WhatsApp “Ghost Pairing” Cyber Fraud

Published On: 23-12-2025

Subject Reference: GS Paper III (Internal Security - Cyber Security)

- **The News (Dec 2025):** MeitY and **CERT-In** issued a high-level advisory regarding "Ghost Pairing." Unlike traditional scams that require an OTP, this technique tricks users into linking a hacker's device to their WhatsApp account using a legitimate "pairing code."
- **Apt Topic: "Social Engineering & The Evolution of Cyber-Enabled Crimes"**
- **The Modus Operandi:** It exploits the **Companion Mode** feature. Attackers send a fake link (e.g., "View this photo") that leads to a phishing site. This site prompts the user to enter a code, which secretly authorizes the attacker’s browser as a "linked device."
- **The "Ghost" Element:** Once linked, the attacker can read, send, and delete messages in real-time, often without the user knowing for months, as the original device remains active.
- **Internal Security Relevance:** Discuss the need for **Digital Literacy** as a defense mechanism and the role of the **National Cybercrime Reporting Portal (NCRP)**.