anti-malware program that also helps prevent infections.
30. Activate Network Threat Protection, Firewall, Antivirus.
31. Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
32. These viruses are the most serious threats to computers.
33. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
34. Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.
35. Maintain current software and updates.
36. Never share passwords .
37. Do not click random links.
38. Do not download unfamiliar software off the Internet.
39. Log out or lock your computer.
40. Remove unnecessary programs or services.
41. Frequently back up important documents and files.
42. Protects system against viruses, worms, spyware and other unwanted programs.
43. Protection against data from theft.
44. Protects the computer from being hacked.
45. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.

Cs204

Mcqs ch (1,

C# 1

1. **Positive** Online Environment of Internet users and a healthy cyber culture for the Internet community
2. A **recognition** of the power of the Internet to benefit oneself and the community at large.
3. To **reflect** on how to become a responsible user of social networking sites and a commitment towards building a healthy cyber culture
4. Focuses on the construction, maintenance and facilitation of community in **electronic** networks and computer mediated communication.
5. **World Wide Web** is the collection of electronic documents.
6. Each electronic document on the web is called a **web page.**
7. Web page can contain **text, graphics, audio and video**.
8. 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.**
9. Like every culture has its own **language**,
10. the cyber culture is not the **exception** to this rule.
11. 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.
12. Now a day's specially in online chatting the cyber language is creates of new **codes** which affects our daily spoken language.

13. 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.
14. 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.
15. A location connected to the **Internet** that maintains one or more web pages.
16. Web pages are the **building blocks** of the website.
17. Web pages includes documents like **texts and multimedia contents**
18. 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.
19. **Electronic mail**, most commonly called **email.**
20. E-mail is the Most widely used **application** on the internet.
21. Messages that are sent electronically from one computer to another is an **e-mail message**
22. A **blog** is a discussion or informational site published on the WorldWide Web consisting of discrete entries ("posts").
23. A regularly updated website or web page, typically , runs by **an individual or a small group**

24. Any kind of communication over the **Internet** that offers a real-time transmission of text messages from sender to receiver is called **online chat**.
25. 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**.**
26. 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**.**
27. **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.
28. **Commercial transactions conducted electronically on the Internet.**
    - Online shopping.
    - Online market places.
    - Business to business buying & selling.
    - Online newsletter for marketing prospective.
29. **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.

30. 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.
31. **Physically** meeting has been reduced due to introduction of cyber
culture
32. **Culture** is an important process in computer related contexts.
33. Culture processes that **create meaning** in actions.
34. 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.
35. 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.
36. The cyber culture has brought great impact on **human individual's life.**
37. In education the style of teaching learning has changed The student teacher **interactivity** can be formed online.
38. The cyber culture has great influence in the **business world.**
39. The use of internet for emails and other social networks is our **participation** in the cyber culture
40. **Face to face** communication is becoming weak due to emerging of these social networks.

41. The People who don't have the ability to communicate face to face they can exchange their views, through these **social network**.
42. Business decision can be made through **video conferences.**

Lecture # 2

Traditional E- Commerce

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

Pure E- commerce

4. All the dimensions are **digital** in nature.
5. Pure online (virtual) organizations.
6. Buy and sell products **online.**

Hybrid Approach

7. A combination of **physical and digital** dimension
8. Primary business carried out in **the physical world**.
9. Provide some services **on line.**
10. **B2B Model** describes commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.
11. 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.

12. The **B2C model**
also includes services online banking, travel services, and health information.
Example: www.daraz.pk, www.amazon.com etc….
13. A **C2B model**, is a type of commerce where a consumer or end user
provides a product or service to an organization
14. The **C2C model** involves transaction between consumers. Here, a
consumer sells directly to another consumer.
eBay.com, olx.com, etc…
15. A consumer uses **Web browser** to connect to the home page of a merchant's Web site on the Internet.
16. The consumer browses the **catalog** of products featured on the site and selects items to purchase.
17. The selected items are placed in the electronic equivalent of a **shopping cart**.
18. 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.
19. 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.

20. The Commerce Server site then forwards the order to a Processing Network for payment processing and **fulfilment.**

21. 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.

22. Disadvantages of e commerce

- Communication improvement.
- 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.

Lecture # 3

1. **Computer crime or cybercrime**, refers to any crime that involves a computer, Mobile and a network.
2. Computer may be used as **a weapon** for crime or as a target.
3. **The Computer as a Target:** Using a computer to attack other computers.
4. **The computer as a weapon**: Using a computer to commit real world crimes.

5. **Cyber Criminals** Those who are doing crimes by using the computer as a target or an object.
6. **Hacking** in simple terms means illegal access into a computer system without the permission of the computer owner/user.
7. **Software Piracy** This crime occurs when a person violates copyrights and unauthorized copying of software.
8. **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.
9. **Malicious Software** 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, email bombing etc.)
10. **Identity Theft** A criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information.
11. **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.

12. **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.
13. **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.
14. **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.
15. Never send your **credit card** number to any site that is not secured.
16. Avoid sending any **photograph** online particularly to strangers.
17. Do not open mails from **strangers.** This prevents your system from unwanted attacks.
18. Don't respond to **harassing or negative** messages.
19. Learn more about **Internet** privacy.
20. Keep your operating system **up to date**.
21. Change passwords **frequently** and Use hard-to-guess passwords.
22. Don't share access to your computers with **strangers**.
23. If you have a Wi-Fi network, password **protect** it.
24. **Disconnec**t from the Internet when not in use.

Cs204

Ch # 4,5,6,7,8

1. Some of the possible prevention measures. One can take to avoid getting **victimized** for a cyber-crime
2. **Virus and Worms** is a “program” that is loaded onto your computer without your knowledge and runs against your wishes
3. **Hackers** A person who secretly gets access to a computer system in order to get information, cause damage, etc.
4. Hackers attack where they see **weakness**
5. The word "**malware**" comes from the term "Malicious software."
6. **Malware** is any software that infects and damages a computer system without the owner's knowledge or permission.
7. Download an **anti-malware** program that also helps prevent infections
8. **Trojan horses** are email viruses that can duplicate themselves, steal information, or harm the computer system.
9. **Trojan horses** viruses are the most serious threats to computers
10. Security suites, such as **Avast Internet** Security, will prevent you from downloading Trojan Horses.
11. **Password attacks** are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites
12. Do not download **unfamiliar** software off the Internet
13. The method of hiding plaintext in such a way as to hide its substance is called **encryption**.
14. Encrypting plaintext results in unreadable gibberish called **cipher text**
15. **CA** is authorized to issue certificates to its computer users. (ACA’s role is analogous to a country’s government’s Passport Office.)
16. The term “**Cyber Law”** Refers to all the legal and regulatory aspects of the Internet and its users
17. The **1st** rule of management is delegation. Don’t try and do everything yourself because you can't.
18. **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

    ICANN Uniform Domain Name Disputes

    Resolution Policy 1998

- DMCA 1998
- EUCD 2001
- ITA 2000
- The Electronic Transaction Ordinance 2002
- Prevention of Electronic Crime Ordinance 2008

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

23. There are **43** sections in this ordinance
24. **Spamming** is Illegal electronic messages to any person without the permission of the recipient
25. There are seemingly **21 'cyber' issues** covered in this Bill
26. The **FIA**, has been given complete and unrestricted control to arrest and confiscate material as they
27. The Government has literally attempted to insert a new word in the **English** language eel necessary
28. The word **TERRORISTIC** is without doubt a figment of their imagination vocabulary
29. Extra **territorial Jurisdiction** refers to a court's ability to exercise power beyond its territorial limits.

Cs204

Lecture#6::

Mcqs by Zeeshan Nadeem

1. The term "**Cyber Law"** Refers to all the legal and regulatory aspects of the **Internet** and its users
2.

Answer: cyber law, internet

1. 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.

Answer: **Cyber Murder**

1. _____ penetrates into every corner of the modern business.

Answer: **E-commerce**

1. The _____ rule of management is _____

Answer: **1st, delegation**

Cyber regulation's evolution Table for remember:

UNCITRAL 1966

Model Law on
E-Commerce 1996

E-Signatures 1996

Wipo Copy Rights Rules 1996

Wipo Performance and Phonograms Treaty Rules 1996

ICANN Uniform Domain Name Disputes Resolution Policy **1998**

DMCA 1998

EUCD 2001

ITA 2000

The cyber regulations in pakistan

1. The Electronic Transaction Ordinance ____

Answer: **2002**

1. Prevention of Electronic Crime Ordinance

answer: **2008**

1. The rule of law and lawyer are

Answer:
. Consultancy
. The Subject matter Expert
. A blend of Law and Technology
- All of above

Cs204
Lecture#6

Mcqs by Zeeshan Nadeem

1. The term "Cyber Law" Refers to all the legal and regulatory aspects of the Internet and its users
Answer: cyber law, internet ✅

2. 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.
Answer: Cyber Murder ✅

3. _____ penetrates into every corner of the modern business.
Answer: E-commerce ✅

4. The _____ rule of management is _____
Answer: 1st, delegation ✅

Cyber regulation's evolution Table for remember:

UNCITRAL 1966 ✅

Model Law on
E-Commerce 1996 ✅

E-Signatures 1996 ✅

Wipo Copy Rights Rules 1996 ✅

Wipo Performance and Phonograms Treaty Rules 1996 ✅

ICANN Uniform Domain Name Disputes Resolution Policy 1998

DMCA 1998 ✅

EUCD 2001 ✅

ITA 2000 ✅

The cyber regulations in pakistan
5. The Electronic Transaction Ordinance ____

Answer: 2002 ✅

6. Prevention of Electronic Crime Ordinance

answer: 2008 ✅

7. The rule of law and lawyer are
Answer:
. Consultancy
. The Subject matter Expert
. A blend of Law and Technology
- [x] All of above ✅
Prepared by Zeeshan Nadeem

by:- Adnan ameer

Lecture#8

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

ans:- jurisdiction

2) The right, power, or authority to administer justice by hearing ----------?

ans:- Determining controversies.

3) Which is not a type of jurisdiction?
a)Territorial Jurisdiction
b) Extra Territorial Jurisdiction
c) celluer jurisdiction
d) Cyber Jurisdiction

ans:- C

4)- ----------Refers-over cases arising in or involving ----------within a defined territory?

answer:-Territorial jursidictio & persons residing

5) which of the following is true about Extra territorail jursidiction?
a) jurisdiction over cases arising in or involving persons residing within a definedterritory.

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

Extra territorail jursidiction

c)refers to a court's ability to exercise power beyond its territorial limits.
d)Beyond the boundaries of nation statesenforcement of cyber laws uniformly accepted. cyber jursidiction

Ans:-C

6) which one is virtual approach of jursidiction beyond states boundaries?

ans:- Cyber jurisdiction

7) what is cyber conflict?

ans:-A tense situation between nation-statesorganized groups where unwelcome cyber attacks may result in retaliation

8) what is the difference between cyber dispute and cyber attack or conflict??

ans:- Both are same

Quize file cs204 created
by Toseef Maryam

Lecture No 4

1. 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.
2. Protecting computer system and information from unauthorized access or destruction / abuse.
3. Security deal with three primary issues, called the CIA triad.
4. Confidentiality Assurance that only authorized user may access a resource.
5. Integrity Assurance that resources has not been modified.
6. Availability Assurance that authorized user may access a resource when requested.
7. Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
8. Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
9. 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.
10. Your home computer is the popular target for intruders.
11. We can use our computers to attack other computers on the internet.
12. Intruder attacks home computer because it is not very secure and easy to break into.
13. They do attack your computers by send us a E-mail with virus.
14. Trojan horses are such programs which are used as the back doors.
15. A Virus is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.
16. Virus can reach to our computer through CD-Rom.
17. Virus can reach to our computer through E – mail.
18. Virus can reach to our computer through Websites.
19. Virus can reach to our computer through download files.
20. Install a security suite that protects the computer against threats such as viruses and worms.
21. Handle E- mail attachments carefully.
22. A person who secretly gets access to a computer system in order to get information, cause damage, etc.
23. Hackers attack where they see weakness.
24. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.

25. Regularly update your operating system.
26. Install Anti virus software's.
27. The word "malware" comes from the term "Malicious software."
28. Malware is any software that infects and damages a computer system without the
owner's knowledge or permission.
29. Download an anti-malware program that also helps prevent infections.
30. Activate Network Threat Protection, Firewall, Antivirus.
31. Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
32. These viruses are the most serious threats to computers.
33. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
34. Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.
35. Maintain current software and updates.
36. Never share passwords .
37. Do not click random links.
38. Do not download unfamiliar software off the Internet.
39. Log out or lock your computer.
40. Remove unnecessary programs or services.
41. Frequently back up important documents and files.
42. Protects system against viruses, worms, spyware and other unwanted programs.
43. Protection against data from theft.
44. Protects the computer from being hacked.
45. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.

Prepared by ::: Kamal asghar

1. Crimes against a government are referred to as .....**cyber terrorism**.
2. In this category, criminals hack military websites or circulate propaganda.....**Cyber Crime Against Government**
3. There are categories of cyber crime....**3**
4. In this case, they can steal a person's bank details and misuse the credit card to make purchases online.....**Cyber Crime Against Property**
5. Damaging or destroying data rather than stealing or misusing them is called .....**cyber vandalism**.
6. ..... is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner....**Cyber bullying**
7. ..... A criminal accesses data about a person's bank

account, credit cards, debit card and other sensitive information---.**Identity theft**
8. The software is used to gain access to a system to steal sensitive information or data or causing damage to software and hardware_____**Malicious Software**
9. _____The crime in which the attacker harasses or threaten a victim using electronic communication, such as e-mail, instant messaging (IM) ..**Cyber stalking**
10. _____ This crime occurs when a person violates copyrights and unauthorized copying of software.**Software Piracy**
11. _____ in simple terms means illegal access into a computer system without the permission of the computer owner/use.**Haking**
12. There are types of cyber crime____**numrous**.

Cyber law
Lecture # 7

Made by Ali
1. **They are two types of cyber law promulgated in Pakistan**
◦ Electronic Transaction Ordinance 2002
◦ Electronic / Cyber Crime Bill 2007
2.Which was the first IT-relevant legislation created by national lawmakers.
The Electronic Transactions Ordinance (ETO), 2002
3..It _____ for Pakistani e-Commerce locally and globally.
Protection
4} It is heavily taken from foreign law related to cyber crime.
5:ETO Protect Pakistan's critical infrastructure
6: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 …

7:Post ETO 2002
• Electronic Documentation & Records recognized
• } Electronic & Digital forms of authentication &
• identification
• } Messages through email, fax, mobile phones,
• Plastic Cards, Online recognized.

8:There are 43 sections in this ordinance ETO 2002

9:ETO 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

10: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

11: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

12:All offences under this __offfences to be non bail able _____Ordinance shall be non- bail able, compoundable and cognizable.

13} :No Court inferior to the Court of Sessions shall try any offence under this prosecution and trail of offences

14:Electronic cyber crime bill 2007 was promulgated by the President of Pakistan on the 31st December 2007.

15:: Electronic cyber crime bill deals with the electronic crimes included:

- ◦ Cyber terrorism
- ◦ Data damage
- ◦ Electronic fraud
- ◦ Electronic forgery
- ◦ Unauthorized access to code
- ◦ Cyber stalking
- ◦ Cyber Spamming/spoofing

16:ELECTRONIC cyver crime bill 2007 apply to every person who commits an offence,irrespective of his nationality or citizenship.

17:Electronic cyber crime bill 2007 exclusive powers to the Federal Investigation
Agency (FIA) to investigate and charge cases against such crimes.

18:} Every respective offence under this __Electronic cyber crime2007_____law has its distinctive punishment which can be imprisonment or/and fine.
19:Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.... Data damage
20: ELECTRONIC cyber crime bill 2007 punishment was 3 years,3 Lac
21: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.Electronic fraud
22:Electronic fraud Punishment was } 7 years and 7 Lac

23:} 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 Electronic Forgery:
24:Electronic Forgery: punishment was 7 year and 7 lac

25:Malicious code:
26:} **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 and } 5 Lac
27:Cyber stalking:
28:} **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 and } 3 Lac

29:Spamming:
} Illegal electronic messages to any person without the permission of the recipient.
Punishment: } 6 month and } 50,000

30::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.
31::Punishment:} 3 Years and 3 Lac

Offence **Imprisonment. Year. ..... fine**		
Criminal Access 3 3 Lac	**3**	**3**
Criminal Data Access 3 3 Lac		
Data Damage 3 3 Lac	**3**	**3**
System Damage 3 3 Lac		
Electronic Fraud 7 7 Lac	**3**	**3**
Electronic Forgery 7 7 Lac		
Misuse of Device 3 3 Lac	**3**	**3**
Unauthorized access to code 3 3 Lac		
Malicious code 5 5 Lac	**7**	**7**
Defamation 5 5 Lac		
Cyber stalking 3 3 Lac	**7**	**7**
Cyber Spamming 6 months 50,000		
Spoofing 3 3 Lac	**3**	**3**
Pornography 10 -----		
Cyber terrorism Life 10 Million	**3**	**3**
	5	**5**
	5	**5**
	3	**3**
	6	**50000**
	3	**3**
	10	**.....**
	Life	**10 million**

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.

Criticm

• 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.

By : Zeeshan Nadeem

Quize file cs204 created by Toseef
Maryam

Lecture No 4

1. 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.
2. Protecting computer system and information from unauthorized access or destruction / abuse.
3. Security deal with three primary issues, called the CIA triad.
4. Confidentiality Assurance that only authorized user may access a resource.
5. Integrity Assurance that resources has not been modified.
6. Availability Assurance that authorized user may access a resource when requested.
7. Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
8. Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
9. 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.
10. Your home computer is the popular target for intruders.
11. We can use our computers to attack other computers on the internet.
12. Intruder attacks home computer because it is not very secure and easy to break into.
13. They do attack your computers by send us a E-mail with virus.
14. Trojan horses are such programs which are used as the back doors.
15. A Virus is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.

16. Virus can reach to our computer through CD-Rom.
17. Virus can reach to our computer through E – mail.
18. Virus can reach to our computer through Websites.
19. Virus can reach to our computer through download files.
20. Install a security suite that protects the computer against threats such as viruses and worms.
21. Handle E- mail attachments carefully.
22. A person who secretly gets access to a computer system in order to get information, cause damage, etc.
23. Hackers attack where they see weakness.
24. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.
25. Regularly update your operating system.
26. Install Anti virus software's.
27. The word "malware" comes from the term "Malicious software."
28. Malware is any software that infects and damages a computer system without the owner's knowledge or permission.
29. Download an anti-malware program that also helps prevent infections.
30. Activate Network Threat Protection, Firewall, Antivirus.
31. Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
32. These viruses are the most serious threats to computers.
33. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
34. Password attacks are attacks by hackers that are able to determine passwords or find passwords

to different protected electronic areas and social network sites.

35. Maintain current software and updates.

36. Never share passwords .

37. Do not click random links.

38. Do not download unfamiliar software off the Internet.

39. Log out or lock your computer.

40. Remove unnecessary programs or services.

41. Frequently back up important documents and files.

42. Protects system against viruses, worms, spyware and other unwanted programs.

43. Protection against data from theft.

44. Protects the computer from being hacked.

45. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.