CURRENT AFFAIRS   1st Sep. 2022

NATIONAL NUTRITION WEEK 2022: 1ST TO 7TH SEPTEMBER

In India, the first week of September every year is celebrated as National Nutrition Week. The week is observed every year from September 1-7. The purpose of this week is to raise awareness among the general public about the value of healthy eating practices and proper nutrition for upholding a healthy lifestyle. The government launches programmes to promote nutrition awareness throughout this week.

National Nutrition Week 2022: Theme

The theme for this year is Celebrate a "World of Flavors". Every year, as part of National Nutrition Week, the government also introduces a special theme that focuses primarily on that year's theme. Last year, the government announced this theme for the week – feeding smart right from start.

National Nutrition Week 2022: Significance

National Nutrition Week is commemorated to educate people about healthy and nutritious food. The Food and Nutrition Board of the Government of India's Ministry of Women and Child Development organises an annual week-long celebration of National Nutrition Week to inform people about this basic phenomenon. The importance and role of a healthy diet in the human body are emphasised. A balanced diet full of essential nutrients is essential for healthy development and function. The Indian government has started programmes that emphasise good nutrition, wholesome food, and a healthy lifestyle.

National Nutrition Week: History

The National Nutrition Week was established in 1975 by the members of the American Dietetic Association (ADA), now known as the Academy of Nutrition and Dietetics. This week was set aside to raise awareness among the general public of the value of good nutrition and the need for an active lifestyle. Due to the positive reception from the masses, the celebration of this week in 1980 stretched for a whole month. At that period of time most of the people in India were suffering from the problem of malnutrition. In 1982 National Nutrition Week was first time introduced in India.

AUTOBIOGRAPHY TITLED "THE HERO OF TIGER HILL" AUTHORED BY SUBEDAR MAJOR YADAV

The autobiography **"The Hero of Tiger Hill: Autobiography of a Param Vir",** is about the inspiring story of **Subedar Major (Honorary Captain) Yogendra Singh Yadav (Retd),** the Youngest Param Vir Chakra (PVC) awardee, at the age of 19 for his actions in the 1999 Kargil conflict. This autobiography is published by **Srishti Publishers & Distributors.**

About the book

Subedar Major Yadav's idea in writing about him began when he was invited to the top colleges in India, he noticed that his simple but honest answers made a lot of impact on young students. His motive in writing the autobiography is to motivate youngsters of India and infuse a sense of patriotism. The book was mainly focused on the night of **July**
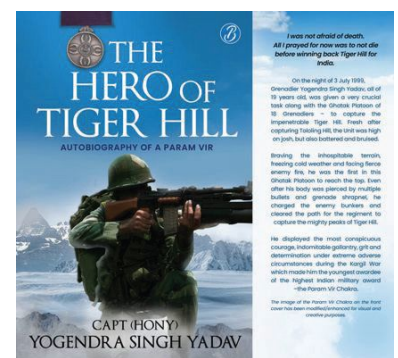
3, 1999, 19 years old Yadav was given a crucial task with the Ghatak Platoon of 18 Grenadiers Regiment in order to capture the Tiger Hill.
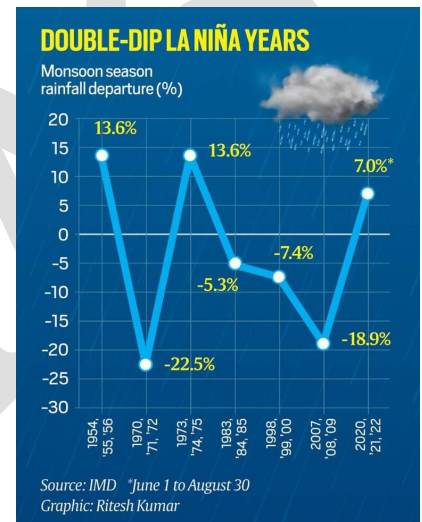
LA NINÃ CONDITIONS ENTER 3RD YEAR, 6TH TIME SINCE 1950

In what may be termed as an uncommon phenomenon, **La Ninã conditions** prevailing over the equatorial Pacific Ocean since September 2020 has entered the third year. There are only six instances of La Ninã lasting for more than two years since 1950s, **data with the India Meteorological Department (IMD) show**.

La Ninã is when the sea surface temperatures (SSTs) along the central and equatorial Pacific Ocean are colder than normal, which, experts say, favour the Indian summer monsoon. However, La Niña years are also infamous for frequent and intense hurricanes and cyclones in the Atlantic Ocean and the Bay of Bengal.

About La Niña

 La Niña (known as little girl) is a weather pattern that occurs in Pacific Ocean. It is observed when sea surface temperatures (SSTs) in Eastern Equatorial Pacific (EEP) get comparatively colder than normal. This results in a strong high pressure over EEP (i.e. tropical west coast of South America). It is counterpart to El Niño (known as little boy or Christ Child), which is characterized by unusually warm SSTs in EEP and causes suppressed Monsoon. Together, La Niña and El Niño are "cold" and "warm" phases of El Nino-Southern Oscillation (ENSO), which involves temperature changes in waters of Eastern and Central Pacific Ocean. Generally, El Niño and La Niña occur every 4 -5 years. El Niño is more frequent than La Niña.

DOUBLE-DIP LA NIÑA YEARS
Monsoon season rainfall departure (%)

13.6%   13.6%   7.0%*
-22.5%   -5.3%   -7.4%   -18.9%

1954, '55, 56 | 1970, '71, '72 | 1973, '74, '75 | 1983, '84, '85 | 1998, '99, '00 | 2007, '08, '09 | 2020, '21, '22

*Source: IMD   *June 1 to August 30*
Graphic: Ritesh Kumar

Impact of La Niña

Better monsoon rains in India. Frequent and intense hurricanes and cyclones in Atlantic Ocean and Bay of Bengal. Causes drought in Peru and Ecuador, heavy floods in Australia, high temperatures in Western Pacific, Indian Ocean, off Somalian coast.

CYBER THREAT TO MOBILE BANKING

Why in News?

According to a recent study, more people are inclining toward digital payments and there is a rise in the number of people's interactions with their bank or bank accounts happen through their smartphones.

- Further, this acceleration brings along with it a vulnerability: an increased threat of cyberattacks on mobile devices.

What are Cyber Threats?

- About:
  - A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. It includes computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

- Different Types:
  - Malware: Malware short for malicious software refers to any kind of software that is designed to cause damage to a single computer, server, or computer network. Ransomware, Spy ware, Worms, viruses, and Trojans are all varieties of malware.

- o Phishing: It is a method of trying to gather personal information using deceptive e-mails and websites.

- o Denial of Service attacks: A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

- o Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

- o Social engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

What are the Issues of Cyber Threats on Mobile Banking?

- ▪ **Increasing Cyber Attacks:**

- o A study by cyber security firm Kaspersky warns of an increase in cyberattacks on Android and iOS devices in the Asia Pacific (APAC) as more people switch to mobile banking in the region.

- o **Use of Trojans & Malware:**

  - As per Kaspersky, mobile banking Trojans are dangerous malware that can steal money from mobile users' bank accounts by disguising the malicious application as a legitimate app to lure unsuspecting people into installing the malware.

  - For e.g, mobile banking trojan, called Anubis, has been targeting Android users since 2017.

    - Further, its worldwide campaigns have hit users in Russia, Turkey, India, China, Colombia, France, Germany, the U.S., Denmark, and Vietnam.

- o **Methodology:**

  - The perpetrators infect the device through legitimate-looking and high-ranking malicious apps on Google Play, smishing (phishing messages sent through SMS), and BianLian malware, another mobile banking Trojan,

    - Roaming Mantis is another prolific malware targeting mobile banking users.

    - The group attacks Android devices and spreads malicious code by hijacking domain name systems (DNS) through smishing exploits.

- ▪ **Interoperability issue:**

- o As various payment platforms like Google Pay, PaytM, PhonePe, Square, PayPal, and Alipay have benefited from changes in consumer behaviour by adopting mobile banking.

  - As a result, they have also permanently changed the payments game to their advantage.

- o **Closed Loop Payment System:**

  - These platforms are operating in a closed-loop payment world where a Google Pay user can send money to another bank account via only the search giant's payment platform.

    - It is similar to how Visa and Mastercard operate as they let payment transactions happen only within their own networks, not between each other.

- o **Change in Business Model:**

  - It's driven partly by regulators that prefer open, standardized platforms that lower barriers to entry.

- Some countries are already making payment platform providers change their business models.

    - China, for instance, has ordered its internet companies to offer their rival firms link and payment services on their platforms.

    - In India, a new law demands all licensed mobile payment platforms be capable of providing interoperability between wallets.

  - The push from regulators to make payment platforms interoperable comes at a time when the demand for technical experts is a serious concern in the banking industry.

- **Shortage of Security Experts:**

  o The shortage of technology, engineering, data and security experts needed by banks to realise their digital aspirations tends to hide a much wider problem: banks' appeal as first-choice employers of all kinds of talent have faded.

- **Lack of Adequate Cybersecurity Policy:**

  o The lack of adequate cybersecurity and the dearth of talent in banking could potentially lead to a further rise in cyberattacks on user devices.

    - And until this mismatch is fixed, it helps to be careful and extremely cautious when using a mobile device to make payments.

Way Forward

- Usual practice of digital hygiene like keeping the phone up-to-date and rebooting regularly can be done.

- Further, consumers can ensure that they use their phones for banking only when the device is connected to a secure VPN (VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks) and iOS 16 users can turn on Lockdown Mode as it limits the device's functionality and protects it from any potential malware.