Mains Practice Question

Q. Discuss different types of cybercrimes and measures required to be taken to fight the menace. (UPSC GS-3 Mains 2020)

16 Feb, 2021 GS Paper 3 Science & Technology

Approach

- Start the answer by briefly discussing what do you mean by cybercrimes.
- Discuss various types of Cybercrimes and measures required to tackle them.
- Conclude suitably.

Introduction

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. Today, Cybercrimes are at an all-time high, impacting individuals, businesses, and countries.

Body

Types of Cybercrime

- **Distributed Denial-of-Service (DDoS) Attacks:** These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources.
- **Botnets:** Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets.
- **Identity Theft:** This cybercrime occurs when a criminal gains access to a user's personal information or confidential information and then tries to tarnish reputation or seek a ransom.
- **Cyberstalking:** This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites, and search engines to intimidate a user and instill fear.
- **Phishing:** It is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Measures To Tackle Cybercrime

- **Need for Massive Cybersecurity Awareness Campaign**: In order to proactively deal with cybercrime, the governments need to carry out a massive cybersecurity awareness campaign, regarding cyber frauds, use strong, unique passwords, being careful using public wi-fi, etc.
- **Need for Data Protection Law:** In the 21st century, Data is referred to as the new currency. Thus, there is a requirement for a stringent data protection regime.
    - In this context, the European union's General Data Protection Regulation and India's Personal Data Protection Bill, 2019 are steps in the right direction.

- **Need for Collaborative Trigger Mechanism:** For developing countries like India where the citizenry is more vulnerable to cybercrime, there is an urgent need for a collaborative trigger mechanism.
    - This mechanism would bind all parties and enable law enforcers to act quickly and safeguard citizens and businesses from a fast-growing menace.
    - In this context, the Indian Cyber Crime Coordination Centre will assist in centralizing cybersecurity investigations, prioritize the development of response tools and bring together private companies to contain the menace.

Conclusion

Given the dependence of information technology in the present era, the need of the hour for the governments is to develop core skills in cybersecurity, data integrity and data security fields while also setting stringent cybersecurity standards to protect banks and financial institutions.