UNIT -V COMPUTER ETHICS AND CYBER SECURITY 17

Computer Ethics And Cyber Security

1.What is cyber-crime?
- A cyber-crime is a crime which involves computer and network.

2.What is Computer ethics
- Computer ethics is set of moral principles that regulate the use of computers by users

3. What are ethical issues? Name some.

An Ethical issue is a problem or issue that requires a person or organization to choose between alternatives
- Cyber crime
- Software Piracy
- Unauthorized Access
- Hacking
- Use of computers to commit fraud
- Sabotage in the form of viruses
- Making false claims using computers

4.What is Harvesting?
- A person or program collects login and password information from a legitimate user to illegally gainaccess to others' account(s).

5.What is Malware?
- Malicious programs that can perform a variety of functions including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring user's computer activity without their permission

6.Write two types of cyber attacks. ref.above ans Differentiate between scam and spam

Scam
- Tricking people into believing something that is not true.

Spam
- Distribute unwanted e-mail to a large number of internet users

7.What is spoofing?
- It is a malicious practice in which communication is send from unknown source disguised as a source known to the receiver

8.What are Warez?
- Commercial programs that are made available to the public illegally are often called warez.

9. Write a short note on cracking.
- Cracking is where someone edits a program source so that the code can be exploited or modified. A cracker (also called a black hat or dark side hacker) is a malicious or criminal hacker.

10. What is a Cookie?
- A cookie is a small piece of data sent from a website and stored on the user's computer memory (Hard drive) by the user's web browser while the user is browsing internet.
- Type of cookies: HTTP cookie, web cookie, Internet cookie, browser cookie, or simply cookie

11.What is the role of firewalls?(layered security)
- Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.

12. Write about encryption and decryption.
- Encryption and decryption are processes that ensure confidentiality that only authorized persons can access the information.
- **Encryption** is the process of translating the plain text data (plaintext) into random and mangled data (called cipher-text).
- **Decryption** reverse process of converting the cipher-text back to plaintext. Encryption and decryption are done by cryptography

13. Explain symmetric key encryption.
- Symmetric encryption is a technique to use the same key for both encryption and decryption. (Secret key)To exchange the key used to encrypt the data before they can decrypt it

14. What are the guidelines to be followed by any computer user?
- Honesty: Users should be truthful while using the internet.
- Confidentiality: Users should not share any important information with unauthorized people.
- Respect: Each user should respect the privacy of other users.
- Professionalism: Each user should maintain professional conduct.
- Obey The Law: Users should strictly obey the cyber law in computer usage.
- Responsibility: Each user should take ownership and responsibility for their actions

15.Define software piracy.

* Software Piracy is about the copyright violation of software created originally by an individual or an institution

Type of Piracy Function

1 Unauthorized access

* Unauthorized access is when someone gains access to a website, program, server, service, or other system by breaking into a legitimate user account.

2 Hacking

* Hacking is gaining unauthorized access to s computer system without the owner's permission.

3 Cracking

* Cracking is where someone edits a program source so that the code can be exploited or modified. A cracker (also called a black hat or dark side hacker) is a malicious or criminal hacker

Prevented Action:

* Stop to chat on Internet Relay Chat(IRC) or by Instant messenger.
* e-mail can also be a source for them.

16.Explain the types of cyber attacks.

1. Virus

A virus is a small piece of computer code that can repeat itself and spreads from one computer to another by attaching itself to another computer file.

2. Worms

Worms are self- repeating and do not require a computer program to attach themselves.

3. Spyware

Spyware can be installed on the computer automatically when the attachments are open, by clicking on links or by downloading infected software.

4. Ransom ware

Ransomware is a type of malicious program that demands payment after launching a cyber-attack on a computer system.

17.Define cyber law.

"Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet

18.Define digital signature.

* Digital signatures are based on asymmetric cryptography and can provide assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed by the signer