Cyber risks on the rise owing to rapid AI adoption, scamsters

SEVERAL incidents concerning cyber security have been reported in last 24 hours. From PHP to eMudhra, such cyber security issues have again raised the threats posed in the digital world, which have real life implications. Back home, eMudhra issue has highlighted India's vulnerabilities.

eMudhra is an Indian digital certification authority, which provides digital certificates that help browser confirm that the website is genuine. Several government websites like Income Tax, Aadhaar issuer- UIDAI and many others use a range of eMudhra's keys to sign their security certificates. Without this authentication, browser will not allow the individual or entity to complete their task on these government websites.

In the recent security incident, security researcher named Wayne said the security encryption issued by eMudhra's certificates were extremely weak and could be cracked in seconds. He alerted major technology firms on such vulnerabilities. As compromised keys could allow cyber criminals to issue fraudulent certificates and impersonate legitimate websites, Apple, Google and Mozilla had blocked the certificates in their browsers- Safari, Chrome and Firefox.

Cloudflare- the cybersecurity firm- also deployed emergency fixes across its network to protect users. Though eMudhra said that no negative impact due to such incident has happened and taken remedial measures, Ministry of Electronics and Information Technology (MeitY) has constituted a special team to investigate the security incident over the vulnerabilities over private keys.

Another global incident involving PHP has led to many government websites going offline across the world. PHP is an open-source scripting language, which is more than 3 decades old, and is used widely across the internet. Globally, more than 70 per cent of websites use PHP.

In a recent incident, two critical vulnerabilities were found. These vulnerabilities could allow cyber attackers to take control of web servers of users without the requirement of any authentication. This incident, which came to light through OpenAI's latest model, prompted the National Security Agency (NSA) of US to give an advisory for installing latest security updates. "If an immediate update is not feasible, it is recommended that organisations take the system offline until it can be fully mitigated," the advisory said.

Several governments including Finland, & Netherland took several government websites offline. These incidents again raise the security threats that are emerging in the digital world owing to artificial intelligence (AI) and other emerging technologies. While cyber security threats have always been there, rapid adoption of AI has increased these risks.

Interestingly, AI is finding out old risks in the current digital world, and at the same time, it is also creating new vulnerabilities. Against this backdrop, India as a nation has to create effective defence against such digital risks. Increasingly, several Indians are falling into the trap of cyber criminals.

According to National Human Rights Commission (NHRC), Indians have lost around Rs 52,976 crore to cyber frauds over the past six years, with nearly 8 per cent of the losses relating to cyber arrest scams. Similarly, trading related cyber scams are on a rise with majority of the losses arising from such events. Apart from individual losses, government agencies are also facing high proportion of risk from digital war waged against the country by enemy nations.

Critical infrastructure projects like airports, dams, power plants and others are regularly facing cyber threats from neighbouring countries. As digital warfare becomes the new normal, India as a country has to devise ways to defend itself from such emerging threats. In this regard, AI can be a great enabler in accomplishing this objective.

Equal before law? Ask the convict and the undertrial

CHOLLETI

IN the same week that an Indian prison system holds thousands of undertrials who have never been convicted of anything, the Allahabad High Court opened its doors wide for a man convicted of murder, so that he may contest an election, possibly on a ruling-party ticket.

The order is almost impossible to read without a double-take. Nandlal Rai, also known as Babloo Rai, was sentenced to life imprisonment by a Varanasi trial court in April 2025 for the murder of Pramod Kumar Nigam, an activist of the Ram Janmabhoomi movement. A division bench of the High Court, comprising justices Siddharth and Vinai Kumar Dwivedi, has now not only granted him bail but stayed his conviction and sentence while his appeal is pending. The stated purpose, in his own lawyer's words, is his wish to fight the 2027 Uttar Pradesh Assembly election as an independent, or "if possible, on a BJP ticket."

The court's reasoning, as reported, was striking: the right to contest elections is "akin to the right to livelihood," and, in the words attributed to the bench, "the common man's right to livelihood... is no less important than a politician's right to contest elections." In one clean sweep, a murder convict's political ambition was elevated into a constitutionally protected livelihood interest.

Now hold that up against another, far more numerous reality. Umar Khalid and Sharjeel Imam have spent more than six years in custody in the Delhi riots "larger conspiracy" case — arrested, accused, never convicted. The trial has not begun. A charge sheet running to 17,000 pages and a prosecution witness list reportedly approaching 900 sit before a court that has not yet framed charges.

On January 5, 2026, the Supreme Court refused them bail, The Delhi High Court has rejected Khalid's plea repeatedly. Across the country, journalists, activists and ordinary citizens are detained under stringent laws, some for years, with no date fixed for charges to be framed, let alone a verdict.

Set the two images side by side and a question forms that no fair observer can avoid: is the higher judiciary now applying one standard to those aligned with power, and another to those who challenge it?

The law gives every judge discretion. The question is not whether the power to suspend a conviction exists. It is whether, in a republic where thousands rot as undertrials and where even the accused in a murder case queue for years for appeals, the most urgent use of that discretion is to rescue the electoral prospect of a convict who, his own counsel concedes, emerged as a suspect only days after the FIR and stands convicted on circumstantial evidence

The honest objection — and why it is not enough

Every fair analysis must state the strongest counter-argument, because it is a real one and not a pretext. The two situations are legally different. Rai's case is a suspension of a conviction pending appeal — a recognised power the High Courts exercise under the criminal procedure code, and one the Supreme Court has itself used for public representatives who stand to lose their office and their constituents' representation while an appeal drags on.

A stay of conviction preserves the status quo until the appeal is heard. It does not declare anyone innocent. Bail for someone accused of terrorism offences, on the other hand, is governed by a far stricter statutory regime — the Unlawful Activities (Prevention) Act inverts the usual presumption and requires a court to be satisfied that the accusation is prima facie not true. The judges denying bail to Khalid and Imam are, on this reading, simply applying a law Parliament wrote.

This is true, and it must be said plainly to keep this article honest. But it answers only the narrow question of jurisdiction and statutory text. It does not answer the larger question of equity, priority and perception — and it is precisely there that the unease settles.

The law gives every judge discretion. The question is not whether the power to suspend a conviction exists. It is whether, in a republic where thousands rot undertrial and where even the accused in a murder case queue for years for appeals, the most urgent use of that discretion is to rescue the electoral prospect of a convict who, his own counsel concedes, emerged as a suspect only days after the FIR and stands convicted on circumstantial evidence — one whom media reports have also linked to the late gangster-turned-politician Mukhtar Ansari.

Nothing in the reported order suggests the bench doubted his eventual acquittal. It suspended conviction to protect a candidacy. Meanwhile, for the accused who has spent six years awaiting trial — for whom the Supreme Court's own judgment in *Union of India v. K.A. Najeeb* recognises that prolonged incarceration can itself justify bail — the discretion repeatedly bends the other way.

Speedy trial, the Court has said for decades, is part of the guarantee of life and personal liberty under Article 21. Six years without charges framed is, on any reading, the failure of that guarantee. Yet the higher courts' remedy has been to let the detention continue.

What is really being tested

It would be wrong to reduce this to a single political party or a single judge. The cases are decided by different benches, under different statutes, on different facts. The deeper trend is institutional.

The contrast reveals what is increasingly the operative hierarchy in Indian criminal justice: political value trumps individual liberty. A conviction can be stayed the moment it threatens a career in representative politics. But a presumption of innocence, the very foundation of a free society, is treated as dispensable the moment an accused is branded a "dissident," an "activist," a "urban Naxal," or a "rioter." The label, not the evidence, becomes the operative fact.

That is how you get the strangest arithmetic in the world's largest democracy: a man proven guilty enough to be sentenced to life for murder is free to seek office, while men never proven guilty of anything sit into a seventh year waiting for a court to even tell them the precise charges they must answer.

The danger to the judiciary is reputational and profound. Courts command obedience not because they hold the sword or the purse, but because the people believe they are even-handed. Every time a stay of conviction drops for a political aspirant while an undertrial's bail fails for the ninth time, a little of that belief drains away. Law, wrote one jurist, is not an ass; but it can be made to look like one when it is ridden by opposing riders on the same afternoon.

Where this is heading

The honest answer to "where is the higher judiciary heading" is that it is heading in two directions at once, and that is the problem.

In one direction lies a judiciary internalising the priorities of state power: alert to the political convenience of a suspect aligned with the ruling dispensation, hardening itself against the accused who stands outside it. In the other direction — visible in the occasional bail grant, in Najeeb, in the rare acquittal — lies the older, better judiciary: the one that saw courts as the last refuge of the friendless and the unpopular. The outcome has not been decided. It will be decided case by case, and it will be decided by whether the higher judiciary remembers a simple, ancient truth: the test of a court's courage is not how it treats the powerful man who wants a favour, but how it treats the powerless man who has nothing left but the law. On the present evidence, the balance of that test is hanging, and not comfortably.

(The writer is with the Cholleti BlackRobe Chambers, Hyderabad, and writes on the economy, politics and law)

SBI data leak: What happened, what data was exposed and what customers should do

DR. MUCHUKOTA SURESH BABU

SBI has identified 3,897 customer records containing personal information in a dataset found on the dark web. The bank is investigating the suspected exposure, which raises concerns about targeted financial fraud and identity theft.

The State Bank of India (SBI) is investigating a suspected data leak after identifying 3,897 customer records containing personally identifiable information (PII) in a dataset available on the dark web.

In a stock exchange filing on October 21, the country's largest public-sector lender said a preliminary analysis of approximately 3.75 lakh records had revealed the customer information. SBI received alerts about the suspected exposure on October 16 from its threat intelligence service provider, the Defence Cyber Agency and the Indian Computer Emergency Response Team (CERT-In).

The bank has activated its cyber incident response and containment protocols and appointed an independent cybersecurity agency empanelled with CERT-In to investigate the incident. The investigation aims to establish the authenticity, source and extent of the suspected exposure. SBI said the incident had no material impact on its business operations, financial performance or business continuity. Its core banking functions continue to operate normally.

What data was exposed?

According to SBI's filing, the records reportedly contained customers' names, gender, registered mobile numbers, dates of birth, email addresses and residential addresses. The dataset also included branch and Customer Information File (CIF) identifiers, lead IDs, loan-related metadata and information from other associated files.

The bank is still verifying the authenticity and completeness of the data and investigating its origin. The findings do not establish that all the customers concerned have suffered financial losses or that their bank accounts have been accessed.

Does the leak mean SBI accounts have been hacked?

Not necessarily. Exposure of personal information does not automatically mean that bank accounts have been compromised. SBI's preliminary findings concern personal information and loan-related metadata. The bank has not established that account passwords, PINs, one-time passwords (OTPs) or transaction credentials were exposed.

However, the information could help fraudsters make scams more convincing. Criminals who know a customer's name, phone number, address or loan-related details could impersonate bank officials and claim there is a problem with an account, loan application or KYC verification.

Because the caller may already know personal details, the communication could appear genuine. Customers should not treat familiarity with their information as proof of identity.

How could the data be misused?

According to Sarthak Dubey, co-founder and COO of Mitigata, customer information can be exposed through systems beyond a bank's core banking infrastructure. Loan applications, KYC documents and account-opening forms may be stored across loan origination systems, employee email accounts, shared drives and third-party platforms used by vendors. Potential entry points include compromised employee or vendor credentials, phishing, infostealer malware and misconfigured storage systems or application programming interfaces (APIs).

Dubey cautioned that investigators must establish whether the information originated from SBI's systems, a third-party service provider or another source before drawing conclusions.

The key concern is that exposed personal information could be used to make fraudulent calls, messages and emails appear legitimate, increasing the risk of phishing, identity theft and financial fraud.

What should SBI customers do?

SBI customers do not need to panic or automatically close their accounts. They should, however, remain alert to unexpected calls, messages and emails involving banking, loans or identity verification.

Never share an OTP, PIN or password with anyone, even if the person claims to represent SBI. Avoid clicking on unfamiliar links or installing applications at the request of an unsolicited caller. Verify suspicious communications independently through SBI's official website, mobile application or verified customer-service channels.

Customers should also keep transaction alerts enabled, review account activity regularly and report unauthorised transactions immediately. Checking credit reports for unfamiliar loans, credit cards or credit enquiries can help identify potential misuse of personal information. Those who do not require Aadhaar biometric authentication may also consider locking their biometrics through official UIDAI channels.

Anyone who suspects financial fraud should contact their bank immediately or call India's cybercrime helpline at 1930.

What happens next?

SBI's investigation must establish the source and authenticity of the data, identify any affected systems or third-party providers and determine the number of customers potentially affected. The bank will also need to secure any vulnerabilities, review access controls and strengthen monitoring for attempts to misuse the information.

Identifying potentially affected customers and communicating verified findings will be important in limiting the risk of follow-on fraud.

SBI has stated that the suspected exposure has not materially affected its operations, financial performance or business continuity. The bank said it would take appropriate remedial and preventive measures in line with applicable regulatory requirements.

The investigation is ongoing, and the full source and extent of the suspected exposure remain unclear.

The bottom line

The identification of 3,897 customer records containing personal information does not, by itself, mean that bank accounts have been hacked or money stolen. Until SBI establishes the full facts, customers should protect their banking credentials, independently verify suspicious communications and report suspected fraud promptly.

LETTERS

Will RSS goad NDA to do better?

A family that bickers in private rarely broadcasts its quarrels to the neighbourhood ('Bhagwat's Dasara message highlights Hindu undivided family', October 22, 2026). The RSS chief's recent speech shows that differences within an alliance do not always mean a divorce. In politics, public silence often hides intense private negotiations. We must look beyond the dramatic headlines.

For the common citizen, the real question is whether these internal debates bring any benefit to their daily lives. A ruling party and its ideological mentor can disagree on election strategies or social issues, but they share a deep, unbreakable bond. They will eventually find a middle ground because their survival depends on each other. Instead of predicting a split, we should watch if this quiet tension forces the government to focus more on jobs, prices, and everyday governance.

K Chidanand Kumar, Bengaluru

India needs to be on guard against 'enemies'

THIS is further to your editorial 'Bhagwat's Dasara message highlights Hindu undivided family'. The annual Dasara Speech by RSS chief Mohan Bhagwat was more in line with an orderly democratic process to be followed in the country by the opposition, in order to draw attention to their demands. Agitations, Mohan Bhagwat said are healthy democratic procedures to remind the government in power for needed course correction. But, the process and procedure must not be with an intention to damage or hurt the orderly and well-oiled administration of the country at the behest of radical elements or inimical forces conspiring against the government. However, the nation has to guard against the vicious designs of destabilising forces out to wreck the country; and the people must be aware of such designs by such agencies. The virtual critic of Mohan Bhagwat was the Karnataka Home minister, Priyank Kharge who needlessly lampooned Bhagwat being the spokesperson for BJP was a very sad demonstration against RSS for no reason by the Congress government in Karnataka.

S Lakshmi, Hyderabad

RSS firmly behind BJP as ever

THIS refers to "Bhagawat's Dasara message highlights Hindu undivided family," (Oct 22). RSS Chief Mohan Bhagwat's Vijayadashami speech warning against "regime change" and foreign-backed plots is not entirely unexpected. The Rashtriya Swayamsevak Sangh (RSS) and the ruling Bharatiya Janata Party (BJP) share the same ideological roots, making the BJP the political arm of the Sangh Parivar. When the RSS chief warns against political unrest or protests targeting the government, it serves a clear purpose: protecting their shared political power. Any threat to the Modi-led BJP government is seen by the RSS as a threat to its own long-term vision for India. While the RSS and BJP may occasionally disagree on minor internal issues, the RSS will never support opposition parties trying to remove the BJP. Defending the current government against criticism or political change is essential for the RSS to safeguard its own ideological goals.

N Sadhasiva Reddy, Bengaluru

Sangh's 'ostrich in the sand' approach

Apropos 'Bhagwat's Dasara message highlights Hindu undivided family' (Hans India; October 22, 2026). RSS Chief Mohan Bhagwat's annual Dasara speech was a damp squid, vis-à-vis the burning issue of the CEC-orchestrated SIR. RSS, the ruling BJP's Godfather obviously doesn't find an exercise that disenfranchised over 13 crore eligible Indians worth addressing.

RSS' silence on a grave issue that has dented Indian democracy badly represents the Sangh's design to cling to power by hook or by crook. This has been disturbing to the commoner, whose hope of a nation of uncompromisingly strong democratic credentials has been dashed. When hope fades, desperation and frustration take shape. It is indeed disappointing to note that Bhagwat chose to adopt an 'ostrich in the sand' approach, so that the hornet's nest isn't stirred. Bulldozing a nation's democratic tradition must be met with eyeball-to-eyeball.

Dr. George Jacob, Kochi

thehansreader@gmail.com

BENGALURU ONLINE

'Stop harassing film producers in the name of awards and subsidies'

BENGALURU: Film director Mansore has urged the government to simplify the application process for state film awards and subsidies, alleging that the existing procedures impose an unnecessary financial burden on Kannada film producers. Applications have been invited for the 2022 and 2023 State Film Awards, with October 31 set as the deadline. However, delays in the award and subsidy process over the past seven to eight years have made it difficult for producers to submit applications, he said in a press release. Mansore pointed out that only a handful of production houses in the Kannada film industry operate on a full-fledged basis, while most are independent or part-time ventures that close their offices after producing one or two films. Many producers do not systematically preserve the necessary permissions and documents related to film production. After a film's release, directors, production managers and other team members often move on to different assignments, leaving producers struggling to collect the required paperwork. He alleged that the government had made the application process excessively complicated, apparently to avoid disputes after announcing awards and subsidies. Applicants are required to submit 10 copies of certain documents separately for awards and subsidies, even though such a requirement does not apply when submitting films for the National Film Awards, he said.

The biggest hurdle, according to Mansore, is the mandatory submission of Blu-ray discs. He said Blu-ray was a preferred format for viewing films in full 2K resolution a decade ago, but DVDs and Blu-ray discs have since largely disappeared from the market.

Read more at https://epaper.thehansindia.com