

WRAP Exams · wrapexams.com

Prelims PYQ, Mains model answers, and copy evaluation. Write to the desk for this paper, a doubt, or the AI waitlist.

ask@wrapexams.com · +91 85951 84903 · wrapexams.com

Q9

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

UPSC Civil Services Mains 2020 · GS III · 10 marks · Cyber Security and Money Laundering

Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention.

Core demand of the question

- Discuss different types of cybercrimes and measures required to be taken to fight the menace
- Keep the explanation within a 10-mark length

Revision summary

Cybercrime targets persons, money, computers, and critical infrastructure, often in mixed form.

Phishing, UPI fraud, ransomware, CSAM, and CII attacks are the live Indian set.

IT Act plus ordinary criminal law, CERT-In, NCIIPC, I4C, and RBI rules are the state toolkit.

Backups, MFA, platform duty, and forensic capacity are the practical layer.

Most retail cases are social engineering, so literacy is a security control.

Introduction

Cybercrime is offence in which a computer or a network is the target, the tool, or the scene of evidence. In India it rides cheap smartphones, UPI, and social media. Types differ; the fight has to mix criminal law, CERT-In, banks, and public habit - not only a new section in the IT Act.

Body**Types**

- **Against persons:** phishing, SIM-swap, OTP fraud, sextortion, cyberstalking, morphing, and child sexual-abuse material online.
- **Against property and finance:** ransomware, business-email compromise, credit-card and UPI fraud, crypto-enabled laundering, and theft of intellectual property.
- **Against the State and infrastructure:** website defacement, DDoS, espionage, attacks on CII (power, finance, telecom), and information operations.
- **Against computers themselves:** malware, botnets, supply-chain compromise.
- **Intermediary-enabled harms:** fake news for riot, terror recruitment, and drug or arms markets on encrypted apps - crime that is social but cyber-delivered.

Legal and institutional measures

- **IT Act, 2000 (with 2008 amendments):** unauthorised access, data theft, impersonation, child pornography provisions; IPC/BNS for cheating, defamation, sexual

offences that merely use a phone.

- **Indian Computer Emergency Response Team (CERT-In)** for incident response and directions; **NCIIPC** for designated critical information infrastructure.
- Police **cyber cells**, the **I4C** (Indian Cyber Crime Coordination Centre), and the national cybercrime reporting portal.
- **RBI** and NPCI rules for payment fraud, two-factor authentication, and bank liability frameworks.
- **International:** MLATs, Interpol, and cooperation even where India is cautious about the Budapest Convention's politics.

Technical and social measures

- **Hygiene:** updates, MFA, segmented networks, backups against **ransomware**, and no internet-facing SCADA.
- **Platform duty:** faster takedown of CSAM and fraud pages; KYC on wallets; audit of large intermediaries.
- **Literacy:** most retail crime is social engineering. School and bank campaigns matter more than a new firewall logo.
- **Capacity:** trained magistrates and forensic labs so **Section 65B** evidence actually convicts.
- **Supply chain:** trusted telecom gear and software bills of materials for government and CII.

Flow diagram

Types -> Person fraud abuse
Types -> Finance ransomware
Types -> State CII
IT Act CERT-In I4C -> Response
Hygiene literacy MFA -> Response

Conclusion

Cybercrime ranges from OTP theft to **ransomware** on a grid. Fighting it needs the IT Act and IPC together, **CERT-In** and **I4C**, payment-system rules, and a public that does not type an OTP to a stranger. Technology without investigation and literacy will not close the menace.

Facts & figures

IT Act, 2000

Principal special law for computer offences, intermediaries, and CERT-In's statutory footing.

CERT-In

National cyber incident response agency; issues directions to service providers.

I4C

Indian Cyber Crime Coordination Centre under MHA for police coordination and the reporting portal.

NCIIPC

Protects designated critical information infrastructure under the IT Act framework.

Ransomware

Malware that encrypts data for ransom; needs backups and segmented nets, not only a payment ban.

WRAP Exams · Write. Read. Analyse. Practice. · <https://wrapexams.com/upsc/mains-answers/gs-3/2020/discuss-different-types-of-cybercrimes-and-measures-required-to-be-taken-to-fight-the-menace/> · ask@wrapexams.com · wrapexams.com

WRAP Exams