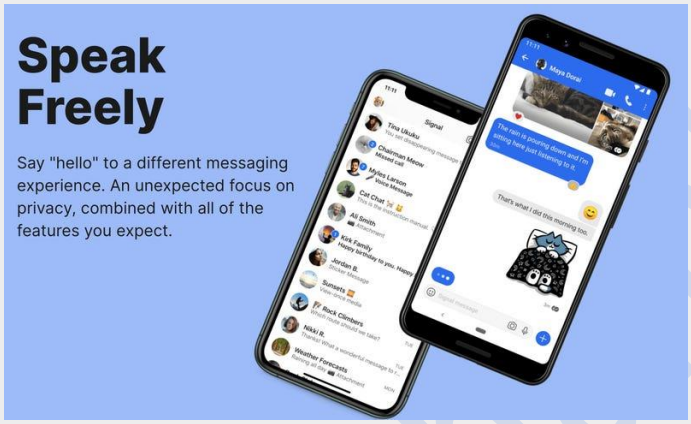
1. Signal: encrypted messaging application

What is Signal?
Signal is an end-to-end encrypted messaging application, regarded as one of the most secure in its category. Experts have lauded the app for its openly available code, allowing them to verify its security in real time.

In theory, all private conversations and calls made by its users cannot be accessed by the service provider. The app collects limited user data. It also has a feature that allows for automated message deletion within a certain time frame. All a user has to do is register with their phone number.



Why in news?
Recently, Editor in Chief of The Atlantic magazine, Jeffrey Goldberg, said he was accidentally added to a group chat on the app with top leaders of the Trump administration.

In an essay, he described how he became privy to sensitive communications about the government's plans to attack the Houthis of Yemen earlier this month. The group chat included US Vice President JD Vance, Defence Secretary Pete Hegseth and National Security Adviser (NSA) Michael Waltz.

How did such a thing even happen?
Goldberg recounted that he received a connection request on the app from Waltz on March 11, and accepted it. Two days later, he was added to the "Houthi small group" on Signal.

While he doubted its authenticity and suspected a larger disinformation campaign was at play, he received classified information about the details of the attack and the targets on the chat. Following news reports of the first attack on Yemen, Goldberg realised the group chat was, in fact, very real.

Why is this a big deal?
Sensitive information should have been relayed in person in a Secure Compartmented Information Facility (SCIF) devoid of the use of any electronic devices. Alternately, a secure official communication channel should have been designated for the task.

The use of Signal bypasses a 2023 memo issued by the US Department of Defense, which had designated Signal as an "unmanaged" messaging app. Unmanaged apps are those "NOT authorized to access, transmit, process non-public DoD information."

Managed apps, as designated by the memo, run on enterprise management systems, which "can enforce controls on the application and data in a way that can reduce the risk of data compromise or exposure/spillage of data to unmanaged applications."

The use of Signal also exposes officials to the threat of hacks. In February, Mandiant, a Google-owned security firm, reported that Russian-linked spies tried to hack into the Signal accounts of Ukrainian military officials by posing as trusted Signal contacts.

Since Signal cannot be downloaded on official devices, personal devices were likely used. The issue of data storage also matters: Signal, like other messaging apps, can be accessed on other devices, allowing data to be stored locally on them. These devices face the risk of hacking and malware, regardless of the app's own security.

Relevance: GS Prelims; Science & Technology
Source: Indian Express

2. National Pest Surveillance System

Introduction

The National Pest Surveillance System (NPSS) has been launched on 15th August, 2024 by the Hon'ble Union Minister of Agriculture and Farmers Welfare to enhance the surveillance and management of pest diseases across the country.

How does System work?

The system utilizes latest digital technologies such as Artificial Intelligence and Machine Learning (AI and ML) to provide quick and instant solution regarding pest attacks, crop diseases, crop damages etc. by issuing real time crop protection advisory to the farmers. It includes a user-friendly mobile app and a portal for identification of pests and disease mitigation.

Use of NPSS

NPSS is being used by the farmers across the country for identification of pests and diseases in 61 crops and pest management advisories for 15 major crops namely cotton, paddy, wheat, maize, pigeon pea, moong, soyabean, sugarcane, brinjal, tomato, apple, banana, grapes, pomegranate. NPSS is currently available in four languages namely English, Hindi, Marathi and Punjabi. So far, 10154 pest management advisories have been issued through NPSS for the benefit of farmers.

Relevance: GS Prelims
Source: PIB

3. Sahyog Portal

Objective
'Sahyog' Portal has been developed to automate the process of sending notices to intermediaries by the Appropriate Government or its agency under IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act. This portal will help achieve a clean cyber space for the Citizens of India.

Functioning
It will bring together all Authorized Agencies of the country and all the intermediaries on one platform for ensuring immediate action against the unlawful online information. In its second phase, the portal's functionality will be extended to also send information requests from law enforcement agencies.

Ministry involved
The SAHYOG portal is being developed by the Union Ministry of Home Affairs. Indian Cybercrime Coordination Centre (I4C) is the nodal agency behind development of SAHYOG portal.

Indian Cybercrime Coordination Centre
Indian Cybercrime Coordination Centre (I4C) was established by MHA, in New Delhi to provide a framework and eco-system for Law Enforcement Agencies (LEAs) for dealing with Cybercrime in a coordinated and comprehensive manner.

I4C is envisaged to act as the nodal point to curb Cybercrime in the country.

Intermediaries on board
So far, 38 intermediaries have already come on board the SAHYOG portal, including Telegram, Apple, Google, LinkedIn, YouTube, Microsoft, Facebook, Instagram, and WhatsApp.

Relevance: GS Prelims; Governance
Source: The Hindu