N1. When govt made 21.9mn e-transactions in a day

Hindustan Times. 10 April 2020

*For a team of 16 from the **National Informatics Centre** (**NIC**), the brief was clear-- prepare for an avalanche of online transactions on the Public Financial ...*

A senior official at NIC said on condition of anonymity that between March 24 and 31, there were 72 million transactions hosted on the system, more than double of the 34.4 million transactions during the same period that the PFMS hosted in 2019.

While there is no clarity on the amount of money transacted during that period, an indication is that on April 9 alone Rs 2004 crore was sent across the network.

On March 30, six days after the prime minister announced a 21-day lockdown in India, the government set a new record : officials across departments carried out 21.9 million financial transactions online, the highest in a single day.

The financial year was coming to a close and many to vendors and beneficiaries of welfare schemes had to be sent out in the last week of March and the first two weeks of April (CHECK) . For a team of 16 from the National Informatics Centre (NIC), the brief was clear-- prepare for an avalanche of online transactions on the Public Financial Management System or PFMS.

A senior official at NIC said on condition of anonymity that between March 24 and 31, there were 72 million transactions hosted on the system, more than double of the 34.4 million transactions during the same period that the PFMS hosted in 2019.

While there is no clarity on the amount of money transacted during that period, an indication is that on April 9 alone Rs 2004 crore was sent across the network.

Many of the the transactions were towards PM Kisan, the cash payout scheme for farmers. "Of the 21.9 million transactions on March 30, 19.7 million were direct benefit transfers for PM Kisan," said the official.

The payouts for PM Kisan, a scheme under which farmers get Rs 2000 every four months, have always mostly happened online. The scheme was launched last year in February. The challenge for NIC this time, however, was to ensure that payments are validated and sent out to the 80 million beneficiaries of the scheme by officers from their homes. And that, in doing so, the officers do not face technical problems at their end.

All of these transactions were hosted on a management information system (MIS), developed by the NIC sometime in 2013. Known as the Public Financial Management System (PFMS) and accessible online, the software application in its earlier avatar was known as the Central Plan Scheme Monitoring System (CPSMS). It was aimed to bring in transparency to government programs.

The application is available on work computers in all government offices through a virtual private network (VPN). The first challenge, the official added, was to ensure that all designated officers had access to it from their homes.

In every ministry, only certain officials can greenlight payments and funds transfers. And before the lockdown, most of the permissions were given out on paper, hand-delivered by a network of clerks.

However, for times like these when physical signatures cannot be accessed, the system has the option of digital signatures, which designated officials can issue from the system online. To access them, a designated officer needs to enrol at the PFMS portal through a Digital Signature Certificate enrolment module and validate credentials.

Nagesh Shastri, deputy director general of the NIC said that apart from direct benefits transfer, other payments made trough the system include funds sent to states and implementing agencies. "The system is integrated with core banking and 400 banks, including the postal bank network, is linked to the system," said Shastri.

Shastri said that the most common problem faced by officials had to do with authorisations of digital certificates. They were all worked out, he added. "o keep it secure, NIC used only its own infrastructure; the central database of the PFMS is in Hyderabad.

News Source: https://www.hindustantimes.com/india-news/when-govt-made-21-9mn-e-transactions-in-a-day/story-O6ebyIknRQ93MmM35mB8OL.html

N2. Software glitches delay salaries, govt draws flak from SAD, AAP

National Informatics Centre (NIC) is operating the new IFMS. Seeking immediate measures to resolve the problem, Punjab civil secretariat staff ...

Chandigarh: The Punjab government has repeatedly announced to give full pay to all its employees, but many of them are still to get salaries for the month of March, with the release delayed by "technical glitches" in a new software.

The state government had introduced an Integrated Financial Management System (IFMS) from April 1 for approval of financial bills, including those related to salaries, and release of payments, after its contract with a private IT firm ended. National Informatics Centre (NIC) is operating the new IFMS.

Seeking immediate measures to resolve the problem, Punjab civil secretariat staff association president Sukhchain Singh Khehra claimed that a large segment of employees who were going out of their homes and performing their duty to contain the spread of coronavirus had been waiting for their salaries, even after nine days.

A finance department official said the government was releasing salaries, but the process was taking extra time due to technical snags in the new system. "Our people and those of the Reserve Bank of India (RBI) are working day and night to remove the glitches and make payments. On Thursday, we released Rs 150 crore for salaries. Banks and government offices did not function for several days this month, due to the financial closing at the start, and then we had some holidays," he added. Unlike several other states which have deferred salaries, Punjab has decided to pay full salaries to all its employees, including contractual and outsourcing ones, for the curfew period.

The opposition Shiromani Akali Dal (SAD), however, flayed the state government for the delay, accusing it of adopting a "callous" attitude towards police personnel, healthcare workers and other frontline workers, fighters against covid-19. "It is unfortunate that in this difficult time, our protectors are not being paid on time by the state government," former minister Bikram Singh Majithia said, asking chief minister Amarinder Singh to intervene and ensure all frontline workers were paid their salaries immediately. Leader of opposition (LOP) Harpal Singh Cheema also urged the CM to ensure that brave hearts fighting coronavirus from the frontlines do not face any difficulty.

News Source: https://www.hindustantimes.com/cities/software-glitches-delay-salaries-govt-draws-flak-from-sad-aap/story-SAqI4l2jWDE5bVYkBBwP3N.html

N3. Zoom lapses: India Inc beefing up cyber-security systems

Financial Express. 10 April 2020

*"We typically use an internal software developed by the **National Informatics Centre**, but some inter-departmental meetings, press interactions were ...*

While Zoom Video Communications CEO Eric S Yuan has apologised for these lapses, India Inc is beefing up cyber-security systems.

"Organisation should consider a risk-based approach in designing a security and privacy framework to address the risk associated with processing of personal data and follow a proactive approach to ensure adequate level of protection," said Manish Sehgal, partner, Deloitte India.

Users of video-conferencing app Zoom, whether they are government bodies, companies or individuals, have discovered they are being "zoombombed". Zoom's lax security features have resulted in meetings being hijacked and there's a fear that data is being leaked. While Zoom Video Communications CEO Eric S Yuan has apologised for these lapses, India Inc is beefing up cyber-security systems.

A large Indian public-sector bank that was using Zoom to interact with the press is now rethinking this strategy. "Because of its popularity, it was an instant decision to have press meetings to disseminate public information on Zoom. But we might review that now," an executive said. The lender currently relies on internal communications systems to communicate regarding sensitive data and does not rely on third parties due to security concerns, another senior executive said.

The Indian central bank, too, steered clear of using Zoom. "We were considering holding a press meeting through Zoom, but decided against it and used already security-tested internal systems instead," an official aware of the matter said. The app's popularity had soared with over 200 million using it daily in March, compared with 10 million in December 2019. But besides "zoombombing", there have been serious concerns raised by international users regarding the privacy of users' data on Zoom. Yuan said the company will be conducting a comprehensive review to understand and ensure the security of users. Despite the recent uproar, many remain nonchalant of the cyber risks involved. Even the Indian arms of global consultancy giants like Bain & Company and Boston Consulting Group continue to extensively use Zoom for internal and client meetings, despite being aware of the risks. "Everyone is using Zoom these days. We have internally shared safety measures that employees should take to avoid zoom-bombing and we continue to update the software," an executive from a top consulting firm said.

The central government has also been using Zoom for some internal meetings and press interactions. "We typically use an internal software developed by the **National Informatics Centre,** but some inter-departmental meetings, press interactions were held on Zoom, recently. There is no directive yet on restricting the usage of the software," a government official told FE. Large volumes of personal data is now stored online as usage of apps and smart devices increase. Companies and individuals must balance privacy with communication needs. "Organisation should consider a risk-based approach in designing a security and privacy framework to address the risk associated with processing of personal data and follow a proactive approach to ensure adequate level of protection," said Manish Sehgal, partner, Deloitte India.

News Source: https://www.financialexpress.com/industry/technology/zoom-lapses-india-inc-beefing-up-cyber-security-systems/1923979/

N4. Covid 19 : TVOS Urge Viewers To Download Aarogya Setu App

Sikkim News-09-Apr-2020

Developed by the National Informatics Centre that comes under the Ministry of Electronics and Information Technology, the app will tell the user if they came ...

Pakyong, 09 April : The Voice of Sikkim Online Digital Media urges all People of Sikkim , Fans and Followers to download AarogyaSetu App for coronavirus COVID-19 updates

Google Play Store Link
https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu

The Voice Of Sikkim , which is North East's largest reached digital media house, has appealed to all connected users to download the newly-launched AarogyaSetu app for the latest updates related to coronavirus COVID-19 pandemic.

As a responsible media , with millions of viewers across the globe, TVOS has been providing accurate and timely updates on the coronavirus-linked cases in the country and abroad.

Through its regular news updates 24×7, TVOS has voiced its full support to all such initiatives taken by the Centre with regard to the coronavirus outbreak in the country and appealed to the countrymen to abide by them in order to contain the further spread of the pandemic.

The Centre on Thursday (April 2, 2020) launched a mobile application – AarogyaSetu – for tracking cases of coronavirus COVID-19 infections. The app has been launched for Android and iOS users. Developed by the National Informatics Centre that comes under the Ministry of Electronics and Information Technology, the app will tell the user if they came near a COVID-19 infected person.

According to the App's description, it is aimed at "augmenting" efforts to "proactively" inform the citizens about the "best practices and relevant advisories pertaining to the containment of COVID-19." Both Centre and state governments have launched a host of coronavirus-related apps over the last few weeks to curb the spread of the pandemic in the country.

AarogyaSetu App will enable people to assess themselves the risk for their catching the coronavirus infection. It will calculate this based on their interaction with others, using cutting edge Bluetooth technology, algorithms and artificial intelligence.

Once installed in a smartphone through an easy and user-friendly process, the app detects other devices with AarogyaSetu installed that come in the proximity of that phone. The app can then calculate the risk of infection based on sophisticated parameters if any of these contacts are tested positive.

The App will help the Government take necessary timely steps for assessing the risk of the spread of COVID-19 infection and ensuring isolation where required. The App's design ensures privacy-first. The personal data collected by the App is encrypted using state-of-the-art technology and stays secure on the phone until it is needed for facilitating medical intervention.

Available in 11 languages, the App is ready for pan-India use from day-1 and has highly scalable architecture.

News Source: http://voiceofsikkim.com/2020/04/09/covid-19-tvos-urge-viewers-to-download-aarogya-setu-app/

M1.   Coronavirus lockdown: National cybersecurity agency asks parents to keep tab on child's Internet activity

Financial Express. 09 April 2020
The national cyber security agency CERT-In has asked all parents in the country to keep monitoring the online activities of their children.

The national cyber security agency CERT-In has asked all parents in the country to keep monitoring the online activities of their children. At a time when children have been using internet services for their entertainment and online classes during the nationwide lockdown which has been imposed to combat Coronavirus, CERT-In believes keeping a check on the online activities will safeguard children from inappropriate content streaming as well as cyber bullying. "The Internet is a good resource for kids to prepare school reports, communicate with teachers and other kids and play interactive games. But online access also comes with risks like inappropriate content, cyber bullying and online predators," the CERT-In said in an advisory.

It is to note that the Computer Emergency Response Team of India (CERT-In) is the federal agency in India that helps combat cyber attacks to guard cyberspace within the country.

Apart from this, the advisory said that the parents should be aware of what their children are watching or listening to on the internet. There are some websites that may pose a threat as they may try to entice children and persuade them to exchange personal information including phone numbers or address. For this, CERT-In has given some guidelines for parents.

CERT-In guidelines for parents

- Devices should be set in the living room and should be accessed in the presence of an adult.
- There should be two-factor authentication for devices and its home screen should be locked with a pin.
- Teach kids how to browse and the content that needs to be looked for in order to maintain appropriate online behaviour.
- It also advised parents to filter content and avoid the chance of the child encountering inappropriate content by mistake
- It asked guardians to add parental control software to family devices.
- The advisory stated that parents should take their child seriously if he or she reports an uncomfortable online exchange.
- Children should also be taught that the internet provides anonymity. Therefore, someone they come in contact with may not be who they think they are.
- CERT-In asked the parents to keep a check on credit card and phone bills as well and look for unfamiliar account charges.

Children have been using the internet more as the schools have started providing online lectures and classes for students as educational institutions are shut pertaining to the spread of Coronavirus in India. Currently, students have been relying on the internet for their studies, entertainment and extra-curricular activities as going out is not an option.

News Source: https://www.financialexpress.com/industry/technology/coronavirus-lockdown-national-cybersecurity-agency-asks-parents-to-keep-tab-on-childs-internet-activity/1923465/

M2. Social sites have to deal with misinformation responsibly: Ravi Shankar Prasad

Economic Times. 10 April 2020

"I appreciate the cooperation of social media platforms, but they must behave responsibly during these times of challenge and stress," said Union Minister for Electronics and IT and Communications Ravi Shankar Prasad.

Along with initiatives around work from home and innovative use of telecom spectrum, incentives worth Rs48,000 crore for the electronics manufacturing sector will play a big role in reviving the economy reeling from the Covid-19 virus outbreak, said Union Minister for Electronics and IT and Communications Ravi Shankar Prasad. In an interview with **ET**, Prasad said that while social media companies have played a commendable role in dealing with the crisis, they need to behave *responsibly in tackling misinformation. Excerpts:*

The PM has asked every ministry for 10 ideas that will help revive the economy after the Covid-19 crisis. What will be your submissions?
We are working on it. One is surely electronics manufacturing; secondly, some great initiatives can be taken on working from home which can lead to more innovation. We can also revisit the spectrum issue. Spectrum can be used to drive a lot of innovation.

You just announced a Rs 48,000 crore push for electronics manufacturing. How will the government go about wooing the big companies?
We are in touch with them and all are very excited. They are waiting for the present situation to ease. Already, we have notified everything.

This is going to be a different world after the Covid-19 crisis. India has to push economic activity in a big way. So, this policy will ensure that it becomes a robust centre of electronics manufa cturing.

How is the government dealing with the issue of videos spreading misinformation about Covid-19 going viral on platforms such as TikTok and WhatsApp?
I appreciate the cooperation of social media platforms, but they must behave responsibly during these times of challenge and stress. I have taken up the matter in a very tough manner with these companies. My simple statement to them was that they have to do the monitoring themselves and encryption can't be (used) as an excuse.

What has been holding back the IT intermediary guidelines, which will address some of these issues?
It is under process. We are looking at finalising them after a final consultation.

The IT industry is seeking several incentives to tide over the current crisis. Are you considering their demands?
We will take all appropriate initiatives that India's robust identity as a good IT services provider and the Digital India initiative require. The IT ministry did a big job by permitting work from home by relaxing norms swiftly; today 85-90% of people are working from home. I have also instructed the department to come up with a policy framework so that work from home becomes a mass movement in India. There is great potential to permit innovation, reduce load on the system and the establishment, taking a cue from the current success of work from home.

What are the ways in which we are leveraging telecom networks during this time?
We are enabling geo-fencing through mobile phones. It is a mobile-based system to monitor the breach of geofencing by Covid-19 infected patients. The moment an infected person breaks his or her quarantine, the system shows an alert, health authorities are informed and the police track the patient.

Arogya Setu is for smartphone users. What about feature phone users?
Today, we launched an Interactive Voice Response Service (IVRS) with the Government of Tamil Nadu. IVRS is for people who don't have smartphones. Arogya Setu and IVRS are taking care of privacy and will be extended to other states as well. The Aarogya Setu app has been downloaded by 2.7 crore people and we are making all efforts to ensure that it is widely used.

Has the quality of telecom services deteriorated?
Our telecom infrastructure is performing to its maximum. Out of 21 lakh Base Transceiver Stations in the country, only 355 today have malfunctioned. BSNL has also surprisingly performed well and I appreciate the good work that the postal department is doing to help the needy and the poor.

News Source: https://economictimes.indiatimes.com/tech/internet/social-sites-have-to-deal-with-misinformation-responsibly-ravi-shankar-prasad/articleshow/75075413.cms

---

Other IT News

O1. No, 5G doesn't cause COVID-19: How Internet giants are cracking down on Internet's biggest Coronavirus conspiracy
Financial Express. 10 April 2020
The conspiracy is so alarming, it is making internet giants, Google and Facebook, sit up and notice, and fight back, where they can.

O2. Zoom effect: Google rebrands Hangouts Meet, highlights how its video conferencing app is more secure than rivals
Financial Express. 09 April 2020
Scores of people are using video calling/conferencing apps around the world for work, for education, or simply staying connected.

O3. Google Meet premium features are now free for all G Suite users till September 30 as service pulls 2 million new users every day
Financial Express. 10 April 2020

All G Suite and G Suite for Education customers globally will have free access to Google Meet 'enterprise' features until September 30.

O4. PayPoint facilitates government's relief package during Covid-19 lockdown
Hindu BusinessLine. 10 April 2020

PayPoint India, a technology-enabled distribution network of financial services, has extended its services to enable the transaction of government's relief package to the poor who are worst-affected by the coronavirus outbreak. The company's micro-ATM, both Adhaar and swipe-based, installed at

neighbourhood shops, ensure easy cash withdrawal of the direct benefit transfer (DBT) during such a crisis, as per the company's official release.

O5. How to secure networks as employees take work home
Hindu BusinessLine. 10 April 2020
Update OS, software, security solutions; go for patches; keep tabs on phishing attacks. As the Covid-19 pandemic forced IT companies to shift work to homes, the Chief Information Security Officers (CISOs or equivalent executives) are burning the midnight oil to ensure secure transmission of information back and forth.

O6. Concerned about global spurt in cybercrimes, PMO's cyber chief issues cyber-advisory for online users

Economic Times. 10 April 2020

There has been a 50% surge in global cybercrimes post the onset of Covid-19, reveals India's National Cyber Security Coordinator Rajesh Pant. Avoid suspicious mails, SMSes, and learn cyber-hygiene through a free online course, he said. The current crisis has increased the dependence on the Internet. Fraudsters are taking advantage of this to ste ..