Defence & Security · GS - III

Discuss different types of cybercrimes and measures required to be taken to fight the menace.

EXAM YEAR	PAPER	SUBJECT
2020	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Phishing; identity theft; ransomware; financial fraud; cyberstalking; critical infrastructure attacks; cyber hygiene; law enforcement; CERT-In; cybersecurity awareness; international cooperation

Model Answer

Introduction

Cybercrime involves unlawful activities in which computers, digital networks or electronic data are the target or means of committing an offence. Increasing digital dependence has expanded the scale and sophistication of cyber threats.

Major types of cybercrime

- **Financial fraud:** Online banking fraud, payment scams and unauthorised transactions cause financial losses.
- **Phishing and identity theft:** Fraudulent messages and websites deceive users into revealing passwords, personal data or financial details.
- **Malware and ransomware:** Malicious software steals information, disrupts systems or encrypts data to demand payment.
- **Cyberstalking and harassment:** Digital platforms may be used for threats, intimidation, impersonation and non-consensual sharing of private material.

- **Data breaches:** Unauthorised access to personal, corporate or government information undermines privacy and security.
- **Critical infrastructure attacks:** Cyberattacks on power, telecommunications, transport or financial systems can disrupt essential services.
- **Disinformation and online exploitation:** Digital platforms can facilitate coordinated manipulation and other forms of unlawful exploitation.

Measures to combat cybercrime

- Strengthen cybercrime investigation units, digital forensics and specialised training.
- Improve implementation of the Information Technology Act and relevant criminal laws.
- Strengthen CERT-In's incident-response coordination and timely reporting.
- Promote multifactor authentication, secure software, encryption and regular security updates.
- Conduct public awareness campaigns on phishing, suspicious links and safe digital payments.
- Establish effective reporting and victim-support mechanisms.
- Improve international cooperation because cybercriminals frequently operate across jurisdictions.

Conclusion

Cybersecurity requires coordinated action by governments, businesses and citizens. Strong enforcement, resilient digital infrastructure and widespread cyber awareness are essential to protect India's increasingly digital economy.