

① What are the key elements of Cyber Security?

⇒ Key elements of Cyber Security :-

- (i) Application Security
- (ii) Information Security
- (iii) Network Security
- (iv) Disaster Recovery Planning
- (v) Operational Security
- (vi) End-User Security.

② Classify Cyber Crime.

⇒ Cyber Crime :- Cyber ~~crime~~ crime on a computer-oriented crime. is a crime that includes a computer and a network. Computers may have been used in the execution of a crime or it may be the target.

Classification:-

- ↳ Cyber Terrorism
- ↳ Cyber Extortion
- ↳ Cyber Warfare
- ↳ Internet Fraud
- ↳ Cyber Stalking

③ What is Phishing?

⇒ Phishing is a Cyber crime that leverages deceptive emails, websites, and text messages to steal confidential personal and corporate information.

④ What is Pharming?

⇒ Pharming is a Scamming practice in which malicious code is installed on a personal computer (PC) or server, misdirecting users to fraudulent website without their knowledge or consent.

⑤ What is the full form of ITA-2000?

→ Information Technology Act, 2000.

⑥ What is a Trojan Horse?

→ A Trojan Horse is a type of malware that disguises itself as legitimate software or files to trick users → into installing it on their devices. Once installed, it can perform various malicious activities, such as ~~stealing~~ stealing sensitive information, damaging files, or allowing unauthorized access to the device.

⑦ What are active attacks?

→ Active attacks -

An active attack could be a network exploit during which the attacker will modify or alter the content and impact the system resources. It will cause damages to the victims.

Active attacks are -

- ① ↳ Modification of messages
- ↳ Denial of Service
- ↳ Trojan Horse

↳ masquerade :- Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data.

⑧ What are passive attacks?

→ Passive attacks

A passive attack attempts to monitor, observe ~~and~~ or make use of information from the system but ~~not~~ does not affect system resources.

→ Eavesdropping attack - Where an attacker listens in on network traffic to collect → sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

→ Leakage of message - Telephonic → Conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

~~Example~~

⑨ Explain Cyber Terrorism with a suitable example.

→ Cyber terrorism (also known as digital terrorism) is defined as disruptive attacks by recognized terrorist organizations against computer systems with the intent of generating alarm, panic, or the physical disruption of the information system.

Examples of Cyber terrorism

→ Introduction of viruses to vulnerable data networks.

→ Hacking of servers to disrupt communication and steal sensitive information.

→ Defacing websites and making them inaccessible to the public thereby causing inconvenience and financial losses.

→ Attacks on financial institutions to transfer money.

(10) What is Cyber Law? Write its advantages and disadvantages.

2) Cyber Law

Cyber Law also called IT Law is the law → regarding information - technology including computers and the Internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

Advantages:-

- (i) Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- (ii) ~~Legal~~ Digital Signatures have been given legal validity and sanction in the Act.
- (iii) The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
- (iv) Cyber Law provides both hardware and software security.

Disadvantages:-

- (i) Ambiguous Terms - Important terms in the law are not clearly defined. This is dangerous as it may have various degrees of interpretation.
- (ii) Threatens Freedom of Speech - The ambiguity of the provisions, particularly the online libel, can cause people to be wary of what they say online. The exposition of the truth may be seen as libellous, depending on the way it is treated.

(iii) Maintenance of the Law The implementation and execution of the cybercrime law would cost much higher. The cyber crime law, deals with delicate subject → matters, and ~~do~~ must be handled with balance and objectivity in order to make it work.

(11) What is Salami Attack

⇒ A Salami attack is a cybercrime that attackers typically use to commit financial crimes. Criminals steal money or resources from financial accounts on a system one at a time. This attack occurs when several minor attacks combine to form a powerful attack. Because of this type of cybercrime, these attacks frequently go undetected. Anyone guilty of such an attack faces punishment under Section 66 of the IT Act.

(12) Discuss about email spoofing and email spamming.

⇒ Email Spoofing :-

• Email Spoofing is creating and sending an email with a modified sender's address. The sender's address is forged in such a way that the receivers will trust the email, thinking it has been sent by someone they know or from any trusted official source. ~~After gaining~~ After gaining their trust ~~at~~ through a forged address, the attackers can ~~take~~ ask for sensitive information, such as personal data like bank details, social security numbers, or organizational data like trade secret and more.

(P.T.O)

Email Spamming

Email spam, also known as junk email, refers to unsolicited email messages, usually sent in bulk to a large list of recipients. Spam can be sent by real humans, but more often, it is sent by a botnet, which is a network of computers infected with malware and controlled by a single attacking party.

Q13) Write down the steps to register a patent in India.

→ Step 1: Patent Search

Patent search is the first step of patent filing procedure in India and is conducted worldwide to determine the novelty of an invention.

Step 2: Drafting Patent Specifications

After conducting thorough searches worldwide, the specification of the invention is written in a techno-legal language with or without the inventor's claims. Without claims is the provisional specification ~~the~~ and with claims is the complete specification.

Step 3: Patent application Filing

After drafting the patent specification, we can begin the procedure for filing Patent Application in India. As we discussed earlier, Patent applications can be provisional or complete, based on the specifications drafted. The drafted provisional or complete specification is filed in Form-2 while Patent Application Form is filled in Form-3 as prescribed by the Indian Patent Act.

Step 4b Patent Publication for Public Opposition

Once the patent application process is complete, then after the expiry of 18 months from the date of patent filing or date of priority whichever is earlier, the patent is published in an official journal and is open for public viewing and inspection. This provides an opportunity to the general public to raise an objection to the patent on ~~step 5b~~ valid grounds.

Step 5b Requesting Patent Examination

The patent application is examined only when a request for examination has been filed. The request for examination has to be filed within 48 months of the patent filing date or date of the priority. The patent examiner examines a patent application and issues an examination report.

Step 6b Grant of a Patent

All the objections to the examination report have been replied to and the examiner is satisfied with the reply of the applicant, the application is put in order for grant of patent registration. This marks the end of the procedure for registration of Patent.