MODULE 1

Types of cyber crimes based on different perspectives:

As per law enforcement agencies

Categories:

1. Advanced cyber crime
2. Cyber enabled crimes
3. Cyber crime against individual
4. email spoofing
5. Spamming
6. Cyber defamation
7. Harassment and cyber stalking
8. Cybercrime against property
9. Credit card fraud
10. Intellectual property crimes
11. Software piracy
12. copyright infringement
13. trademark violations
14. theft of computer software
15. internet time thief
16. Cybercrime against organization
    1. Denial of service
    2. Virus attack
    3. Salami attack
    4. Email bombing
    5. Logic bombing
    6. Trojan horse
17. Cyber crime against society
    1. Forgery
    2. Cyber terrorism
    3. Web jacking

Violent cybercrimes:

1. Cyber terrorism
2. Cybertalking
3. Assault by threat
4. Child pornography

Non-violent cybercrimes

1. Cyber theft
2. Cyber trespass
3. Cyber fraud
4. Destructive cybercrime

CYBERBULLYING

MALWARE  
PHISHING

EXTORTION VIA INTERNET

RANSOMWARE  
CYBERSPYING

TYPES OF HACKERS:

Knowledge basis:

1. Coders
2. Admin
3. Script kiddies

Activity basis:

1. Black hat
2. White
3. Grey

Reasons for hacking:

1. Hacking for fun
2. Hacking to steal (knowledge)
3. Hacking to disrupt
4. Hacking for ego satisfaction
5. Hacking for knowledge recognition

Prevention from hackers:

*special information security research team*

*defending hackers*

*ethical hacker*

Impact of hacking:

1. Loss in finance
2. Information loss
3. Decline in privacy
4. Reputation can be damaged

Steps or phases performed by hackers

1. Performing reconnaissance
2. Scanning and enumeration
3. Gaining access
4. Maintaining access and pacing backdoor
5. Covering tracks