Helpline for Cyber Fraud

Why in News

The **Ministry of Home Affairs** has operationalised the **national Helpline 155260** and **Reporting Platform for preventing** financial loss due to **cyber fraud.** The helpline was **soft-launched on 1st April.**

- The National Helpline and Reporting Platform **provides a mechanism for persons cheated in cyber frauds** to report such cases to prevent loss of their hard earned money.
- Also, a **National Cyber Security Strategy 2020** is being formulated by the Office of National Cyber Security Coordinator at the National Security Council Secretariat.

Cyber Security

- **Cyber Security** is **protecting cyber space** including critical information infrastructure from attack, damage, misuse and economic espionage.
- **Critical Information Infrastructure:** According to **Section 70(1) of the Information Technology Act,** CII is defined as a “computer resource, the incapacitation or destruction of which, shall have **debilitating impact on national security, economy, public health or safety”.**
- **Cyber Fraud:** It is the crime committed via a computer **with the intent to corrupt another individual’s personal and financial information** stored online.
    - It is the most common type of fraud and individuals and organisations need to be vigilant and protect their information from fraudsters.

Key Points

- **About:**
    - The helpline has been made **operational by the Indian Cyber Crime Coordination Centre (I4C),** in coordination with the **Reserve Bank of India**, all major banks, **payment banks**, wallets and online merchants.
    - The **Citizen Financial Cyber Fraud Reporting and Management System** has been developed by I4C to integrate Law Enforcement Agencies and Banks and Financial Intermediaries.
    - The facility **empowers both the banks and the police,** by leveraging new-age technologies **for sharing online fraud related information** and taking action in almost real time.
    - Since its soft launch, in a short span of two months, the helpline has assisted in saving **more than Rs 1.85 crore.**
- **Indian Cyber Crime Coordination Centre:**
    - The scheme to **set up I4C** was approved **in October 2018,** to deal with all types of

cybercrimes in a comprehensive and coordinated manner.
    - It has **seven components:**
        - National Cyber Crime Threat Analytics Unit
        - **National Cyber Crime Reporting Portal**
        - National Cyber Crime Training Centre
        - Cyber Crime Ecosystem Management Unit
        - National Cyber Crime Research and Innovation Centre
        - National Cyber Crime Forensic Laboratory Ecosystem
        - Platform for Joint Cyber Crime Investigation Team.
    - 15 States and Union Territories have given their consent to set up Regional Cyber Crime Coordination Centres.
    - This state-of-the-art Centre is **located in New Delhi.**
- **Other Initiatives to Tackle Cybercrime:**
    - **Draft Personal Data Protection Bill**, 2018 (based on the recommendation of **Justice BN Srikrishna Committee**) to secure citizens data.
    - **Cyber Swachhta Kendra:** The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's **Digital India initiative** under the Ministry of Electronics and Information Technology (MeitY).
    - Indian Computer Emergency Response Team (CERT**-IN)**: It is an organisation of the MeitY, with the objective of securing Indian cyberspace. It is the nodal agency which deals with cybersecurity threats like hacking and phishing.
- **Related International Convention (Budapest Convention):**
    - The **Council of Europe’s (CoE) Cybercrime Convention,** also known as the Budapest Convention is the sole legally binding international multilateral treaty on cybercrime. It coordinates **cybercrime investigations between** nation-states and criminalizes certain cybercrime conduct.
    - It was opened for **signature in 2001** and came into **force in 2004.**
    - The Budapest Convention is supplemented by a **Protocol on Xenophobia and Racism** committed through computer systems.
    - India is **not a party** to it. India recently **voted in favour of a Russian-led UN resolution** to set up a separate convention. The resolution seeks to set up new cyber norms considered as a counter alternative to the US backed Budapest Accord.

Source: TH

PDF Refernece URL: https://www.drishtiias.com/printpdf/helpline-for-cyber-fraud