Bluebugging

Why in News?

Several smartphones have their Bluetooth settings on discovery mode as it is a default setting, making it vulnerable to **bluebugging.**

What is Bluebugging?

- **About:**
  - It is a **form of hacking** that lets attackers access a device **through its discoverable Bluetooth connection.**
  - A hacker can gain unauthorized access to these apps and devices and control them as per their wish through bluebugging.
  - Any **Bluetooth-enabled device** including True Wireless Stereo (TWS) devices or earbuds are susceptible to bluebugging.
  - Once a device or phone is bluebugged, **a hacker can listen to the calls, read and send messages and steal and modify contacts.**
  - Even the most secure smartphones like iPhones are vulnerable to such attacks.
- **Preventive Measures:**
  - Turning off Bluetooth and disconnecting paired Bluetooth devices when not in use.
  - Making Bluetooth devices undiscoverable from Bluetooth settings.
  - Updating the device's system software to the latest version.
  - Limited use of public Wi-Fi.
  - Watch out for suspicious activities on your device.
  - Monitoring of sudden spikes in data usage.
  - Usage of modern anti-virus software.

What are the Related Government Initiatives?

- **Cyber Surakshit Bharat Initiative**
- **Cyber Swachhta Kendra**
- **Online Cybercrime Reporting Portal**
- **Indian Cyber Crime Coordination Centre (I4C)**
- **National Critical Information Infrastructure Protection Centre (NCIIPC)**
- **Information Technology Act, 2000**
- **National Cyber Security Strategy 2020**

UPSC Civil Services Examination, Previous Year Question (PYQ)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Exp:

- According to section 70B of the Information Technology Act, 2000 (IT Act), the Union Government by notification should appoint an agency named Indian Computer Emergency Response Team (CERTIn) to serve as the national agency for incident response.
- The Union Government under section 70B of the IT Act, 2000 established and notified rules of CERT-In in 2014. According to Rule 12(1)(a), it is mandatory for service providers, intermediaries, data centers and corporate bodies to report cyber security incidences to CERT-In within a reasonable time of occurrence of the incident. **Hence, 1, 2 and 3 are correct.**
- **Therefore, option D is the correct answer.**

Source: TH