Name : Mayur Pimpude Roll no. : 43

Class : D16AD Subject : CSL

# Assignement - 1A

Q1. Explain the classification of cyber crime .

↳

Classification of cybercrime :-

1. Crime against individual
   - ↳ password sniffing
   - ↳ computer sabatage
   - ↳ Spamming
   - ↳ pornographic offence

I Spoofing :- Attempt to gain confidence get access of system , stealing data.

II Cyberstalking :- Browsing anyone's internet activities with help of social media .

III cyber demation !- cyber defamation mean injuring other persons reputation via internet .

2. Cybercrime against organization :-

1. Attack by virus :-
   A computer virus is a kind of malware which connect itself to another computer program + can replicate .

II Salami Attack :-
tactics to steal money , by which hacker steals

money in small amount. Attacker uses an online database to obtain customer infor. over time debutes insignificant amount from each account.

3. Cyber Crime Against Society :-

   1. Cyber Terrorism :-
      using cyberspace to hurt someone or general public.

4. Cyber Crime Against Property :-

   1. Illegally possesing an individual's bank or credit card details.

   11. Illegally possesing Intellectual property rights.

5. Crime emanating from usernet newsgroup :-
   usenet newsgroup constitute one of largest source of child pornography available in cyberspace.

Q2. what are the different trends in mobility? Explain

↳ Mobility refers to movement of various elements within a network environment.

Iphones, Android are example of trends in mobility.

Types of mobility :-

1. user mobility :-
user who have access to similar communication services at different places.

2. Device mobility :-
movement of the communication device from one location to another with or without a user.

3. session mobility :-
A user move from one device to another from ongoing network session with interruption.

4. Service Mobility :-
Capability of network service to migrate between different servers or location seamlessly to maintain availability.

Q4. Explain various types of identity theft.

↳ Crime where an individual's personal information is stolen and used fraudulently for financial gain.

Types are :-

1. Finicial Identity Theft :-
Attacker steals personal information such as credit card, bank login detials.
It is important to check your credit history regularly to ensure it contains accurate information.
This can be extremely damaging to victims credit score & their ability to get a loan in the future.

2. medical Identity theft :-
Involves stealing person's medical insurence information which is then used to obtain medical services.
This type is costly & complicated crime to resolve.

3. Criminal Idntity theft :-
Happens when someone gives false information to police at the time of arrest.
Criminals will get state-issued identity document using credentials that they have stolen from someone else or will create fake ID.

4. child Identity theft :-
children can also be victims of identity theft. uses a child's personal information which often goes undetected for years because parents typically do not monitor.

5. Identity cloning :-
Attempting to impersonate someone else so they can simply hide their true identity. A minor form of this are people using photo of someone else on social media.

Q3. Discuss the security implications for organizations.
↳ Security Implications for organizations encompass a wide range of concerns related to protecting sensitive data ensuring confidential, integrity & avaliability of system & information. Some security implications are :-

1. Data Breach :-
can result in exposure of sensitive customer, employee. This can lead to finicial loss.

2. Insider Attack :-
Employees, partner can pose security risks though intenal or unintentional actions.

3. Third Party Risks :-
organization often rely on third-party vendor

and partner. These relationships can be introduce security risk if 3rd party donot have robust security practices.

4] Cloud Security :-
Organization using cloud service must address cloud security concerns including data protection.

5] Social engineering :-
Employ may fall victim to phishing attacks.

6] physical security :-
Measures to protect equipment, facilities & data centres from physical threats.

7] compliance & Regulation :-
Organization must comply with various data protection and privacy regulation.

8] cyber attack :-
Organization face threats from a variety of cyber attack including malware, ransomware, and distributed denial of service (DDoS) attack.