Roll No. : 51153
Class : FY-MCA
Div : B
Name : Hrushikesh R. Ranjput

Page No. | YOUVA
Date

Q.1. What is Cybercrime? Explain its origin in the world.

* Definition : Cybercrime is any illegal activity that involves a computer, network or the internet. Basically, if someone uses technology to commit a crime, it's called cybercrime.

* Origin of Cybercrime :

① Early Days (1960s - 1970s) :

It started with "phone phreaking", where people maniputed phone systems to make free calls.

② 1980s :

Hacking become popular as computers started connecting to each other.
People like Kevin Mitnick became famous for breaking into systems.

③ 1990s :

With rise of the internet, more people went online and cybercrime grew.
Viruses and malware began to spread.

④ 2000s :

Organised crime groups formed online, using techniques like phising (fake emails/websites) and identity theft to steal information.

⑤ 2010s - Present :

Cybercrime has become very advanced. Ransomware (locking files and demanding money) and cyber espionage (spying) are common.

Q2] What is Cyber ~~Security~~ space ? How it is related with cyber security. ?

=> Cyber space means virtual environment created by computers, networks and the internet

- It includes all the interconnected system, such as websites, apps social media platforms, emails and digital communication channels.
- It is essentially a digital world where information is created shared and stored

Relation with cyber security:-

Cyber security focuses on protecting cyberspace from harm such as hacking viruses or data theft. Since cyberspace is used for storing personal information, financial information and business information, it is at risk of being attacked by cyber criminals

Cyber security works to:-

1] Protect the data like sensitive information Eg:- passwords, bank details and private messages.

2] Secure the devices like phones, computers, laptops, tablets and make secure them from harmful softwares or unauthorised access.

3] Defend the networks by securing the internet connection and prevent cyberattacks on systems like wi-fi or corporate networks.

Eg:-

1] We use antivirus to protect device from harfulharmful softwares in cyberspace.

2] We use firewalls to block unwanted access to network.

Q3: Classify the cybercrimes into it's various categories & subcategories.

Sol:

I. Cyber Crime Against Individuals.

- These crimes directly target individuals, affecting their personal information, online security & digital well-being.

(i) Email spoofing :- A technique where the sender's email address is forged to appear as if it is coming from a trusted source, often used in scams.

(ii) Phishing (spear phishing, vishing):- Fradulent attempts to obtain sensitive information like passwords, credit card details through emails, phone calls or through sms.

(iii) Spamming :- Sending a large volume of unsolicited messages, often containing, advertisments malwares etc.

(iv) Cyber defamation :- Using online platforms to spread false information that damages a person's reputation.

(v) cyberstalking & Harassment :- persistent online threats, tracking or intimidation of an individual causing fear & distress.

(vi) Computer sabotage :- The deliberate destruction or disruption of computer systems often through malware or hacking.

(vii) password sniffing :- Intercepting & stealing login credintials using software or hardware tools.

PAGE NO.
DATE / /

II Cybercrime Against Properties

These crime involve the unauthorized use or damage of digital assests, financial resources & intellectual property.

(i) Credit card fraud:- stealing credit card details to make unauthorized transactions.

(ii) Intellectual property crime:- violating copyrights trademarks or patents by distributing or using protected content without permission.

(iii) Internet time theft:- Unauthorized use of someone's internet bandwidth or services without their knowledge.

III Cybercrime Against Organizations.

These attacks are directed at buisness, government institutions, or corporate entities, aiming to disrupt operations or steal data.

(i) Unauthorized Access of Computers (Hacking):- Gaining illegal access to a computer system to steal or manipulate data.

(ii) Password sniffing:- capturing ~~credit~~ credentials to access restricted systems or steal sensitive info.

(iii) Dos Attack (Denial of service):- Flooding a network or server with traffic to make it unavailable to users.

(iv) Email bombing:- Sending large volume of emails to overlod

and crash an email server.

(vi) Salami Attacks :- Conducting small, undetected financial frauds by taking minor amounts from many transactions.

(vii) Logic bombs :- A hidden piece of malicious code that activates under specific conditions to cause damage.

(viii) Trojan Horse :- A deceptive software program that appears useful but contains harmful malware.

(ix) Data diddling :- Altering data before or during processing to commit fraud.

(x) Industrial espionage :- illegally spying on competitors to gain trade secrets or confidential data.

(xi) Software Piracy

IV Cybercrime Against society :-

These crimes have a broader Impact, affecting the general public or national security.

(i) Forgery :- Creating fake digital documents, such as passports, ID cards, or contract for fraudulent purposes.

(ii) Cyberterrorism :- Using digital means to carry out acts of terrorism, such as hacking critical infrastructure, spreading propoganda or causing public fear.

(iii) web jacking :- Taking control of a website by exploiting security vulnerabilities, often to spread misinformation or demand ransom.

V Crimes Emanating from Unsent newsgroups :- These crimes arise from the misues of online discussion forums leading to illegal activities.

(i) illegal Content sharing :- posting or distributing pirated software, copyrighted materials or confidential data.

(ii) fraudulent Activites :- Using newsgroups to promote scams, phising schemes or fake investment opportunities

(iii) Drug & weapon Trade :- Facilitating illegal transaction involving drugs, firearms or other illicit goods.

Q.4. Explain the concept of cyber defamation and identity theft? | Roll no 51164 B

Ans Cyber defamation:

cyber defamation is a cognizable offense. In Section 499 of chapter XXI of IPC, regarding 'defamation' there is a mention that "whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the case hereinafter expected, to defame that person."
Cyberdefamation happens when the above takes place in an electronic form. Defamation can take any form, including spoken or written words, gestures or images.

Defamation can be divided into two categories: libel and slander. Libel is the written or published form of defamation, such as newspaper article, a blog post, or a social media post. Slander is the spoken form, such as false statement made in a conversation or a public speech.

Essentials to prove cyber defamation:
- The defamatory statement must be published, which means it must come to the attention of a third party.
- The statement must refer to the plaintiff.
- The statement should be defamatory in nature.

Identity theft:

Identity theft is a fraud involving another person's identity for an illicit purpose. This occurs when a criminal uses someone else's identity for his own illegal purposes. Such stolen identity is typically used to make unauthorized purchases, open new accounts, apply for loans, or file fraudulent tax returns. Identity thieves used sophisticated methods to steal information from unsuspecting victims. They use social engineering and phishing schemes, malware attacks, skimming devices, and even old-fashioned tactics like dumpster diving to get their hands on sensitive data.

Types: There are various amount of threats but some common ones are:
- criminal identity theft: the thief uses the victim's ID to commit crimes, making the victim responsible for the acts.
- Tax Identity theft: thieves used employee ID or SSN to fraudulen

claim tax refunds.

- Medical identity theft: Thieves use the victim's health info to create fraudulent medical services and bills.

Following are some methods by which you can enhance your security for identity theft:

- Use strong passwords and never share PINs.
- Enable two-factor authentication for emails.
- Don't share sensitive info on social media.
- Always verify authenticity when entering passwords.
- Never share AADHAR/PAN with untrusted individuals.
- Don't fill out suspicious forms or provide OTPs to strangers.

CIE - I

[Que ⇒ 5]

Que 5] Write short notes on ① Pornographic offences
② Forgery
③ Web Jacking.

⇒ ① Pornographic offences.

- These offences involves the creation, distribution publication or access to obscene and sexually explicit digital content.

- Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.

- As Internet has become cheaper its expansion has made the children a viable victim to the cybercrime.

- As the broad-band connections get into reach of more and more homes, larger child population will be using the Internet and therefore large population get attracted by such digital content.

- This results in the more childrens got falling into the aggression of pedophiles. Pedophiles are people who physically or psychologically coerce minors to engage in sexual activities, which the minors could not consciously consent to.

- Engaging in such activities can lead to severe legal consequences, including imprisonment fines and a permanent criminal record.

- Cybercriminal may use hidden online platforms encrypted communication or the dark web to distribute such content, making it harder.

for law enforcement to track them.

Preventive Measures:-
- Strict content moderation, cybersecurity policies for online platforms
- Awareness programs to educate users about the risks and consequences.
- Safe browsing to block user's access to websites containing dangerous or offensive material.

b) Forgery:-
- Digital forgery refers to the act of falsifying or manipulating digital documents, signatures, images, or identities to decieve others.

- Common example include fake digital certificate forged bank documents, manipulating emails and fraudulent digital transactions.

- Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners.

- Outside many colleges there is a sale of fake marksheets and degrees

- This becomes business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

- Such acts are considered serious cybercrimes as they can lead to financial fraud, identity theft.

Preventive Measures.

- Organisations can implement security measures such as digital signatures, blockchain technology and encryption to prevent forgery and ensure document authenticity.

- Penalising the peoples involves in the forgery activities and implementing strict laws.

3] Web Jacking.

- Web Jacking is a form of cybercrime where hackers take control of a website by exploiting vulnerabilities, hijacking domain names or altering DNS settings.

- Attackers may use phishing malware, or brute-force attacks to gain authorised access to websites administration.

- It occurs when someone forcefully takes control of a website.

- Web Jacking is a serious threat to business as it can lead to financial losses, reputational damage and legal liabilities.

- The ~~first~~ First step in web Jacking involves "password sniffing", ~~The~~ Actual owner of the website does not have any more control over what appears on that website.

Preventive Measures.

- Website owners should use strong authentication methods (e.g. two factor authentication).

- Regularly update software.
- Monitor DNS records and apply web security solutions. Like firewalls and intrusion detection system.

- Penalties for web jacking activities.

Page No.
Date

6 Correlate the cyber crime of identity theft for cyber defamation.

→ To understand how identity theft and cyber defamation are correlated we need know this term means.

① identity theft: this is a cybercrime where someone steals another person's personal information (like their name, social security name / number, bank details or passwords) Without their permission. the theif then uses these information to commit Fraud, such as making purchases, opening accounts, or even pretending to be the victim online.

② Cyber Defamation: This is when someone uses the Internet to harm another person's Reputation by spreading False or damaging Information about them. this can be happen On social media, blogs, Forums or other online Platform. the goal is to embarrass, humiliate or ruin the victim's image.

How identity theft and cyber defamation are connected.

① Using stolen identities For Defamation: A Cybercriminal might steal someone's identity like their social media account or email) and use to post false or harmful Information about another person.

For example: they could log into your Facebook Account and post offensive messages or lies about

someone else, making it look like you did it.

② DeFaming the victim of identity theft: in some caseses the theif might use the stolen identity to deFame the original owner. For instance, they could post inappropriate or illegal content using your name, making it seem like you are the one doing it. This can ruin your reputation and cause emotional distress.

③ Creating Fake identities For DeFamation: Cybercriminals sometimes create fake online profiles using stolen personal information. they might use these Fake accounts to spread lies or harmful content about someone else. since the account is Fake, it's harder to trace the real culprit and the victim of deFamation suffers without knowing who is behind it.

④ Blackmail and Extortion: identity theives might use the ~~se~~ stolen information to blackmail the victim. For example, they could threaten to spread false information to blackmail victim unless the pays them money.

Q.7. Explain the concept of credit card frauds in detail with a suitable example.

→ Credit card fraud is a financial crime where an unauthorized person misuses someone else's credit card info. to make purchases, withdraw money, or commit fraudulent activities. It can lead to financial loss for individuals, businesses and banks. With the rise of online transactions, fraudsters have developed more sophisticated techniques to steal credit card details and exploits vulnerabilities.

Some common types of credit card frauds are:

① Card-Not-Present (CNP) Fraud

This occurs when a fraudster uses stolen credit card details for online, phone, or mail transactions where the physical card is not required.

② Card Skimming

Fraudsters install skimming devices on ATMs or point-of-sale (POS) machines to secretly capture card's information allowing the fraudster to create a duplicate card.

③ Lost or Stolen Card Fraud

If a credit card is lost or stolen, it can be used by fraudsters for unauthorized transactions before the owner reports it. This can be used for small purchases that do not require PIN verification before the bank blocks it.

④ Phishing and Social Engineering

Scammers tricks victims into revealing their credit card details by sending fake emails, messages, or phone calls

pretending to be from a bank or a trusted institution

⑤ Identity theft

Criminals use stolen personal details like Aadhar, PAN, and banking credentials to apply for credit cards in the someone else's name.

⑥ Account Takeover

In this type of fraud, criminals hack into a card holder's account, change login details, and use the account for fraudulent activities.

Person X, an online shopper, receives an email from what appears to be his bank, stating that his credit card has been temporarily suspended due to suspicious activity. The email contains a link directing him to a website that looks exactly like his bank's official page. Without suspecting anything, X enters his credit card number, CVV and OTP to "reactivate" his card. Moments later, he notices unauthorized transactions on his account from international websites. By the time he contacts his bank, significant damage has already been done. This is an example of phishing fraud, where fraudsters trick victims into voluntarily providing their sensitive details.

What is s/w piracy? How this cyber crime is performed & by whoom?

→ Cyber crime is any illegal behaviour directed by means of electronic operations that targets the security of computer system & the data processed by them.

There are 5 types of cyber crimes :-

crime against: 1) indivial
2) property
3) society
4) organizations
5) from usenet newsgroups.

So in all this s/w piracy is a cyber crime agains organization. It is the illegal approach of unauthorized copying, distributing, modifying, selling or using s/w. In simple terms we can say s/w piracy is a act of stealling legal s/w.

s/w piracy can be performed by various types such as :-

1) Softlifting :-

In this piracy legal owner of s/w is one by others will illegally use that s/w by downloading it to their computers. ~~e.g.~~
e.g. many times we borrow s/w from our colleques & install a copy of that on our computers just to save money which rises to softlifting.

2) Hard-disk loading :-
It is one type of commercial s/w piracy which mainly happens in PC resell shops. The shop owner buys a legal copy of the s/w & reproduces its copies on multiple comps. by installing it. most of the times consumers are not aware of these things & get the pirated version of the s/w in the original c/w price or less than original price.

3) Counterfeiting :-
It is a form of piracy that occurs when s/w is illegally copied & distributed under the guise of authenticity. counterfeit s/w programs are usually sold at cheaper price than the real thing which may be attractive to certain buyers.

10

4) Licenced overuse :-

Licensed overuse can be international or caused by a lack of asset management protocols

e.g. when too many people on same network use single original copy of piece of s/w. simultaneously.

or the s/w is used outside the loca^ or company domain

5) Online piracy :-

In this illegal s/w is aquired from onlin auction sites & blogs which is mainly achieved thr. the P2P system as it is aquired using internet often it is called internet piracy.

Also s/w piracy can happen by

- Downloading s/w from unauthorized site
- Using s/w beyond licensed agreement
- Installing unauthorized s/w.
- Duplicating s/w.
- Gaining illegal access to s/w.

s/w piracy can be done by the people for personal use or companies installing unlicensed s/w on their computers to cut costs & criminal networks that distribute pirated s/w on large scale.

To prevent s/w piracy →

- Always purchase licensed s/w
- Detect & block potential threats used strong anti-virus s/w
- Raise awareness about consequences of s/w piray.

Name:- Rahul Nandu Nathe
Class:- FYMCA
Div :- B
Roll No:- 51148.

9.9]

Q) What is IT act 2000 of, in detail?

→ The Information technology Act 2000 (ITA-2000) also known as IT act is a primary law in India that deals with cybercrime & electronic commerce.

~~Key provisions~~:
Objectives of IT Act..

1] To provide legal recognition to electronic transactions: This means that electronic documents and digital signatures have the same legal status as their physical counterparts.

2] To facilate electronic governence:- This ensures that government record, can be maintained in electronic form, thus enabling more efficient transparent & cost effective governance.

3) To prevent cybercrime:- It defines various cybercrimes & prescribes penalities for them.

Key Sections And Provisions:-

1) Section 43:-

This section deals with unauthorized access to computer systems, data theft & virus attacks. It imposes penalities for accessing, downloading, copying & extracting data from computer systems without permission.

2) Section 66:

It defines hacking and prescribes imprisonment & Fines for hacking & related offenses.

3) Section 66A :-

This section was about sending offensive messages through communication service. etc.

4) Section 66B, 66C, 66D, 66E :-

These section deal with receiving stolen computer resources or communication devices, identify theft, cheating by personation using computer resources and violation of privacy.

5) Section 67 :- It deals with publishing or transmitting obscene material in electronic

form and prescribes penalties for the same.

6) Section 69: It empowers the government to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource.

7) Section 72:
It prescribes penalty for breach of confidentiality & privacy.

Amendments.
The IT Act 2008, brough significant changes.

1) Section 66A:
Introduced and later struck down by the supreme court.

2) Section 69A:
provides the power to issue direction for blocking public access to any information through computer resource.

3) Section 69B: Empowers to monitor and collect traffic data or information through any computer resource for cyber security.

Section 70 B:

Establishes the Indian computer Emergency Response Team (CERT-in) to oversee cybersecurity incidents & responces.

Section 79: Introduced safe harbor provision providing immunity to intermediaries from certain liabilities.

Date

Q9] What is IT Act of India 2000 & Explain in detail.

⇒ The Information Technology (IT) Act of India 2000 is a law in India that focuses on managing electronic transactions, digital communication, and cyber security. It was introduced to regulate the use of computers, the internet and related technologies ensuring legal recognition of online activities and addressing crimes related to them.

- It is India's first law to handle issues like hacking, identity theft, online fraud and data protection.

Why it was introduced :-

Before 2000, there were no specific laws in India for online activities, making it difficult to deal with cybercrimes and e-commerce issues. It is introduced to

- Give legal recognition to electronic documents and signatures.
- Handle online fraud, hacking and other cybercrimes
- Promote safe and secure electronic communication and transactions.

Features :-

1] Legal Recognition of Electronic Records :-
- Digital documents considered valid like paper document.

2] Digital Signatures :-
- Way to verify and authenticate online transaction.

3] Cybercrime Regulations :-
- Act defines and penalize various cybercrimes like hacking, identity theft and phishing.

4] E-Governance support :-
Allows government agencies to use electronic records and digital signatures.

5] Regulation of cyber activities :-
Establishes guidlines for safe use of internet, ensuring online security

6] Cyber Appellate Tribunal :- A special tribunal was created to resolve dispute related to online activities and transaction.

Q10) Elaborate the global perspective of cyber crimes.

⇒ Cyber crime:- Any unlawful act being performed by an individual against indian legal system using an electronic device and which is liable for punishment under IT Act of India is called cyber crime.

Global Impact:-

- Cyber crimes costs the global economy billions annually, disrupting business and governments.
- They harm national security by attacking important systems like power grids or defence.
- People's personal information get stolen and leading to misuse like identity theft or cyber defamation.

Challanges:-

- Cyber crimes happens accross countries, making it hard to catch the criminals.
- Different countries have different laws which slows down the investigation.
- Criminals use advanced tools and techniques to hide their identity.

For stopping cybercrimes:-

- Countries should work together with agreements like the budapest convention.
- Agencies like interpole helps nations fight cyber crimes together.
- We have to use better technology to prevent the cyber crimes.