

CYBER LAW



BY

ADV Dr. SAI SUSHANTH

CYBER LAW EXPERT & TECHNO LEGAL CONSULTANT

CEO, SUSHANTH IT LAW ASSOCIATES

Email id: sushanth@sushanthitlaw.com,

Contact/ WhatsApp No- +91 9849085940

USUAL RESPONSE WHEN I TAKE A SESSION



CYBER LAW APPLICABILITY

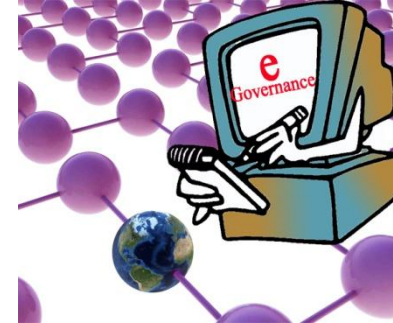
- ▶ COMPUTERS
- ▶ COMPUTER SYSTEMS
- ▶ COMPUTER RESOURCES
- ▶ COMPUTER NETWORKS
- ▶ COMMUNICATION DEVICES
- ▶ DATA OR INFORMATION IN ELECTRONIC FORM OR DIGITAL FORM



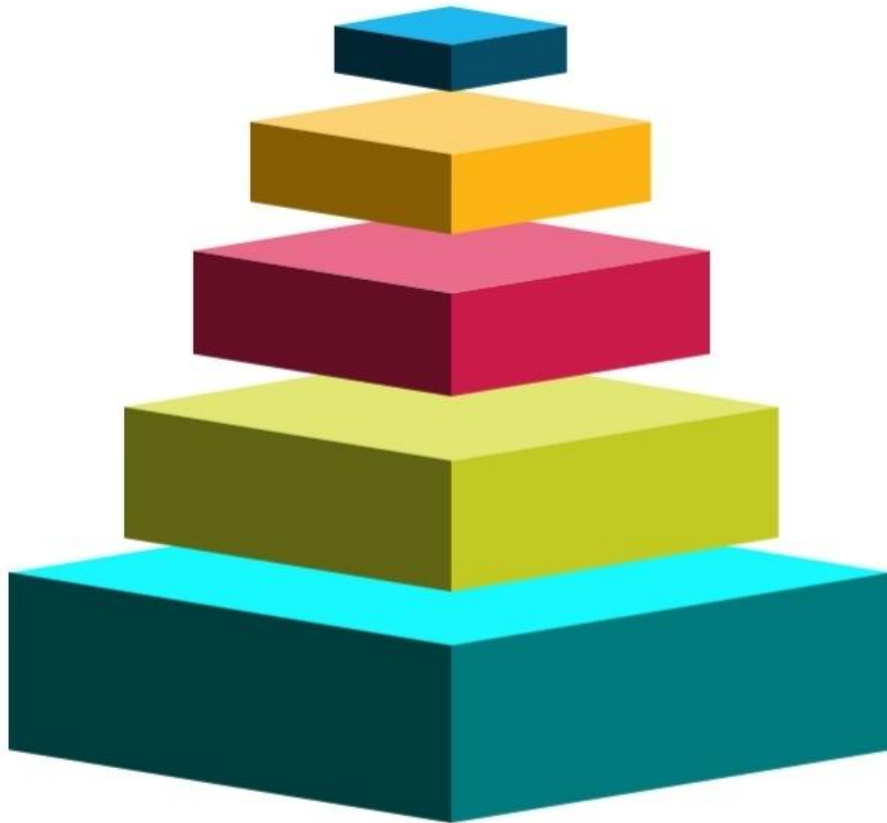


PHILOSOPHY OF IT ACT

- ▶ INFORMATION TECHNOLOGY ACT 2000
- ▶ INFORMATION TECHNOLOGY AMENDED ACT 2008
- ▶ Essentially, it is not a penal statute.
- ▶ It is not yet another weapon in the arsenal of the stake holders.
- ▶ The act is essentially intended to promote e-governance of which an essential part is e-commerce



Principles of IT Act- Preamble



1

To provide legal recognition to all transactions carried out in Electronic Format

2

To give a legal recognition and boost E-Commerce

3

To promote and provide legal recognition – E-Governance

4

To provide legal recognition to E-Communication

5

To facilitate Electronic Filings of Documents with Govt. Agencies

ELECTRONIC RECORDS

- ▶ SEC 2 (1) (t) - IT ACT
- ▶ SEC 4 - IT ACT



DIGITAL PAYMENTS



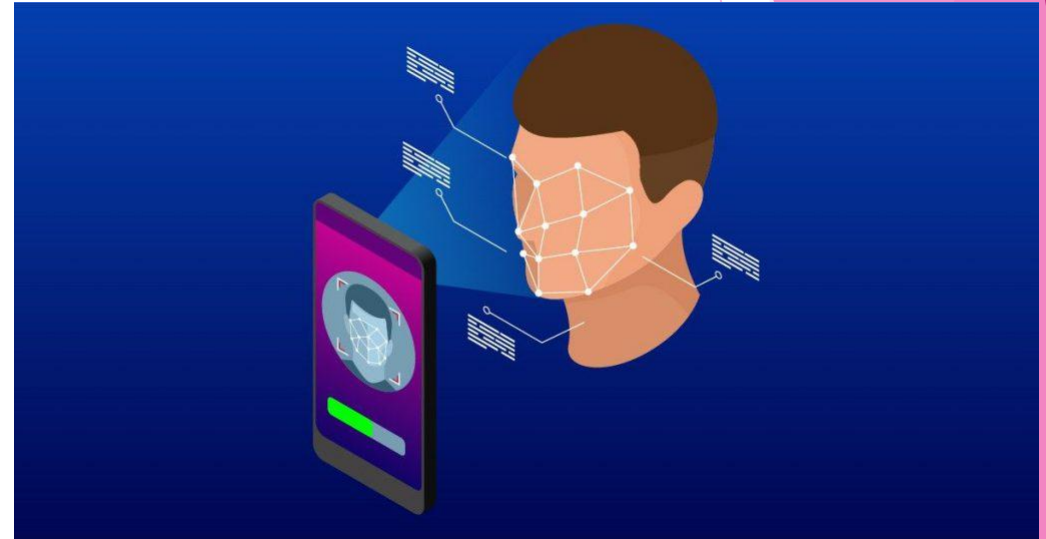
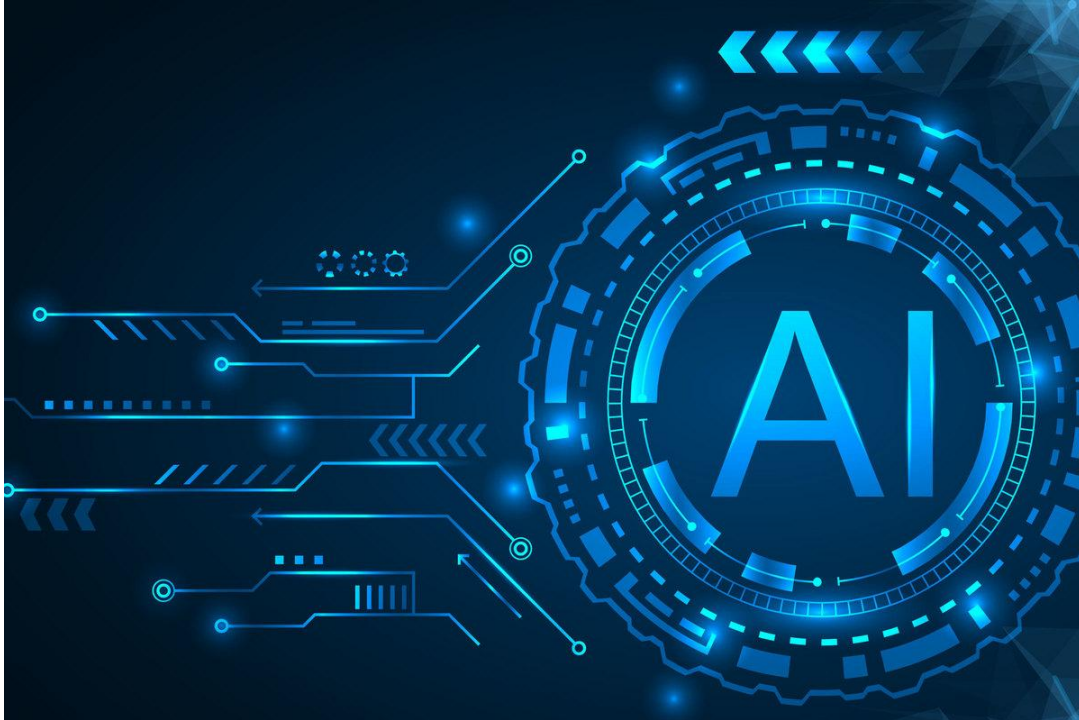
VIDEO CONFERENCING & CYBER LEGAL ASPECTS



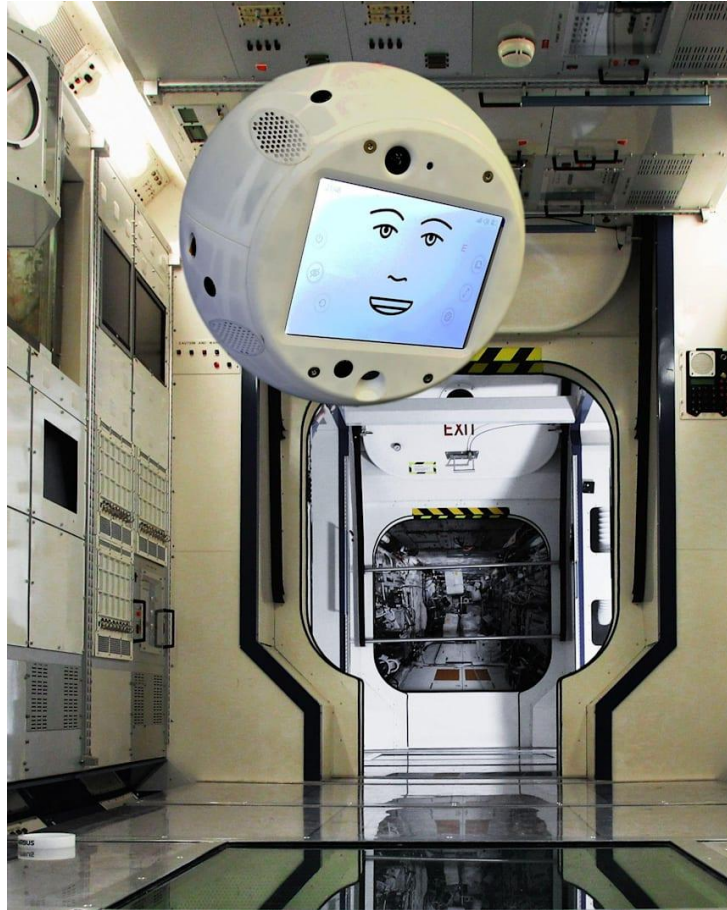
FACIAL RECOGNITION & INDIAN CYBER LAW



AI- ARTIFICIAL INTELLIGENCE



AI CASE STUDY - AI ASTRONAUT COMPANION



AI VIDEO CONFERENCING ACT- ILLINOIS



TLNT Talent Management & HR

TRAINING

CONFERENCES ▾

WEBINARS

RESEARCH

JOBS



ERE DIGITAL 2.0

OCTOBER 27 - 28, 2020

REGISTER NOW



New Illinois Law Puts Limits On AI In Video Interviews

By JESSICA NEWMAN AUGUST 16, 2019

Popular

1

4 Interview Questions to Avoid Hiring Toxic Employees



Ghar Ke Kalesh ✓

@gharkekalesh

Subscribe

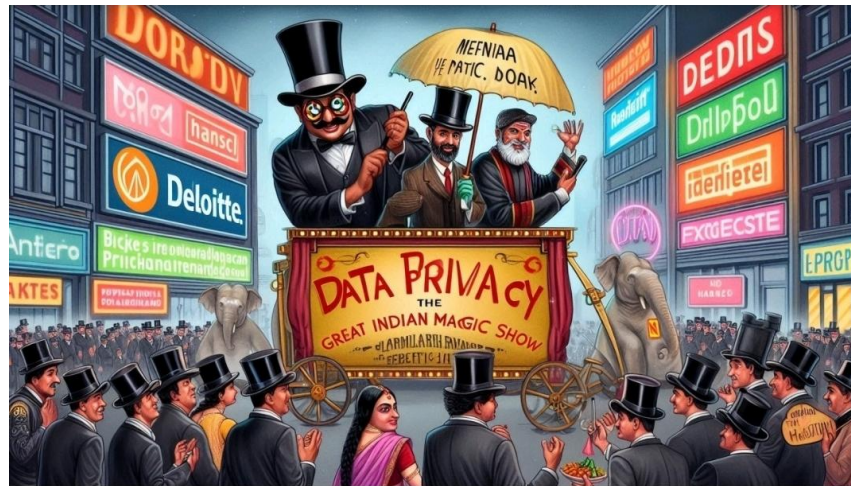


A guy from Lucknow used AI to add a leopard to his photo and posted it online, saying, “Spotted near my house.”

It went super viral, people got scared, and even the forest team came running—only to find out it was fake.

Now he’s in jail for the prank! 😏





Privacy: The Great Indian Magic Show (Now in 4K!)



Dhananjay Rokde ✓

Perpetual Student of Technology & Security
#Top40Under40 #AI #Fraud & #Investigation,

January 18, 2026

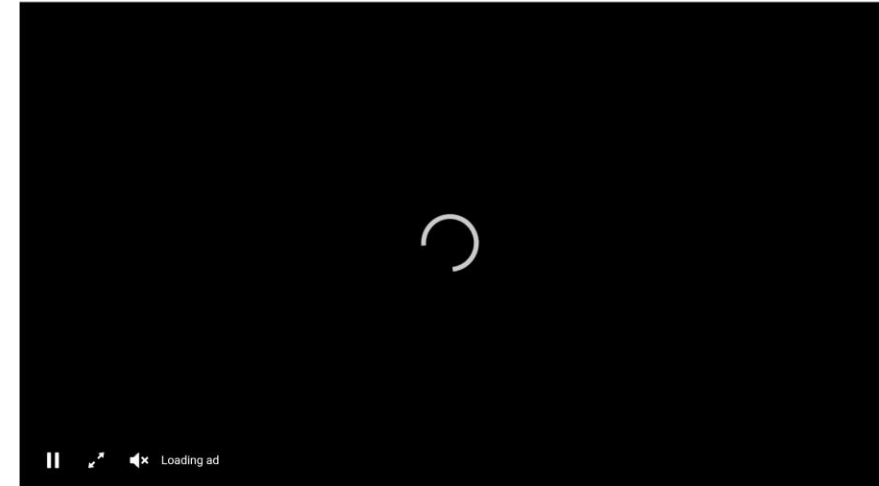
Welcome to the era of The Privacy Paradox, where we guard our CVs like the Kohinoor but share our live location with a pizza app for a ₹40 discount. If you thought "Privacy" in Bharat meant keeping your salary a secret from your neighbors, congratulations—you've been living in a pre-#DPDPA (Digital Personal Data Protection) simulation.

HOME / NEWS / CITIES / CHENNAI

Radisson Blue GRT relaunches with Chennai's first Anglo-Indian restaurant and a humanoid robot named Nanba

COMMENTS SHARE

READ LATER



Best known for The Great Kebab factory, the newly renovated hotel relaunches this week, offering the city's first Anglo-Indian restaurant, Ministry Of Chutneys, a Turkish hammam and treadmills that face the runway

December 22, 2022 05:15 pm | Updated December 23, 2022 10:58 am IST

ndtv.com/feature/ai-generated-images-of-wedding-couples-from-inc

NDTV

View simplified page?

CROSSWORD SWASTH SHOPPING

RENDS

View

Home > Feature > AI-Generated Images Of Wedding Couples From Indian States Go Viral, Internet Divided

Advertisement

Advertisement

Advertisement

Advertisement

AI-Generated Images Of Wedding Couples From Indian States Go Viral, Internet Divided

While some users gave a thumbs up to the concept, another section wasn't impressed and noted that the representational images seemed unrealistic.

Feature | Edited by Ritu Singh | Updated: January 02, 2023 5:23 pm IST

TRENDING

NDTV Tamil Nadu Governor Walks Out Amid Row With MK Stalin Over His Speech

NDTV CBI Arrest Of Ex Banker Chanda Kochhar Not Ok, She Will Be Freed: Court

NDTV "I Drank Because...": What Mumbai Men, Who Peed On Woman, Told Co-Flyer

NDTV Beauty Ananya Panday's New Year Holiday Beauty 10 Slides

NDTV Beauty Mouni Roy's New Year Holiday Beauty Looks 10 Slides

NDTV Celeb Katrina Kaif's Winter Style 10 Slides

Image tweeted by @baghardh

An artist has reimagined what wedding couples from Indian states would look like

f t w i m e s

Images generated by Artificial Intelligence (AI) have been making waves recently and social media is brimming with photos of artsy illustrations shared by users. Thanks to technology, what was once an impossible task in the realm of photo editing can now be completed in a matter of seconds without putting a lot of effort into it. Recently, a Delhi-based artist shared a series of images generated by AI that depicted what men and women from different Indian states 'stereotypically' look like. Now, another Twitter user has reimagined what wedding couples from different Indian states would look like when thought of as 'stereotypically'.

Twitter user, @baghardh took to the microblogging site to share the images and the compilations have become an instant hit online. The post includes couples from states like Punjab, Bihar, Uttar Pradesh, Tamil Nadu, Gujarat, Rajasthan, Himachal Pradesh, West Bengal, Kerala, Nagaland, and Arunachal Pradesh.

QUICK LINKS

Business News Coronavirus Cases

Hindi News Latest News Tech News

India News World News Sports News

New Hindi Movie PNR Status

Live Train status

SHORT VIDEOS

By Firework



Master's (MS) in Data Science
from Top European Universities

Learn More



Analytics Insight

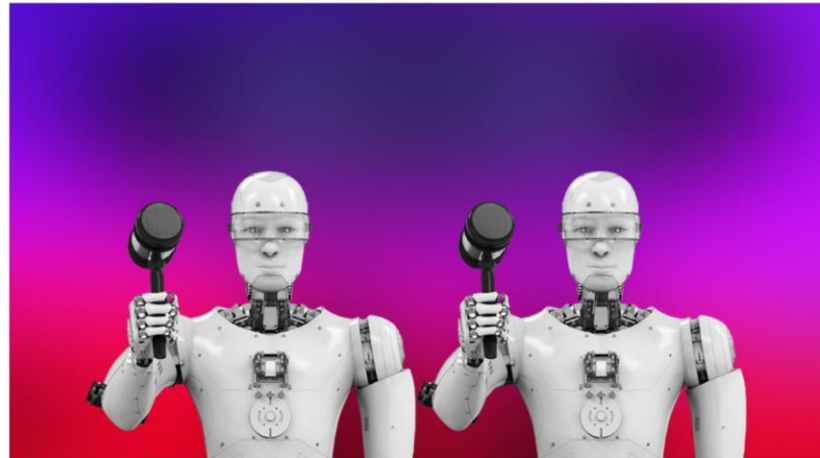
Artificial Intelligence . Latest News . Robotics

First time in History! An AI Robot to defend a human in Court



sirisha

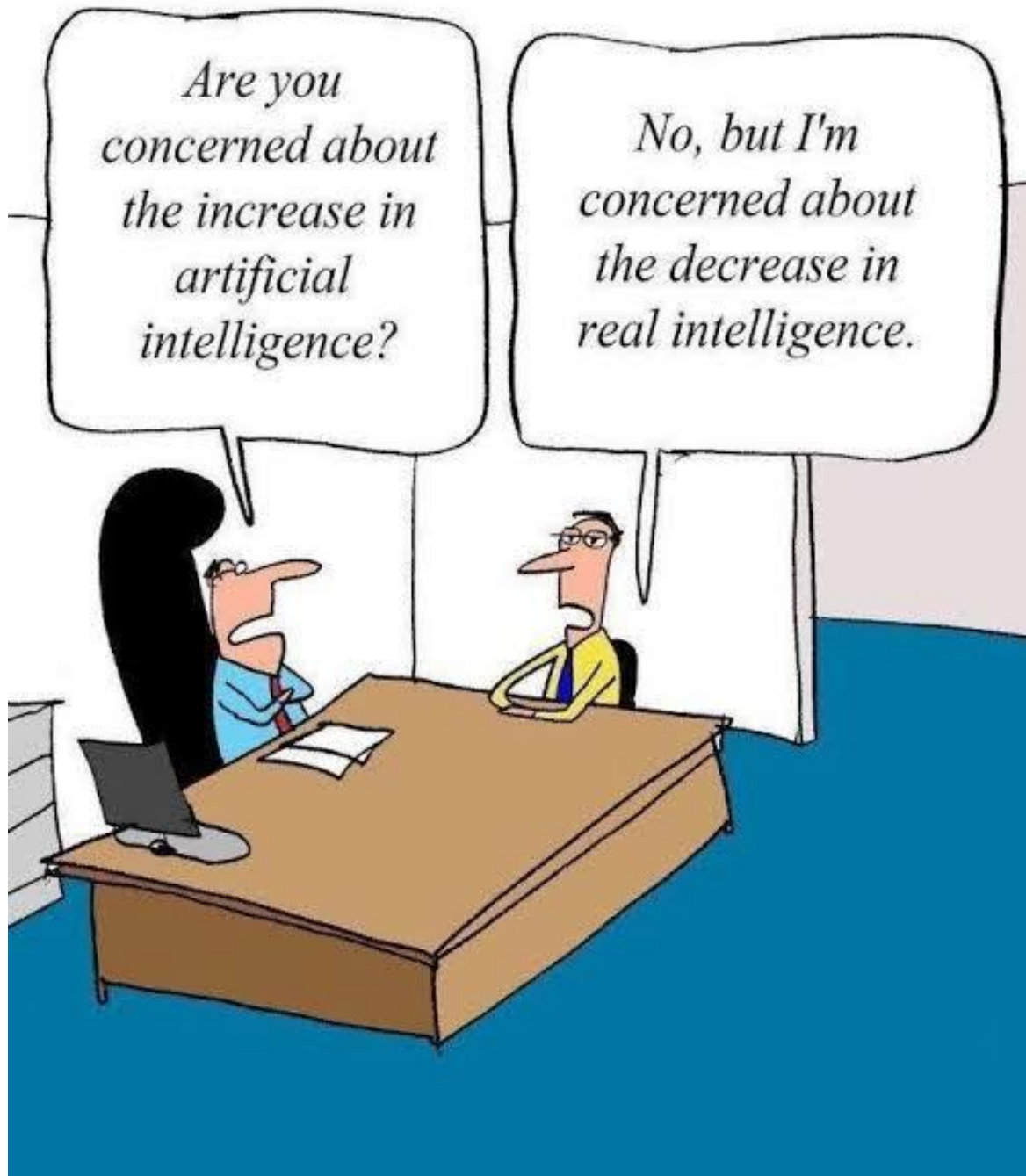
January 6, 2023 . 2 mins read



AI robot to defend a human? DoNotPay says its robot lawyer can deliver the arguments a defendant needs

"Fight corporations, beat bureaucracy, and sue anyone at the press of a button", reads the homepage of DoNotPay App, an AI company that develops legal services chatbots. The caption describes what its new bot and what it can do. They have developed an AI Robot to defend a human in court. It is literally a kind of digital lawyer that can be loaded into your very favourite hand held device. A defendant in a court proceeding can take its help in suggesting the right arguments and win the case. It will take up a case in February as legal assistant to help the defendant fight the case for traffic tickets. The AI lawyer assistant will hear the arguments in real time and deliver





The Indian Generative AI..



AI Governance Laws and Frameworks

Laws & Regulations



EU AI Act



EU AI Liability Directive



AI Bill 2338/2023



AI and Data Act



Executive Order on Trustworthy AI



NYC Bias Audit Law



Algorithmic Recommendation Law



Generative AI Services Law



Deep Synthesis Law



Peru Law 31814



South Korea AI Act



Indonesia Presidential Regulation on AI



Mexico Federal AI Regulation



Chile Draft AI Bill

Frameworks & Principles



NIST AI Risk Management Framework



Blueprint for an AI Bill of Rights



OECD AI Principles



OECD AI Risk Classification Framework



Framework Convention on AI, Human Rights and Rule of Law



Singapore AI Verify Framework



Singapore Generative AI Governance Framework



UNESCO AI Ethics Recommendation



G7 Hiroshima Process AI Guiding Principles

Technical Standards



ISO/IEC 42001 AI Management System



ISO/IEC 23894 AI Guidance on Risk Management



IEEE P2863 Organizational Governance of AI



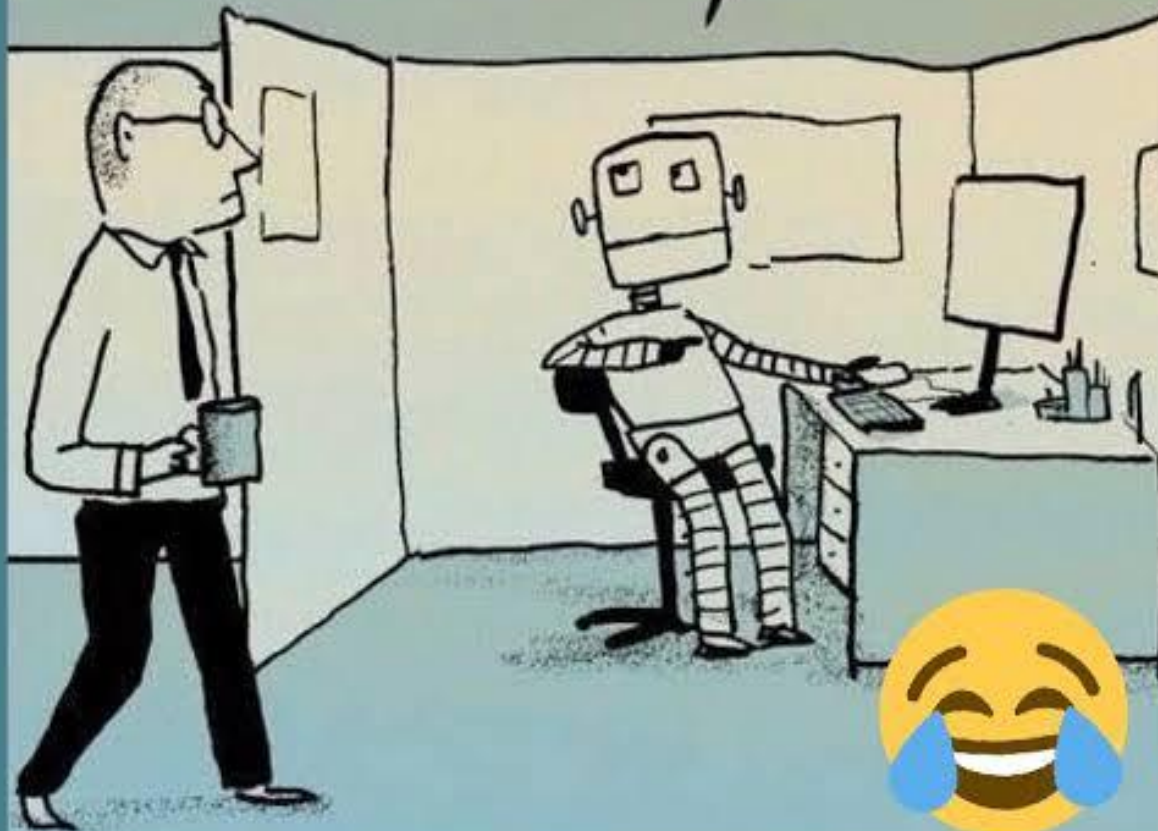
IEEE P7003 Algorithmic Bias Considerations



CEN-CENELEC EU AI Act Standards (tbc)



HEY MAN... WOULD YOU TICK THIS
"I AM NOT A ROBOT" BOX FOR ME?



moneycontrol.com/tecl

moneycontrol

Go PRO Now

Markets News Editor's Picks Tech India Learning Curve Portfolio

₹50K To ₹50 Lakhs – Instant Cash! Claim Now

Home > Technology > CERT-In makes annual cybersecurity audits mandatory for public, private sectors, brings AI under scanner

Trending Topics Battlefield 6 Open Beta Amazon Great Freedom F

CERT-In makes annual cybersecurity audits mandatory for public, private sectors, brings AI under scanner


Annual audits now expected across public and private sector entities, AI tools to be evaluated through AIBOM disclosures

AIHIK SUR

AUGUST 04, 2025 / 13:35 IST

CREDIT CARDS

f X in WhatsApp Telegram Email



Cybersecurity



JLR Cyberattack Triggers 25% Sales Drop, ₹1.5 Lakh Crore Revenue Hit

CYBER CRIME

JLR Faces Estimated ₹1.5 Lakh Crore Hit Following Devastating Cyber Attack

f X WhatsApp in

3 Min Read

THE 420

By The420 Correspondent

Last updated: October 9, 2025 7:01 pm



SHARE



London, October 2025 — British luxury automaker Jaguar Land Rover (JLR) has reportedly suffered an estimated ₹1.5 lakh crore (~£1.5 billion) revenue loss following a devastating cyber attack that disrupted both production and sales systems. The attack resulted in a nearly 25 percent drop in sales over a three-month period, including the shutdown in September.

Contents

1 Production and Sales Disrupted by Cyber Attack

2 Sales Data Analysis

3 JLR's Response and Recovery Efforts

4 Implications for the Global Auto Industry

5 Conclusion:

According to JLR's latest figures, total dealer sales for the three months ending September 2025 dropped to 66,165 vehicles, representing a decline of 21,138 units compared with the same period in 2024. With an average revenue of ₹72 lakh per vehicle, the company faces an estimated financial impact of ₹1.5 lakh crore.



Is Your Computer Mouse a Secret Microphone? New Vulnerability Raises Privacy Fears

CYBER CRIME

Is Your Computer Mouse Secretly Listening? Study Reveals How Hackers Can Turn Standard Mice Sou Vibrations To Extract Data

f X S in

4 N

THE 420

By [Shakti Sharma](#)

Last updated: October 15, 2025 11:25 am



SHARE



In a finding that has reportedly left cybersecurity experts “stunned,” researchers have demonstrated that a standard, commercially available computer mouse can be secretly exploited to record audio. The vulnerability, named “*Mic-E-Mouse*” by the team at the University of California, USA, centers on very sensors that allow the mouse to track movement. These sensors, it turns out, are so highly sensitive that they can detect the slightest vibrations, including those created by human speech traveling through a desk or surface. The researchers found that these minute room vibrations can be converted into recognizable sound, allowing nearby conversations to be overheard by a malicious actor. This is particularly alarming because, as the study notes, these peripheral sensors are typically not checked in standard security scans, which tend to focus on devices with dedicated microphones or cameras.

Contents

- 1 Accuracy and The Role of Artificial Intelligence
- 2 The Real-World Danger: Financial Fraud and Eavesdropping
- 3 Practical Steps for Complete Prevention



"Business Invoice Swapper," and How Did It Cost Companies Millions?

IME

Meet The 25 yr-Old 'Digital Nomad' Who Sold His 'Crime-as-a-Service' Tools That Hit Over 300 Financial Targets

🕒 in 🔗

5 Min R

By Shakti Sharma

Last updated: October 12, 2025 12:14 pm

MADRID— Spanish law enforcement has announced the arrest of a prolific international cybercrime ring, the "GXC Team," culminating in the arrest of its 25-year-old Brazilian leader. The group specialized in the sale of sophisticated, ready-to-use tools, including advanced AI-powered phishing kits, which it marketed to criminals across the dark web and Telegram, effectively running a global "Crime-as-a-Service" operation that targeted financial institutions and government agencies across more than 200 entities.



CYBER CRIME ECONOMIC FRAUD

Cyber Criminals Dupe SBI Deputy Manager Of Lakhs: The Officer Took A Loan To Cover The Loss

f X W in

5 Min Read

THE
420

By [Shakti Sharma](#)

Last updated: October 12, 2025 2:32 pm



SHARE



Raipur, October 2025 — In a chilling reminder of how advanced cybercrime has become, an officer from the State Bank of India (SBI) — who often educated customers about online fraud prevention — has himself fallen prey to a meticulously executed investment scam. The victim, Tej Prakash Sharma, a Deputy Manager posted in Raipur and a resident of Mayur Vihar, lost ₹13 lakh after being convinced to invest in a fake trading scheme. What makes this case particularly alarming is that Sharma not only lost his entire savings but had to take a personal loan to settle his financial commitments following the fraud.

Contents

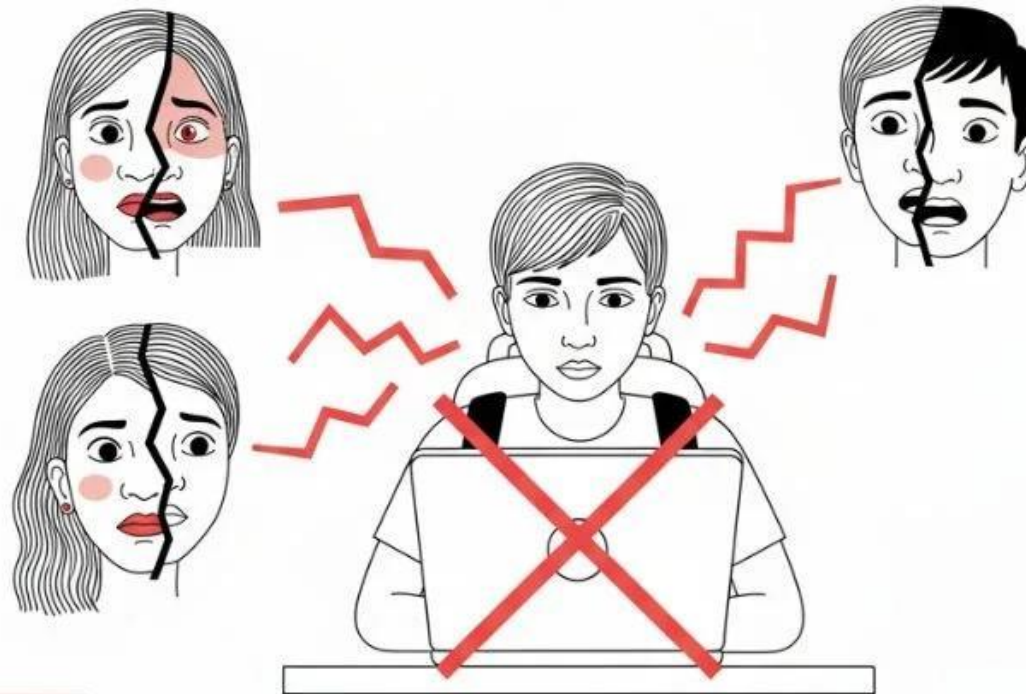
- | | |
|--|--|
| 1 The Scam Unfolds via WhatsApp | 4 A Cautionary Tale for Financial Professionals |
| 2 ₹13 Lakh Lost in Six Transfers | 5 Expert Insight: "No One Is Immune Anymore" |
| 3 Police Action After CM Helpline Complaint | 6 The Broader Lesson |

The Scam Unfolds via WhatsApp

According to the complaint filed with the Raipur police, the incident dates back to December 2024, when Sharma received a WhatsApp call from an unknown number. The caller, identifying herself as Divyanshi Agarwal, introduced herself as an "official" from a reputed investment company. She claimed that the firm was duly registered with the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) — a detail intended to instill credibility. During multiple conversations, the woman persuaded Sharma to invest in a "high-return trading program," assuring guaranteed profits within weeks.

STUDENT USES AI TO MORPH MORPH CLASSMATES' PHOTOS

- Non-Consensual Transformations
- Ethical Violation
- Digital Harassment





Microsoft Shuts IE Mode Amid Cyber Attack Reports

CYBER CRIME

Microsoft Removes One-Click Internet Explorer Mode Access in Edge to Stop Ongoing Attacks

f X W in

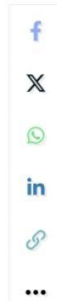


By [Swagta Nath](#)

Last updated: October 15, 2025 10:57 am



SHARE



Redmond, Washington: Microsoft has rolled out a critical change to its Edge web browser, disabling the convenient Internet Explorer (IE) mode toggle after receiving "credible reports" that cybercriminals were actively exploiting the feature to compromise systems. The company confirmed that the attacks, first detected in August 2025, leveraged a combination of social engineering techniques and 0-day vulnerabilities in Internet Explorer's outdated JavaScript engine, known as Chakra.

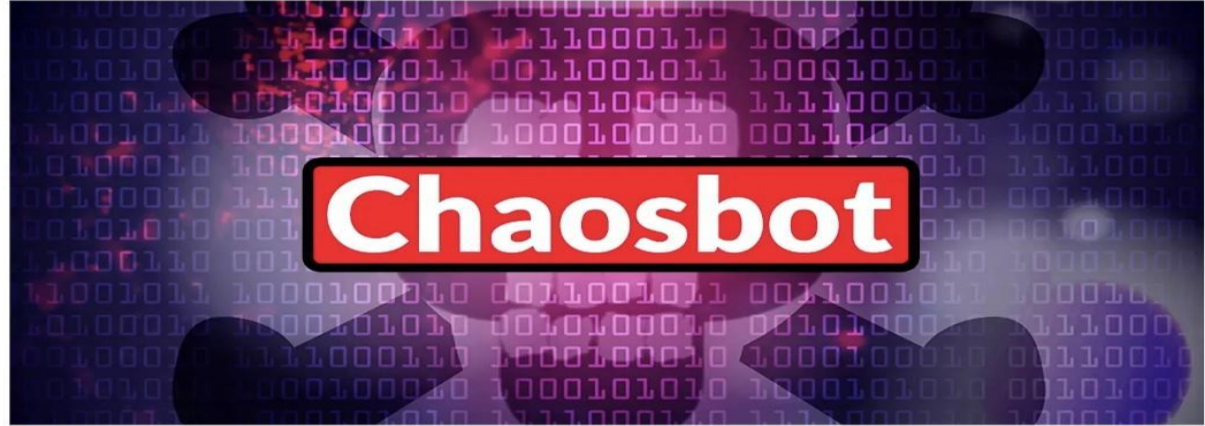
Contents

1 The Exploit: Legacy Compatibility Becomes a Cyber Risk

2 Microsoft's Rapid Response and New Restrictions

3 Expert Commentary: Legacy Features Still Pose Modern Threats

4 The Broader Implication: End of the IE Era



ChaosBot and Chaos-C++ Signal New Era of Destructive, Discord-Based Cyber Threats

CYBER CRIME

ChaosBot Malware Exploits Discord for Cyberattacks, Targets Financial Firms

5 Min Read

THE 420

By [The420 Correspondent](#)

Last updated: October 13, 2025 8:19 pm

 SHARE

Toronto, October 12, 2025 – Cybersecurity Desk: Cybersecurity researchers have uncovered a new Rust-based backdoor malware dubbed “ChaosBot” that leverages Discord servers for command-and-control (C2) operations, allowing hackers to remotely execute commands, steal files, and maintain persistent access to corporate networks.

Contents

- | | |
|---|--|
| 1 Discord Weaponized: The Rise of ChaosBot | 4 The Expanding “Chaos” Threat Family |
| 2 Multi-Stage Infection and Stealthy Persistence | 5 A Growing Threat Landscape |
| 3 Advanced Evasion Techniques | |

The discovery was made by Canadian cybersecurity firm eSentire, which first detected the malware in late September 2025 within the network of a financial services organization. Researchers say ChaosBot represents a growing class of sophisticated, modular threats built to exploit cloud-connected collaboration platforms.



CYBER CRIME

Lured by Online Lover, 74-Year-Old Mumbai Man Loses ₹3.7 Crore in Investment Fraud

[f](#) [X](#) [W](#) [in](#) [Link](#)

5 Min Read

THE 420

By [The420 Correspondent](#)

Last updated: October 15, 2025 1:02 pm

 SHARE

- [f](#)
- [X](#)
- [W](#)
- [in](#)
- [Link](#)
- [...](#)

In mid-2025, a 74-year-old retired man from Mulund, Mumbai, received a friend request on Facebook from a user calling herself "Diya Sharma." Their conversations grew frequent: heartwarming messages, video calls, expressions of care. Over weeks, "Diya" cultivated an emotional connection, weaving trust and companionship.

Contents

- 1 An Investment Mirage — Built to Deceive
- 2 Victims, Vulnerability, and Systemic Gaps
- 3 The Wider Trend: Romance Frauds and Financial Frontiers

But lurking behind her profile was a different intent. As the man grew emotionally invested, "Diya" introduced him to what she claimed was a legitimate investment opportunity with high returns. She said she worked for a Delhi-based firm called Bonanza Store and offered to guide him through the process. She shared a registration link and a referral code, encouraging him to establish an account that would supposedly yield 20 percent returns.



euroweeklynews.com



EuroWeekly NEWS
NEWS AND VIEWS SINCE 1998



News

Technology

€42,000 fine for adding employee in WhatsApp group during her time off

By **Ion Axinescu** • Published: 16 Jun 2025 • 19:23 • 2 minutes read



The company used her private phone number, despite her explicit request not to be contacted.
Credit: Shutterstock



A Deceptive Message and a Costly Mistake

CYBER CRIME

Ghaziabad Man Falls Prey to WhatsApp Link Hack in Major Cyber Fraud Case

f X 🕒 in 🔗

3 Min Read

THE 420 By The420 Correspondent
Last updated: October 12, 2025 5:08 pm

Ghaziabad – In a serious cybercrime incident in Indirgarhi, local resident Vedprakash became a victim of online fraud after clicking a suspicious link shared in a WhatsApp group. The link, labeled “PM Yojana 13”, contained an APK file and was posted in a group associated with the Indian Kisan Yuva Jagrook Sangathan.

- f
- X
- 🕒
- in
- 🔗
- ...

📖 Contents ^

1 Complaint Filed, Police Launch Investigation

2 Cybersecurity Alert: Awareness is Crucial

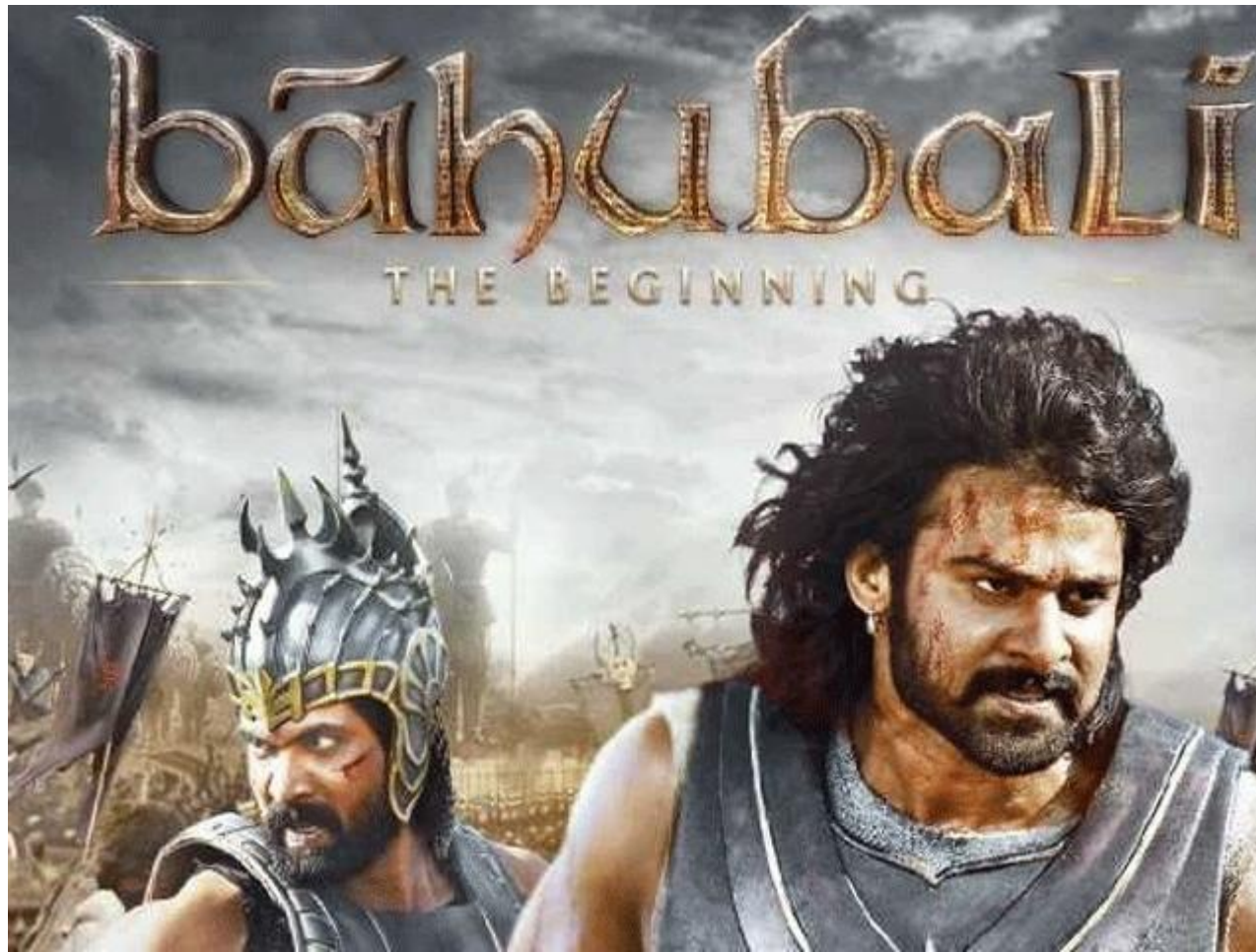
3 Precautionary Measures

4 Rising Threat of Mobile Cybercrime

5 Conclusion: Digital Vigilance is Essential

Within just five minutes, cybercriminals hacked Vedprakash’s mobile device and executed four UPI transactions, siphoning a total of ₹2.70 lakh from his bank account. The unauthorized transactions went unnoticed until around 11 PM, when his son checked the mobile device and discovered the fraud.

CYBER LAW & CYBER SECURITY LEARNINGS FROM BAAHUBALI ..



CYBER INTERNAL ATTACK



INVASION OF TRUST



SHARING OF CONFIDENTIAL INFO



EACH CYBER CRIME DIFFERENT APPROACH



CYBER SECURITY- INNOVATION STRATEGY



CYBER SECURITY- INDIGENOUS WAY



CYBER SECURITY INCIDENT RESPONSE



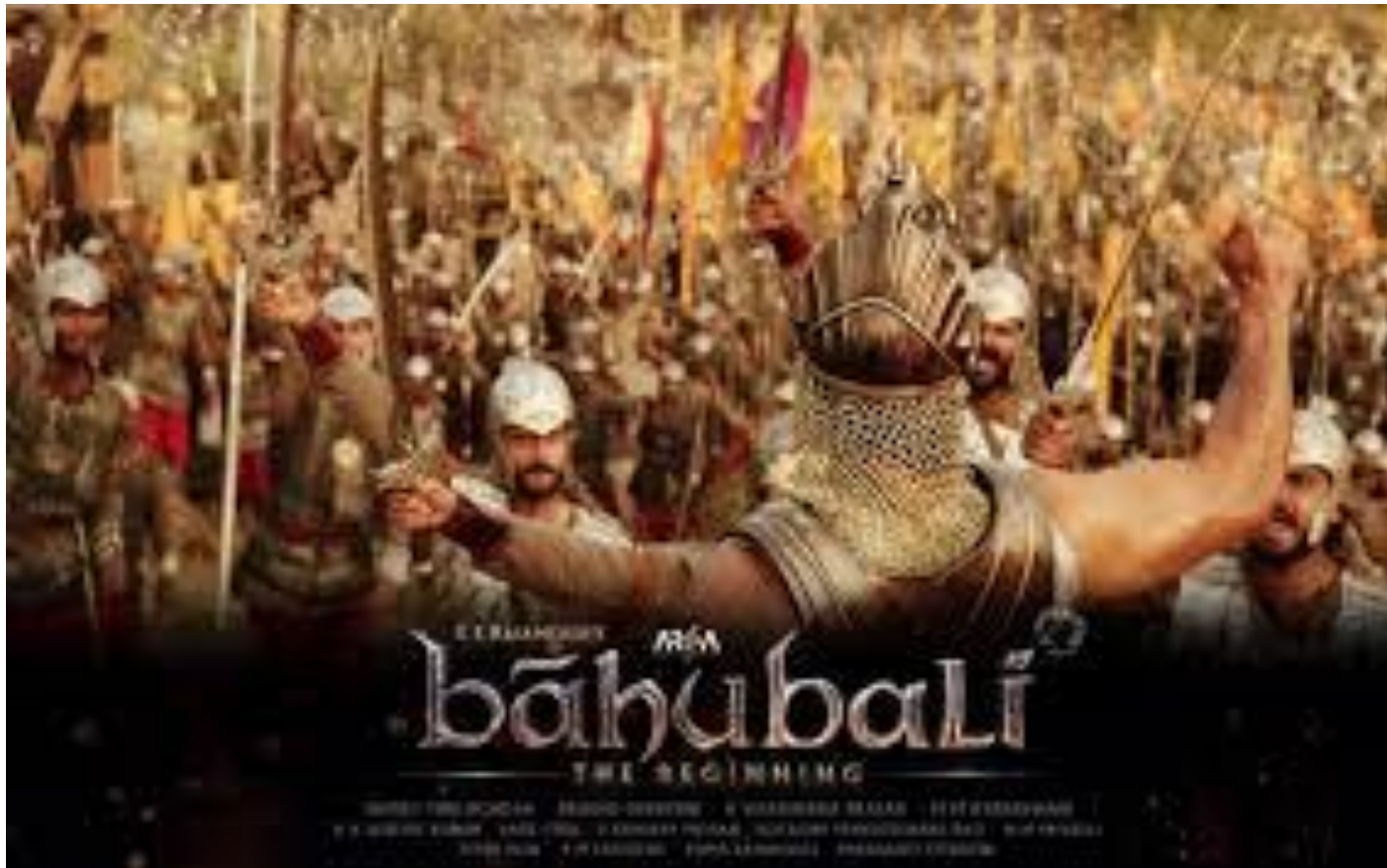
CYBER LAW PREPAREDNESS



CYBER CRIME DETECTION



CYBER LAW AWARENESS



AI, CYBER LAW & CYBER SECURITY LEARNINGS FROM SPECIAL OPS 2



KEY LEARNINGS FROM SPECIAL OPS 2

- ▶ AI & DIGITAL MANIPULATION
- ▶ AI - DOUBLE EDGE SWORD- AS A TOOL FOR ATTACK & DEFENSE
- ▶ AI & CYBER WARFARE
- ▶ ROBUST CYBER STRATEGIES & DEFENSES
- ▶ PROACTIVE MEASURES - POTENTIAL CYBER THREATS



CYBER LAW & CYBER SECURITY LEARNING FROM JSK MOVIE



AI LEGAL LEAP FROG STEPS

- ▶ EU AI ACT
- ▶ SOUTH KOREA - FEB 2025 APPROACH
- ▶ CHINA NEW RULES ON GEN AI
- ▶ AI LEGAL STATUS
- ▶ CYBER SECURITY BREACH

Technology Disaster

I was setting the voice recognition password of my mobile, a dog barked and ran away...

I am still looking for the dog to unlock my mobile...!!!



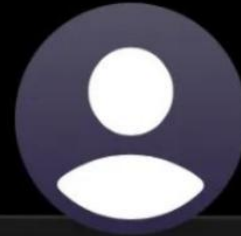
Don't play with new technology in a AI world!
Be careful!

17:23

10:11



9152



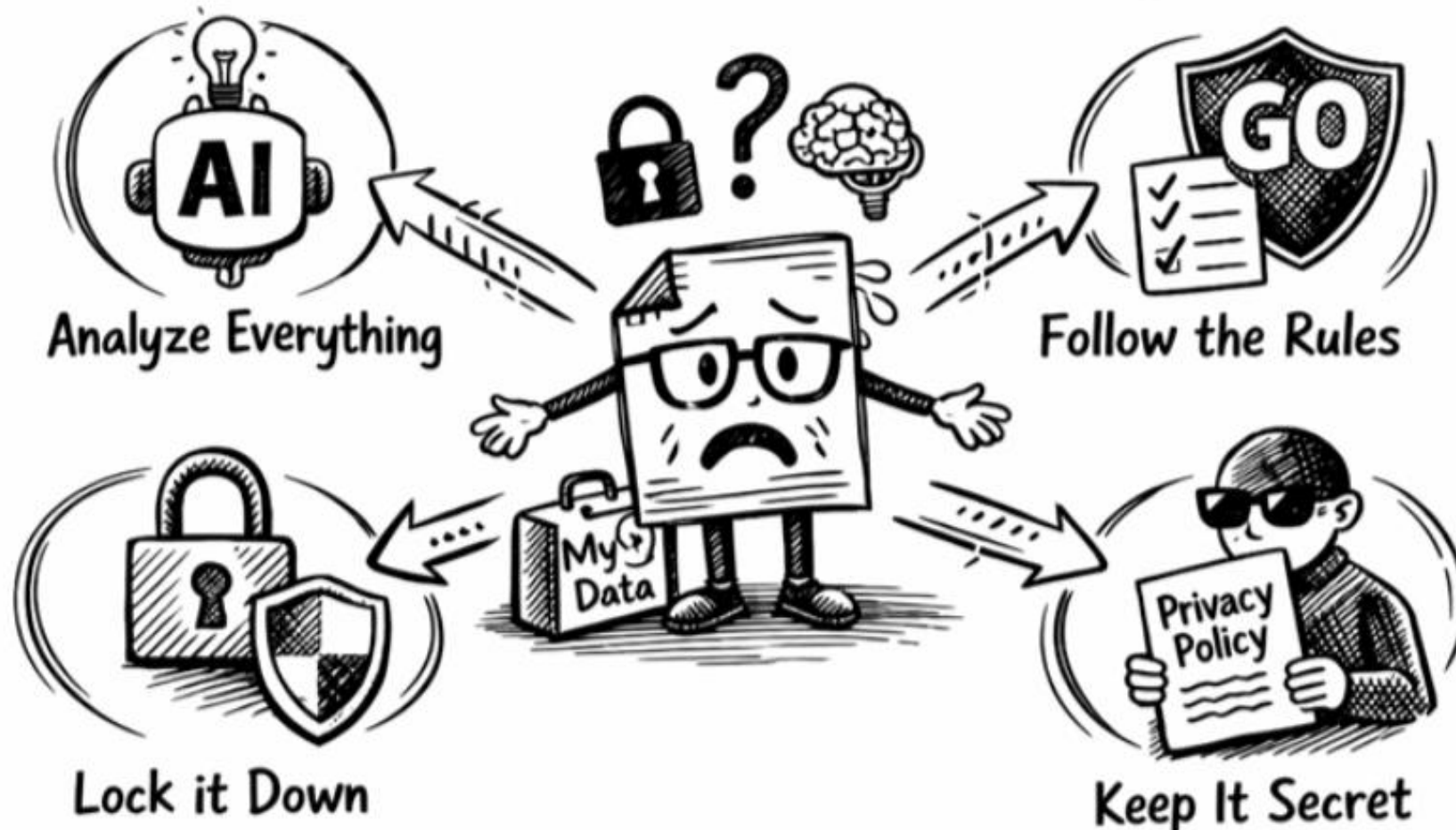
+91 94867 51557 ›

Text Message • SMS
Today, 09:38

Overspeeding violation noticed.
Challan No DL774509122.
Penalty INR 500 imposed. Issue
Date: 12-01-2026. [https://
ehallacn.rsscode.com/in](https://ehallacn.rsscode.com/in)

Data's Dilemma

(A Very Serious Story, Told Unseriously)



DIGITAL PERSONAL DATA PROTECTION FRAMEWORK

DPDP Act 2023 + DPDP Rules 2025

1. SCOPE (ACT §3)

- Applies to digital personal data in India.
- Applies extraterritorially when services target people in India.
- Covers State + private entities.
- Govt. has notified an 18-month compliance window.



2. ACTORS (ACT §2; RULES 4, 17–23)

- Data Principal.
- Data Fiduciary.
- Significant Data Fiduciary.
- Data Processor.
- Consent Manager — Indian company; ₹2 crore net worth; DPB-registered; interoperable; 7-year records; DPB may suspend.
- Data Protection Board — digital; online complaints; appeals to TDSAT.

3. PERSONAL DATA (ACT §2(13))

- Identifies an individual.
- No “sensitive” category.
- Rules protect children (parental consent) & persons with disability (guardian verification).

4. LAWFUL PROCESSING

Consent

- Standalone notice (Rule 3).
- Free, specific, informed, unconditional, unambiguous.
- Notice may use English or any Eighth Schedule language.

Legitimate Uses (May)

- Voluntary data.
- State functions (Rule 5 + Schedule II).
- Compliance with law/court.
- Public health, disaster, employment, public order.

5. DATA FIDUCIARY DUTIES (ACT §8; RULES 3–12,14)

- Implement security safeguards; retain logs 1 year.
- Ensure processor security.
- Erase when purpose ends; 48-hr pre-erasure notice (Rule 8).
- Sector retention: up to 3 years (e-commerce, gaming, social media).
- State security: 1-year retention.
- Breach: notify DPB without delay; DP ASAP; full details in 72 hrs.
- Children: no profiling/targeting except essential services.
- Disability: guardian verification.
- Publish grievance mechanism; respond within 90 days; display DPO/contact.

6. SIGNIFICANT DATA FIDUCIARIES DUTIES (ACT §10; RULE 13)

- DPO in India;
- independent auditor.
- Annual DPIA + annual audit.
- Algorithmic safeguards.
- Govt-identified restricted data shall not leave India.

7. RIGHTS OF DATA PRINCIPALS (ACT §§11–14; RULE 14)

- Access, correction/update, erasure, grievance, nomination.
- DF shall publish rights + verification steps + timelines.

8. CROSS-BORDER TRANSFERS (ACT §16; RULE 15)

- Allowed unless Government restricts.
- Conditions may apply.

9. DATA PROTECTION BOARD (ACT CH V; RULES 17–23)

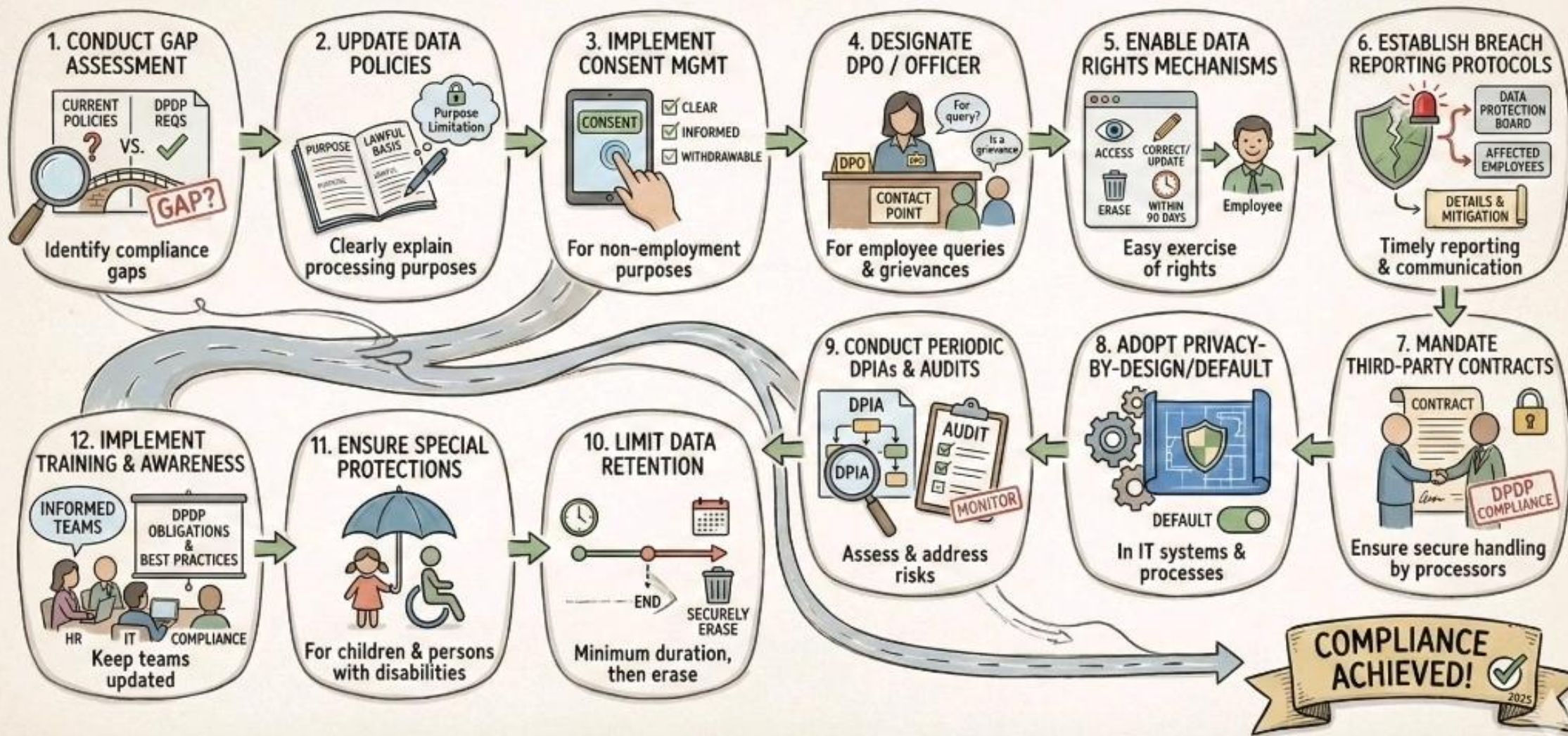
- Digital; online complaints; undertakings/mediation; penalties up to ₹250 crore.

10. COMPLIANCE WINDOW

Immediate (13 November 2025) In one year (13 Nov 2026)

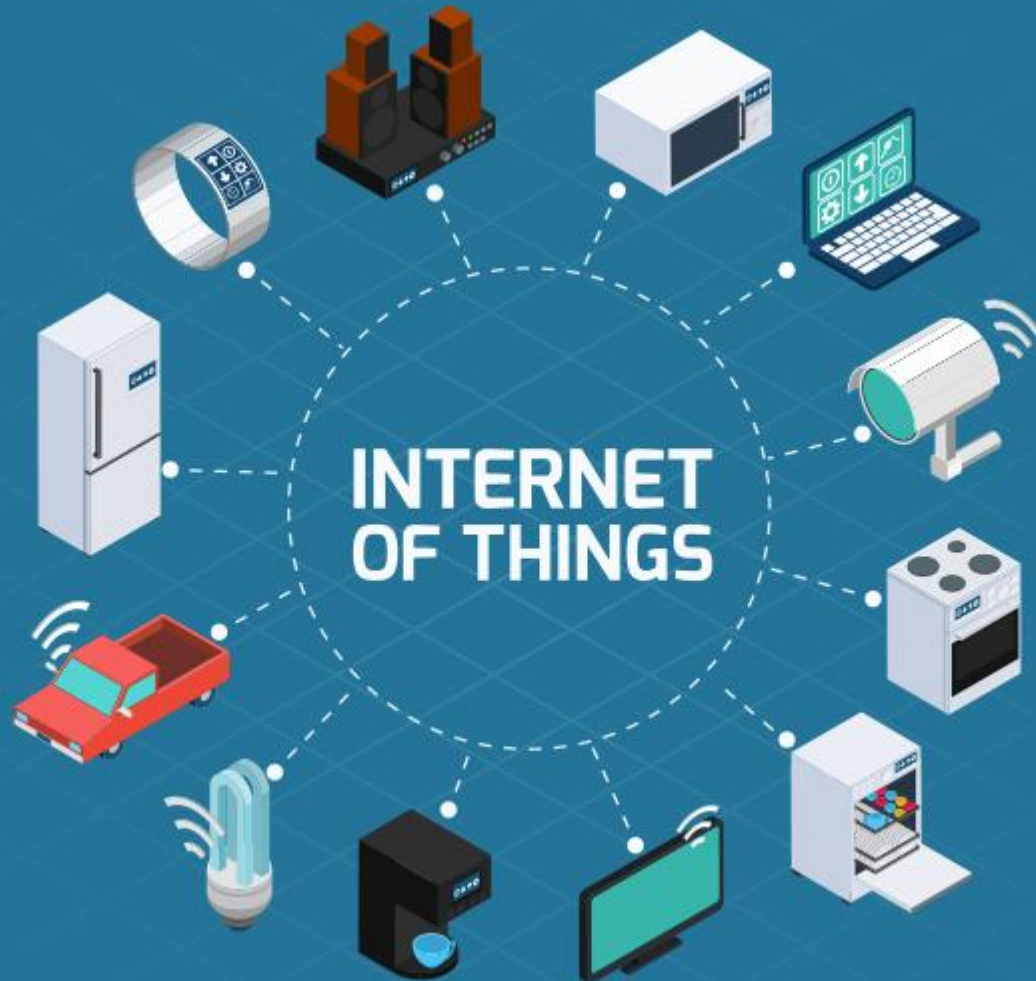
- | | | |
|--|--|---|
| <ul style="list-style-type: none">• Applicability and definitions• Data Principal rights (access, correction, erasure, grievance)• Data Protection Board establishment & functions• Adjudication, penalties & appeals | <ul style="list-style-type: none">• Legal proceedings lawful basis (Section 6(9))• Cross-border safeguards for legal obligations (Section 27(1)(d))• Consent Manager obligations commence (Rule 4) | <p>In 18 months</p> <ul style="list-style-type: none">• Deploy full DF controls: security, breach response, retention, processor oversight.• Implement lawful processing: consent flows, legitimate-use checks, cross-border controls.• SDF duties: annual DPIA, annual audit, enhanced safeguards.• Grievance flow, DPB-ready documentation. |
|--|--|---|

EMPLOYER'S GUIDE TO DPDP RULES, 2025 COMPLIANCE (INDIA)





IoT- INTERNET OF THINGS & INDIAN CYBER LAW



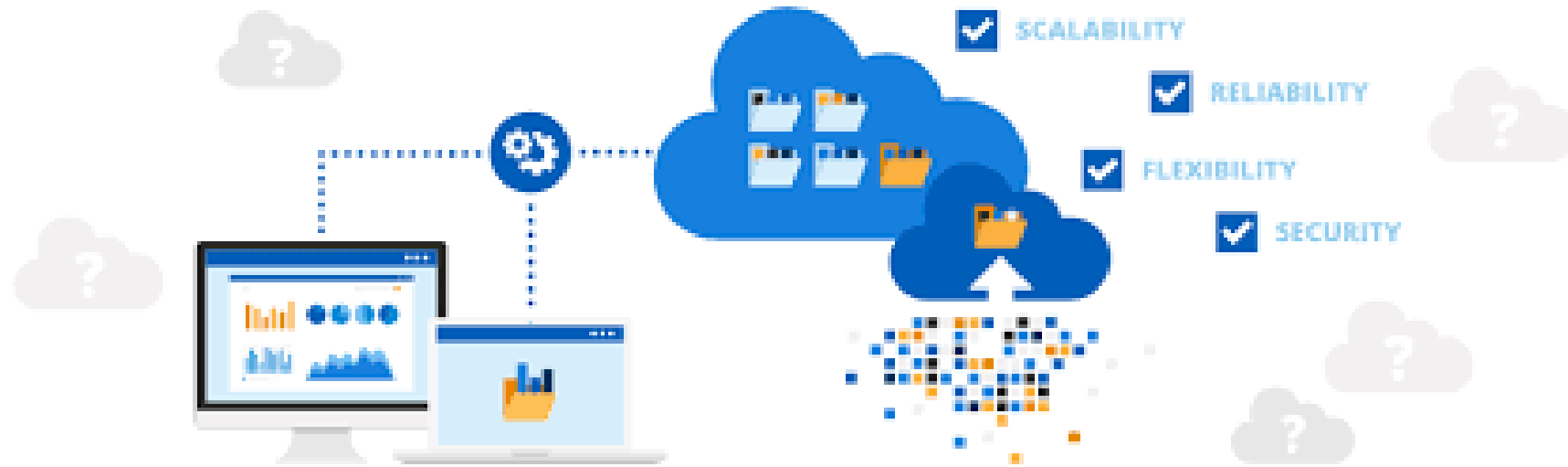
WEARABLE DEVICES & INDIAN CYBER LAW

- ▶ The terms “wearable technology“, “wearable devices“, and “wearables” all refer to electronic technologies or computers that are incorporated into items of clothing and accessories which can comfortably be worn on the body.

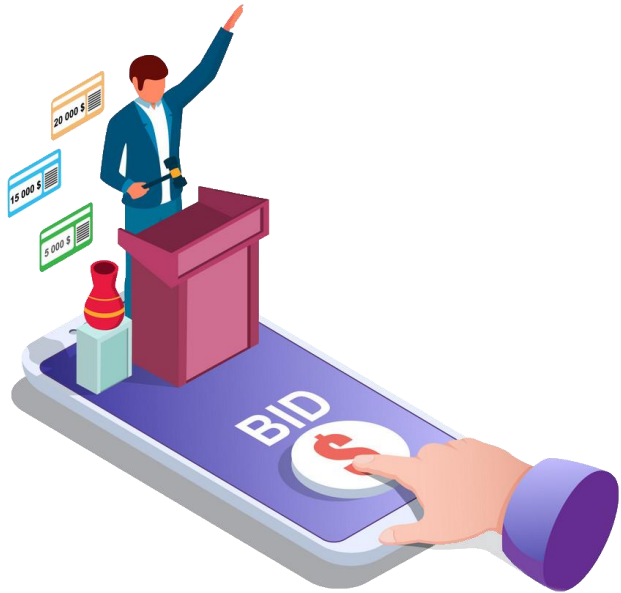
Designed for leading devices



CLOUD & INDIAN CYBER LAW



E-AUCTION & INDIAN CYBER LAW



5G - SIM FRAUD



IMPERSONATION ATTACKS



POLICIES - T & C



A HACKER LOGGED INTO
MY FITNESS TRACKER AND
STOLE ALL MY STEPS.





Why are Pirates
interested in data
privacy?

Because they
GDP
RRRRRRRR!

Must Read

What are

Home / Industry / Technology / Tata Powers It Systems Affected Due To Cyberattack Heres All You Need To Know

Tata Power's IT Systems affected due to cyberattack; here's all you need to know

Tata Power has taken important measures to retrieve and restore the systems and the company will update about the recent development in the coming time.

ADVERTISEMENT

Written by [Abhinav Anand](#)

October 16, 2022 6:55:43 pm

Follow Us



Tata Power has taken important measures to retrieve and restore the systems and the company will update about the recent development in the coming time. (Photo Credit: Reuters)

Latest News

Tata Power's IT Systems affected due to cyberattack; here's all you need to know



France ramps up war support for Ukraine, rebuilds armories



India's 1st Hindi MBBS books released in Madhya Pradesh, 'will free education completely from English,' says CM



Iran prison fire kills four, injures 61 as protests persist



Policybazaar introduces the new pay-as-you-go motor insurance in its latest brand campaign



Video: Govt focusing on procurement from women, SC-ST MSMEs, says Addl DC MSME Ishita Ganguli Tripathy

IT cos headed for lower attrition in coming quarters as global macro woes tame high churn, say analysts



PRIVACY AND SECURITY

Uber's Former Security Chief Convicted of Covering Up 2016 Data Breach

The firm's former chief information security officer was found guilty of hiding a massive data breach from federal investigators.

By Lucas Ropek | 10/05/22 5:39PM | Alerts



Photo: ROBYN BECK/AFP (Getty Images)

Click here for top news alerts

Home > Technology News > **Over 40% Of Indian Consumers Suffered Data Breach Online, Says**

Over 40% of Indian consumers suffered data breach online, says a new ISACA study



2 Min(s) Read



By Pihu Yadav

Oct 13, 2022, 03:13 PM IST (Published)

MINI

One in three respondents in India reported a significant increase in cybercrimes over the past 12 months, and nearly half do not think there is anything they can do or use to protect themselves from cybercrimes.




NEWS / BLOGS / INDIA / Cyber-attack on Kudankulam Nuclear Power Plant underlines the need for cyber deterrent strategy

INDIA

Cyber-attack on Kudankulam Nuclear Power Plant underlines the need for cyber deterrent strategy

November 29, 2019, 1:18 PM IST / SD Pradhan in Chanakya Code, India, TOI





SD Pradhan

S D Pradhan has served as chairman of India's Joint Intelligence Committee. He has also been the country's deputy national se ... MORE

The cyber-attack on the Kudankulam Nuclear Power Plant in October 2019, raises certain important questions about the security of our critical infrastructure and more importantly the adequacy of our response. Cyberattack on nuclear power plants was perturbing given the potentially catastrophic consequences of such an attack.



However, the press release issued after the attack reflected that the government considers that 'its system is infallible and no penetration into the nuclear power control plant is possible'. The reflected overwhelming confidence, complacency, and ignorance about the emerging dimensions of cyber threats.

Indian Police Arrests Crypto Fraudster Accused Of \$31 Million Scam

By [Alyz](#) — 7 hours Ago



Pixabay



Notably, the cryptocurrency industry expanded its boundaries in India in recent years. But unfortunately, [cybercriminals and crypto fraudsters also ramped up their efforts](#) to loot investors' hard-earned money in this sector. As a result, it put the law-enforcement forces on their toes and led government authorities to stricter regulations.

Similarly, the Indian police force in the country's second most-populous state, Maharashtra, has pinched a fraudster in Thane city, who had allegedly taken the money of 1,441 investors and vanished in thin air, per the country's [local media outlet](#).

Related Reading: [Increasing Crypto Crimes Forced Australia To Set Up Dedicated Police Unit](#)

The report estimates that the crypto scammer may have significantly looted the money, an excessive 2.5 billion rupees (\$31.2 million). Notably, only 24 investors have appeared to file their cases so far. They collectively lost \$55,085 in the scam.

In order to make investors dump their money, the scammer ran two fake programs on the platform set named 'SMP' and 'Magic 3x'.

The specialized workforce of the Thane police department, the Economic Offence Wing (EOW), which investigates

- Advertisement -



India's Luxury Brand Retailer
The Collective

Home | Hyderabad | Hyderabad Man Loses Rs 3 Lakh To Kaun Banega Crorepati Fraud

- Advertisement -

Hyderabad man loses Rs 3 lakh to Kaun Banega Crorepati fraud

BY TELANGANA TODAY PUBLISHED: UPDATED ON - 02:34 PM, TUE - 6 SEPTEMBER 22



Representational Image



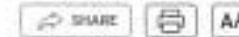
Hyderabad: A man from the city was duped to the tune of Rs.3.03 lakh by fraudsters in the guise of a [Kaun Banega Crorepati](#) lottery.

LATEST NEWS

- Hyderabad man loses Rs 3 lakh to Kaun Banega Crorepati fraud
6 seconds ago
- I have neither ruled myself in nor out: Shashi Tharoor on running for Congress president
12 mins ago
- Delhi CM Kejriwal to launch 'Make India No. 1' campaign from Haryana
29 mins ago
- 'India is our friend', says Bangladesh PM Sheikh Hasina
54 mins ago
- Youngsters win laurels by worshipping eco-friendly idols of

New threat on WhatsApp: Your phone can be hacked with a 'Zero-click'

TOI Trending Desk / etimes.in / Updated: Feb 7, 2025, 15:40 IST



WhatsApp has alerted nearly 100 individuals in over 24 countries to a sophisticated 'zero-click' spyware attack. The attack, traced to Israeli surveillance company, Paragon Solutions, compromises victims' devices without user interaction. WhatsApp is working with law enforcement and Citizen Lab to address this security breach.



WhatsApp has become one of the vulnerable platforms for cybercriminals due to its popularity and ease of availability among the users. The fraudsters and hackers use various tactics to deceive their victims and take away their information. Some of the common types of cyber fraud on WhatsApp are phishing scams where users are fooled into revealing their sensitive details via fake websites or messages or where links are provided to redirect an individual to a fake platform that forfeits sensitive information or reckless amounts of money from their bank accounts linked to the phone. However recently a new 'zeroclick' hacking attack has also come under limelight.

WhatsApp has recently opened up about nearly 100 individuals across more than two dozen countries who were targeted by a sophisticated "zero-click" spyware attack. This spyware required no action from the users, targeting mostly journalists and those in civil society, with concerns about privacy and freedom of speech.

The worrying breach was spotted in December and WhatsApp has followed up by contacting affected users to inform them about the breach while also trying to disrupt the hacking attempt. It has referred the matter to a Canadian-based watchdog group on internet issues known as Citizen Lab while informing law enforcement and industry partners. The incident showcases how commercial spyware is emerging as a grave threat and makes it necessary for a greater legislation to check this kind of intrusion into a person's personal space.



Delhi

Delhi HC seeks Centre's response on cyber crime PIL over 'digital arrests'

Fraudsters have reportedly been forging court orders and fabricating FIRs, using fake arrest warrants to extort money through bogus settlements.



Image used for representational purpose.

Shekhar Singh

Updated on: 08 Feb 2025, 7:12 am • 2 min read



NEW DELHI: The Delhi High Court has sought a response from the Centre regarding a public interest litigation (PIL) that raises concerns over emerging cyber crimes, particularly "digital arrests." The court granted the Union government four weeks to submit its reply, with the next hearing scheduled for March 19.



Related Stories

- Delhi poll results a 'setback', AAP's fight against BJP to continue: Atishi

PTI • 1 minute ago
- Congress' wipeout, AAP's defeat in Delhi deepen uncertainty within INDIA bloc

Preetha Nair • 21 minutes ago
- Results LIVE | BJP sweeps Delhi, ends AAP's 12-year rule as Kejriwal, Sisodia lose; Modi



ADVERTISEMENT

HOME / NEWS / INDIA / TELANGANA

Cyber crime police warn against medical emergency scam

Published - February 06, 2025 07:20 pm IST

THE HINDU BUREAU



READ LATER PRINT

HYDERABAD

Continue reading after this ADVERTISEMENT

The Cyberabad cyber crime police have warned citizens against fake hospital emergency scams. This comes at a time when impersonation frauds have been on a rise in the State.

Police said in such cases, fraudsters target 'unsuspecting' families by impersonating hospital staff. They claim that a family member is having a medical emergency and play on the emotional vulnerability of people.

Continue reading after this ADVERTISEMENT



News / India / Cyber frauds jump 900% in 4 years: Small cities like Deoghar, Nuh, Mathura emerge as new scam Capitals

Cyber frauds jump 900% in 4 years: Small cities like Deoghar, Nuh, Mathura emerge as new scam Capitals

The Centre has developed a working online 'suspect registry' which contains data of 1.4 million criminals linked to financial fraud and various cybercrimes.

Written by **Mahender Singh Marwal** [Follow](#)
New Delhi | Updated: February 5, 2025 10:34 IST

NewsGuard

3 min read



The registry contains data of 1.4 million cybercriminals linked to financial fraud and various cybercrimes. (File Photo)



☆

lock

indianexpress.com

☰

↺

FE

POCKET BOOSTER

Co-presented by

MOVADO

Associate Sponsor

KIA

pnb

Sections

ENGLISH | தமிழ் | বাংলা | ગુજરાતી | हिन्दी | BUSINESS | Sports

Newsletters

🔔

🌐

📱

EDITION India

Friday, Feb 07, 2025 | EPAPER | TODAY'S PAPER

The Indian EXPRESS

JOURNALISM OF COURAGE

Home

ePaper

My Express

UPSC

SCREEN

Explained

Opinion

Politics

Business

Sports

Cities

Lifestyle

Sign In

TRENDING

Delhi Exit Polls

Delhi Elections

Mixi Crossword

Premium

Express Shorts

Podcast

Health & Wellness

ADVERTISEMENT

News Cities Pune Hotel rooms for mules, couriers for bank kits: How Cambodia cyber syndicate's shadow network operated in Pune

Hotel rooms for mules, couriers for bank kits: How Cambodia cyber syndicate's shadow network operated in Pune

Details on this shadow network surfaced, when Pimpri Chinchwad police arrested 6 key operatives in January last week in connection with a share trading scam.

Written by [Sudhant Kulkarni](#)
Pune | Updated: February 7, 2025 09:33 IST

NewsGuard

5 min read



The investigation team with the suspects involved in the shadow network in Pune. (Source: Express Photo)

☆

lock

www.thehindu.com

↺

THE HINDU

FREE TRIAL

SUBSCRIBE

LOGIN

🔍

ADVERTISEMENT

HOME / NEWS / CITIES / HYDERABAD

YouTuber Masthan Sai arrested in cybercrime, sexual exploitation case

Updated - February 06, 2025 06:08 pm IST - HYDERABAD

THE HINDU BUREAU



READ LATER PRINT

The Narsingi police has arrested YouTuber Masthan Sai in connection with an alleged large-scale cybercrime and sexual exploitation case involving illegally recorded private videos and hacked personal data of multiple women, including teenagers.



The case came to light after Actor Raj Tarun's wife Lavanya, a resident of Kokapet Village, filed a complaint on February 2, said the Narsingi police.

New Copyright Ruling Just Made AI Skills The Biggest Advantage

Dan Fitzpatrick, Contributor

Dan is a bestselling author on AI & the future of education

Follow



1

Feb 3, 2025, 05:57am EST

Updated Feb 3, 2025, 03:42pm EST



New Copyright Ruling Just Made AI Skills The Biggest Advantage - GETTY

The **U.S. Copyright Office** has concluded that AI-generated work can be copyrighted when it embodies meaningful human authorship. This is big news. It means that those who develop expertise in working with AI can be rewarded with intellectual property.

Over the last couple of years, the critical question of who owns the creative output of generative AI tools has been a confusing one. Can the individual who prompts a tool like **ChatGPT** claim copyright protection? In the U.S. we now have an answer.



Home / Labour & Service / Personal Information Of Employees...

Personal Information Of Employees Like Service Records, Copies Of Promotion & Financial Benefits Can't Be Disclosed Under RTI Act: Delhi High Court

Namdev Singh

15 Oct 2024 12:00 PM

Share this



A single judge bench of the Delhi High Court comprising of Justice Sanjeev Narula, while deciding writ petition held that the personal information of employees like service records, copies of promotion & financial benefits can't be disclosed under the RTI Act. Background Facts On April 19, 2017, respondent No. 3 submitted an RTI application. It was sent to the Public...



News / Cities / Bangalore / AI-based attack responsible for Kaveri portal crash, suspects Karnataka Stamps and Registration Department

AI-based attack responsible for Kaveri portal crash, suspects Karnataka Stamps and Registration Department

The Stamps and Registration Department will file a cyber crime complaint after receiving the relevant details about the suspected Artificial Intelligence-based Distributed Denial of Service attack from the Department of E-governance.

By: Express News Service
Bangalore | Updated: February 9, 2025 22:42 IST

NewsGuard

3 min read





POLICY WATCH

Government Bans AI Tools Like ChatGPT in Offices Over Data Confidentiality Concerns

CYBER CRIME POLICY WATCH

RBI Launches Secure Internet Domain 'bank.in' to Shield Indian Banks from Cyber Fraud

POLICY WATCH

Future Crime Summit 2025 Concludes the Biggest Global Hackathon on Digital Forensics

POLICY WATCH

CopsLock – A Secure, Unified Communication & Data Management Solution for India's Security Forces

POLICY WATCH

Top CISOs and Cyber Experts to Gather for Exclusive Cybercrime Conference

POLICY WATCH

5 Workshops & Product Demos at India's Biggest Digital Forensic Summit, New Delhi – Register Now!

POLICY WATCH

Biggest Police Technology Conference in New Delhi – A Must-Attend for Police, Defence & LEA Officers!

POLICY WATCH

FutureCrime Summit 2025: Only 10 Days Left – Register Now!

POLICY WATCH

China's AI-Enabled Drones Pose Strategic Challenge for India

POLICY WATCH

Workshop on UAV Technology and Drone Forensics: Must-Watch Event at FutureCrime Summit 2025

POLICY WATCH

SEBI Cracks Down on Influencers, Bans Use of Live Stock Prices in Education

POLICY WATCH

FutureCrime Summit 2025: Only 14 Days Left – Register Now!

POLICY WATCH

Future Crime Summit 2025 Global Hackathon Dates Announced!

POLICY WATCH

FutureCrime Summit 2025 to Feature Exclusive DFIR Workshop for Cybersecurity Enthusiasts

POLICY WATCH

Official Launch of CopsGPT: A Must-Attend Event at FutureCrime Summit 2025

POLICY WATCH

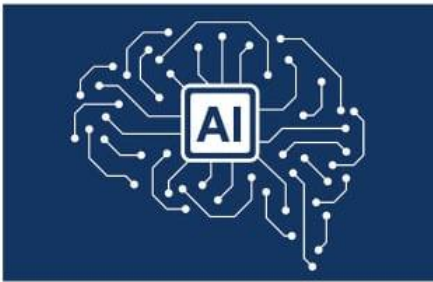
20 Days to Go: FutureCrime Summit 2025 Gears Up to Address Technology-Driven Crime

POLICY WATCH

Government Bans AI Tools Like ChatGPT in Offices Over Data Confidentiality Concerns



Published 1 day ago on February 7, 2025
By Swagta Nath



The **Finance Ministry** has issued a directive instructing its employees to strictly avoid using AI tools such as ChatGPT and DeepSeek on office computers and devices due to concerns over the confidentiality of government data and documents. The directive, issued by the Department of Expenditure on January 29, warns that AI applications pose potential security risks when used on official systems.

The advisory emphasizes that AI-based tools can compromise sensitive government information and, therefore, should not be used by employees in office environments. Employees are urged to strictly adhere to this policy, ensuring the protection of confidential documents from unauthorized access or leaks.

Register Now for FutureCrime Summit 2025 – Secure Your Spot Today!

This move aligns with global concerns over AI applications handling sensitive government data. Several countries have already restricted AI usage in government offices, particularly focusing on privacy risks associated



ADVERTISEMENT

ACC BUILD A DURABLE HOME WITH

- Right Material**
Consistent product quality
- Right Technique**
On-site services from ACC experts
- Right Experts**
Assistance from top experts

Call 1800 103 3444 to get ACC Certified Technology.

Voice cloning, fake couriers: How AI is supercharging Bengaluru's cybercrime

Police sources highlighted the increasing use of Artificial Intelligence (AI) to execute these scams, significantly boosting their effectiveness. Investigators have struggled to recover the stolen funds, with only 20 per cent of the lost amount retrieved.



Chetan B C

Last Updated : 16 January 2025, 02:30 IST

Follow Us :



Representative image indicating cybercrime Credit: iStock Photo

To avail Ambuja Certified Technology
Call - 1800 22 3010

Bengaluru: Nearly 78.7 per cent of the total Rs 2,270 crore lost to cybercrimes in Bengaluru between 2021 and September 2024 – amounting to Rs 1,788 crore – was siphoned off through six major fraud categories, according to police data.

ADVERTISEMENT

START HERE



Centre's Recent Move to Regulate Online Gaming Will Further the 'Illegalities' of IT Rules

Rights

These proposed amendments to incorporate rules for online gaming have been introduced by the government without any discussion or white paper.

Jan 04, 2023 | Tejasi Panjiar, Tanmay Singh and Prateek Waghre



Representative image. Photo: bestonlinecasinos/Pixabay

ADVERTISEMENT

Home > Business > 2000 Cyber Attacks Every 24 Hours On Indian Oil Companies: 3.6 Lakh Cyber Attacks Reported In 6 Months

BUSINESS

2000 Cyber Attacks Every 24 Hours On Indian Oil Companies: 3.6 Lakh Cyber Attacks Reported In 6 Months

By Shreya Bose — Last updated Apr 25, 2022



2000 Cyber Attacks Every 24 Hours On Indian Oil Companies: 3.6 Lakh Cyber Attacks Reported In 6 Months

A study conducted by CyberPeace Foundation, a civil society organisation found that Indian oil companies faced 3.6 lakh cyberattacks in six months.

STAY WITH US

Facebook Likes

478k Like our page

Followers Follow Us

Comments Comments

Instagram Followers

RSS Subscribe Follow Us

World Class Cloud GPU Infra based on NVIDIA T4

Starting @ 30/hour

All the GPU servers of EZ Networks run in Indian data centers, reducing latency.

www.eznetworks.com

RECENT POSTS



This Tata Company Will Launch IPO In September: Rs



Mastercard Become Title Sponsors Of All BCCI

INSTAGRAM PAGE SHARES PICS OF WOMEN ON BENGALURU METRO





Can AI-Generated Images Result in Jail Time in South Korea?



DIGIPIN

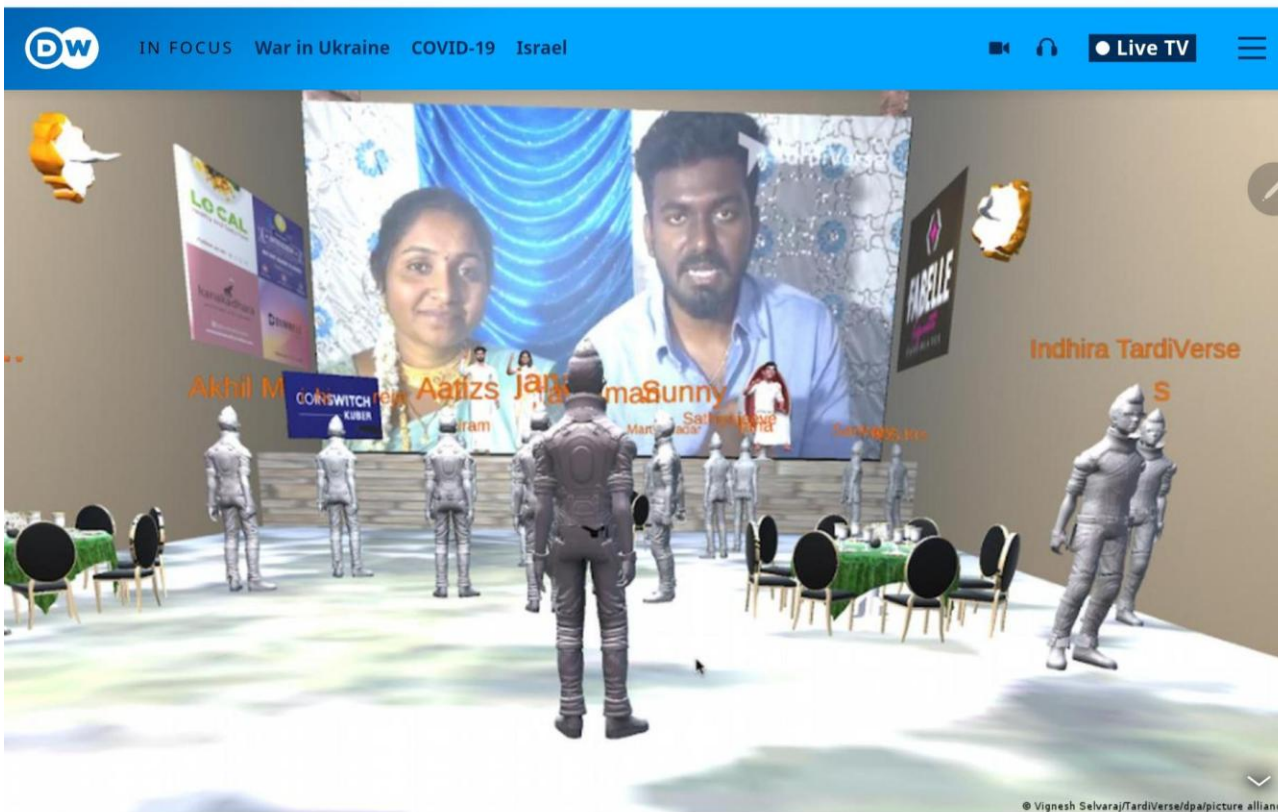


METAVERSE & INDIAN CYBER LAW



METaverse- DIGITAL CRIME & DIGITAL AVATAR





CULTURE | INDIA

Are 'metaverse' weddings the new normal in India?

Aparna Ramamurthy Tamil Nadu

02/22/2022

India is taking its big fat weddings to the next level with 'metaverse' ceremonies, which even the deceased can attend. COVID triggered a digital acceleration in India, but are 3D weddings really going to go mainstream?



USA
TODAY

SPRING CLEANING 🧹

Try this method

MENTAL HEALTH 🧠

Stars open up

WELLNESS GLOSSARY

Find what your feeling

AFRAID OF THE DARK? 🌑

You aren't alone

START
TRI
2 Month

News

Sports

Entertainment

[Life]

Money

Tech

Travel

Opinion



48°F 🌤️

Subscribe

Sign In ▾

HEALTH AND WELLNESS

A woman said she was 'raped' in the metaverse. When will it matter?



METaverse LAND- VIRTUAL LAND





HOME / UAE / HEALTH

Gitex 2022: Medcare emerges as UAE's first metaverse hospital

Healthcare chain aims to provide accessibility and affordability with full-scale Web 3.0 rollout



By Joydeep Sen Gupta

Published: Fri 14 Oct 2022, 5:47 PM

Medcare Hospitals & Medical Centres, under Aster DM Healthcare, has emerged as the UAE's first medical facility to be present in the metaverse, winning the historic race to the future by planning a full-scale rollout of their hospitals on Web 3.0.

Medcare is one of the largest healthcare provider chains in Dubai and Sharjah.



CULTURE | INDIA

Are 'metaverse' weddings the new normal in India?

Aparna Ramamurthy Tamil Nadu

02/22/2022

India is taking its big fat weddings to the next level with 'metaverse' ceremonies, which even the deceased can attend. COVID triggered a digital acceleration in India, but are 3D weddings really going to go mainstream?

Metaverse to be key enabler of Indian M&E sector



Synopsis

A new set of emerging technologies will drive digital transformation and define customer experience going forward. "Businesses will continue to adopt these technologies if it enables their vision to provide the best customer experience at a reasonable cost," said Ashvin Vellody, Partner, Consulting, Deloitte India.

ETTech

Dec 13, 2022, 06:00 AM IST



Deloitte's new report, **Metaverse: The Hype, Possibilities, and Beyond** said that one of the key drivers of economic possibilities within the metaverse will be Web3.0's ability to spur digital transformation. "The metaverse will serve as a key enabler for the **Indian** media and entertainment sector opening newer avenues for India's vast talent pool in engineering, graphics, video, and animation," said Jehil Thakkar, Partner and Media and Entertainment sector leader, **Deloitte India**.

A new set of emerging technologies will drive digital transformation and define customer experience going forward. "Businesses will continue to adopt these technologies if it enables their vision to provide the best customer experience at a reasonable cost," said Ashvin Vellody, Partner, Consulting, Deloitte India.

Home > automobile > Hyundai Motor India Launches Hyundai Pavilion On Metaverse

AUTOMOBILE

Hyundai Motor India Launches Hyundai Pavilion On Metaverse

Hyundai Pavilion on Metaverse will introduce the much-awaited all-electric SUV Hyundai Ioniq 5 for users to experience its various features.

Published: January 6, 2023 9:48 AM IST By Shubham Verma

ADVERTISEMENT

realme 10
From ₹12,999*
First sale on 15th Jan, 00:00Hrs



METaverse POLICING..



METaverse CITIZENSHIP



NEWS

[Home](#) | [War in Ukraine](#) | [Coronavirus](#) | [Climate](#) | [Video](#) | [World](#) | [Asia](#) | [UK](#) | [Business](#) | [Tech](#) | [Science](#)

More

Tech

ADVERTISEMENT

A PREMIER VIRTUAL EVENT
ZERO TRUST LIVE
Unveiling the next generation of zero trust, today.

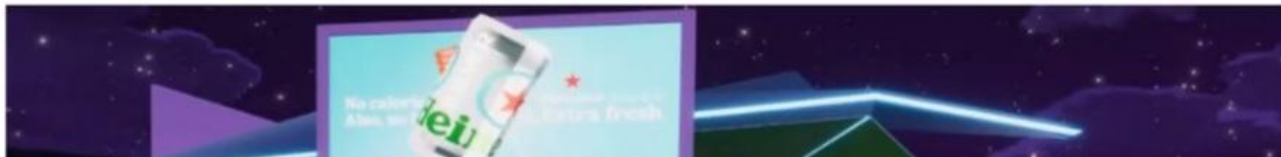


Register Now

Heineken launches virtual beer in self-mocking metaverse 'joke'

By Jane Wakefield
Technology reporter

🕒 2 days ago



Top Stories

🕒 **LIVE** Besieged city ignores
Moscow surrender deadline

Ukraine rejects Russian offer
to give up Mariupol

🕒 1 hour ago

Omicron vs Zero-Covid: How
long can China hold on?

🕒 2 hours ago

ADVERTISEMENT

NFT- NON FUNGIBLE TOKENZ



WEB 3.0



NEWS > CITIES > MUMBAI

Mumbai Court awards life imprisonment to computer engineer in cyber terrorism

Additional judge A. A. Joglekar noted that Ansari misused the access of authorised computers to threaten the sovereignty of India which falls under the purview of cyberterrorism.

The Hindu Bureau

MUMBAI

OCTOBER 22, 2022 16:07 IST

ADVERTISEMENT



CYBER SOVEREIGNTY

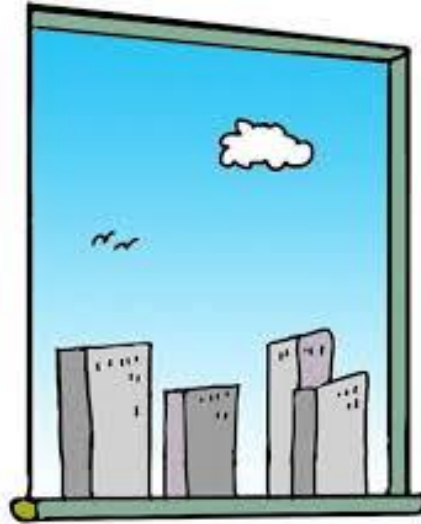
- ▶ The concept of Cyber Sovereignty has already seen evolution wherein countries have included not just the physical boundaries, but also have extended the same to the Outer Space, Deep Seabed, Arctic and Antarctic regions.





News

Gujarat High Court grants ₹1 lakh damages to man who spent 3 years in prison as jail authority could not open bail order attached to email



ALL I KNOW IS
THE BOSS SAID WE
HAD TO MONITOR
THE CLOUD.





I finally
realized it
that people
are prisoners
of their
phones that's
why it's
called Cell
Phones.

-- Arrested --

Amit Singh frequently served as a guest lecturer on ethical hacking and cybercrime threats at police institutions and universities ..

Beware of such Fake Tech Consultant !!!



Ethical Hacker's Dark Side: 'Digital Bhuva' Amit Singh Nabbed in Extortion and Threats Case - The420CyberNews

the420.in • 3 min read



90's: "don't sit too close to the tv"

2023:





India's First AI News Anchor Launched At India Today Conclave 2023 | Meet Ageless & Tireless Sana

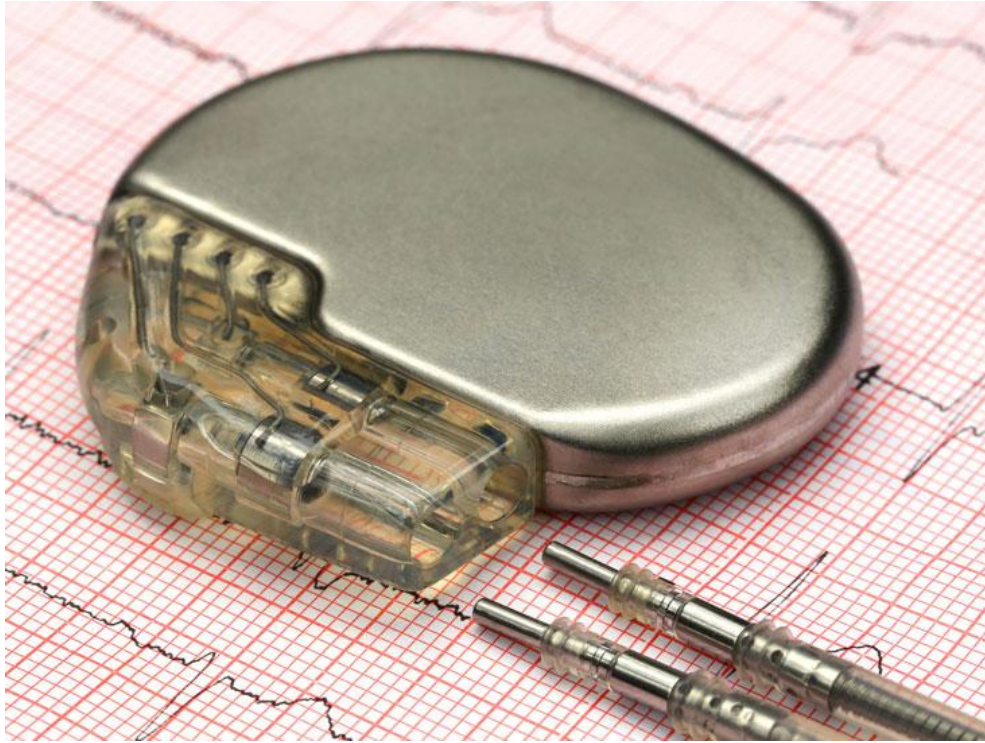
16,954 views · 8 days ago #indiatodayconclave2023 #indiatodaymore



DID YOU KNOW ?

**WOMAN FOUND OUT HER
BOYFRIEND WAS CHEATING WHEN
FITBIT WATCH SHOWED A SPIKE AT
2 AM . THEY HAD SYNCED THE FITBIT
WATCH TOGETHER AND SHE GOT A
NOTIFICATION THAT HE BURNED 500
CALORIES AT 2 AM .**

PACEMAKER AS DIGITAL EVIDENCE....



IoT CASE STUDY - 1-WITNESS “ALEXA”- IoT Device

- ▶ WITNESS - “ALEXA” - CALLED - GIVE EVIDENCE - MURDER INVESTIGATION- FLORIDA
- ▶ A WOMAN WAS KILLED BY A SPEAR- FLORIDA, - JULY 2019
- ▶ ALEXA -AUDIO RECORDINGS - DURING ATTACK
- ▶ DIGITAL EVIDENCE - SOLVE THE MURDER



IoT DEVICES AS EVIDENCE

▶ IOT DEVICES- AMAZON ECHO AS EVIDENCE

- ▶ In 2015, James Bates was charged with the murder of Victor Collings, who was found strangled and drowned in Bates's hot tub. Though Bates claims it was probably accidental drowning and that he was asleep at the time of death. However, based on inconsistencies in the timeline and his story, the police suspected him of the murder.
- ▶ Further, among the IoT devices possessed by Bates, the police sent a warrant to Amazon asking for recordings from his Amazon Echo. Home Assistant Devices such as Google Home, Echo have mics that are always recording. This data could potentially break open the case.

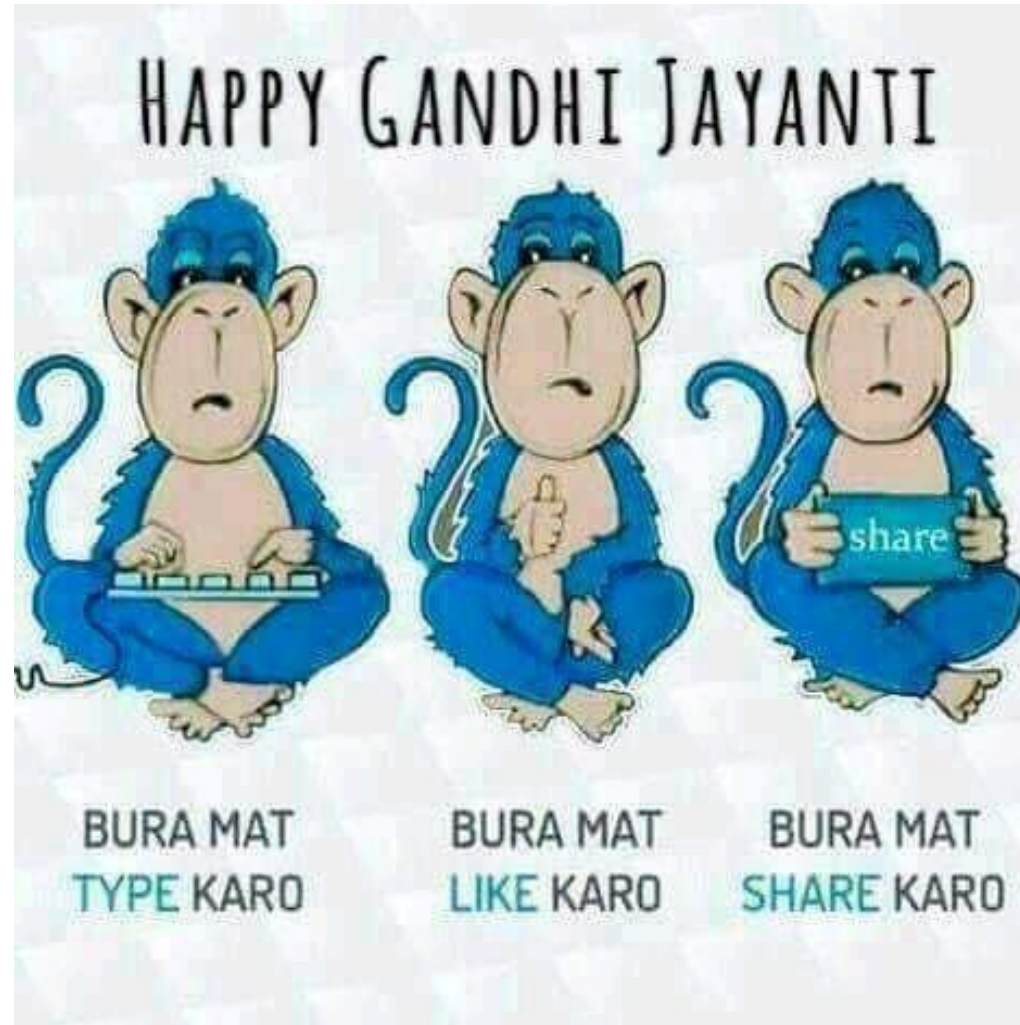


IoT CASE STUDY- 2 -GEOLOCATION DATA- DENMARK- MOBILE PHONE

- ▶ DENMARK RELEASED 32 PRISONERS
- ▶ RELIABILITY OF GEOLOCATION DATA - MOBILE PHONE - MOBILE NETWORK OPERATORS
- ▶ SOFTWARE- SYSTEM - CONNECTED TO SEVERAL TOWERS AT ONCE-
- ▶ WRONGFUL CONVICTIONS



CYBER VERSION...



STRATEGY....

Chinese : We will hack Indian
Database
Indian : Le Le



IT ACT...





**HIGH SPEED
DATA TRANSFER**

And the password is...
'Don't tell anyone'

Upgrade your digital skills or
perish. Applies to everyone 🤖🤖

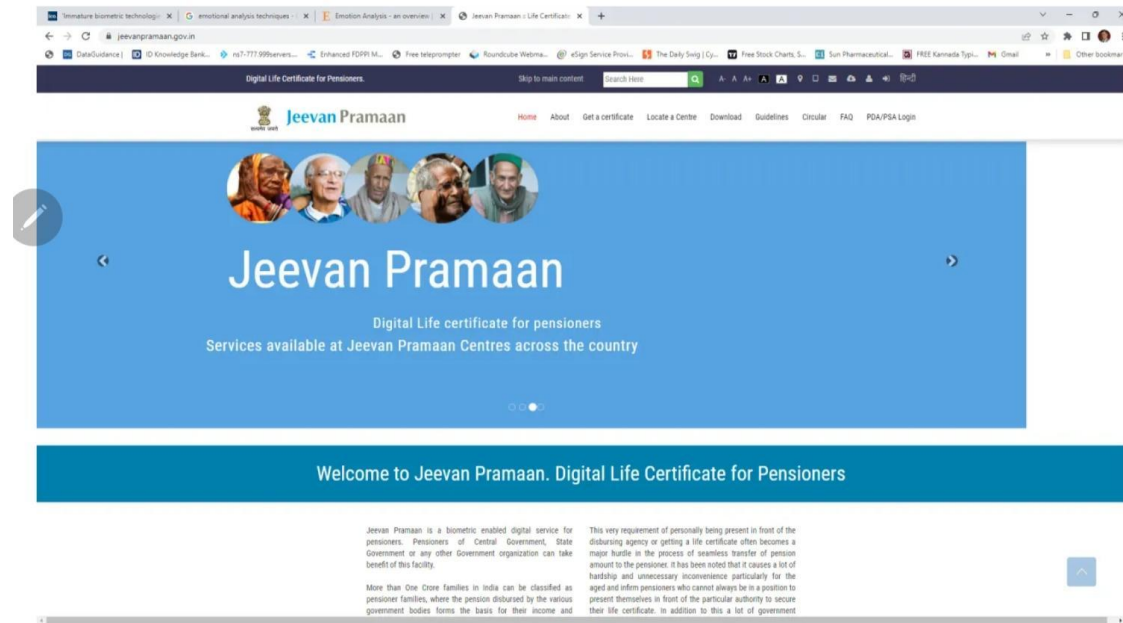


NEW CYBER FRAUD..

A Russian cosmonaut in a white spacesuit is shown floating in space. The cosmonaut is wearing a white helmet with a gold visor and has a Russian flag patch on the chest. The background is a dark, starry space.

Fake Russian Astronaut Duped Woman Of Rs 24 Lakh, Said He Needed Money To 'Return To Earth'

WEBSITE PHISHING & NEW SEARCH ENGINE FRAUD



SWEET & CRYPTO...

Soan Papdi is the original crypto currency. No utility, only gifting value, and you can never tell who the original owner is.

FANCY WEBINAR FRAUDS..



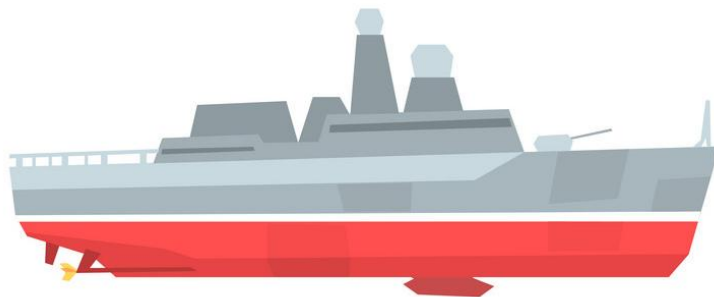
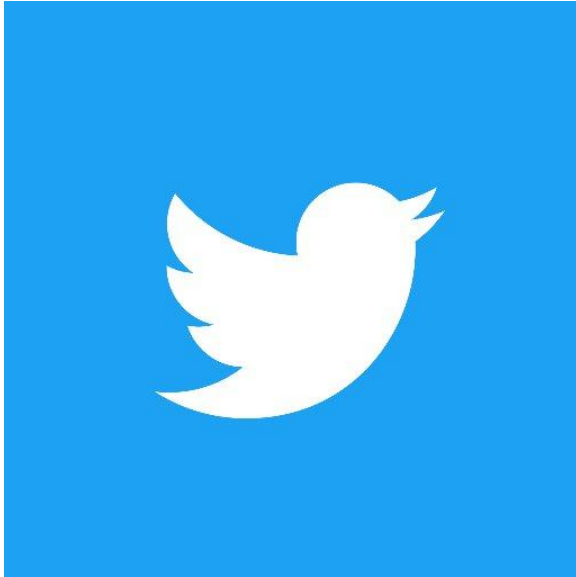


inshorts

In a bid to get refund of ₹578 from IRCTC, Mumbai man loses ₹1.78 lakh

A man lost ₹1.78 lakh to a cyber fraudster while he was trying to get a refund of ₹578 from Indian Railway Catering and Tourism Corporation (IRCTC). An FIR was registered at Tardeo police station. Reports said that the man searched for IRCTC's helpline number online and got connected to cyber fraudster. He extorted man's bank details and cheated him.

TWITTER- SAILOR CASE...



IOT CASE STUDY.....

▶ SMART TV CASE STUDY- MALAYSIA



HACKING OF IT ACCOUNTS

► CA STUDENT



CYBER MURDER



Tracer



CASE STUDY

- ▶ HUSBAND SUSPECTS WIFE
- ▶ GIFTS HER A DIAMOND STUDED MOBILE
- ▶ HAS A PROGRAM/TOOL PRE-INSTALLED ON PHONE
- ▶ TO COLLECT ALL DATA - GATHER EVIDENCE
- ▶ MATRIMONIAL DISPUTE



CYBER INSURANCE

 newsorigins.com/cyber-liability-insurance-market-58029/ 



TECHNOLOGY

Cyber (Liability) Insurance Market 2021-2026 analysis examined in new Industry research report

 Published: 22 hours ago  Admin [Request Free Sample](#)



Statistics presented in research report on the Cyber (Liability) Insurance market demonstrate the present growth rate and potential for the future over the assessment period of 2022-2028. It encompasses pivotal factors such as growth drivers and opportunities, as well as concrete responses to urgent threats, to facilitate a clear understanding of market dynamics.

Apart from that, the market is expected to showcase a decent growth rate as supported by reliable primary and secondary research methodologies.

A comprehensive analysis of the key market segments is also provided. For the benefit of stakeholders, the competitive landscape prevalent within the industry space is overtly assessed on the basis of their product offerings, financials, pricing model and research and development

Cyber security



- ▶ The term “Cyber Security” has been newly added in the IT Amended Act 2008, under Section 2 (nb) which is as under-
- ▶ “Cyber Security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.



E-CONTRACTS & DIGITAL SIGNATURES

- ▶ E-contracts - Click Wrap, Browse Wrap etc
- ▶ Digital Signatures - authentication
- ▶ Electronic Signatures - IT Amended Act 2008



DIGITAL SIGNATURE & ELECTRONIC SIGNATURE



Digital
Signatures

&



Electronic
Signatures

Create digital signature

Signature valid

Digitally signed by PlotSoft LLC
Date: 2013.05.06 21:03:05:00
Reason: I'm the author
Location: USA



Valid signature



REGISTRATION OF PROPERTY- DIGITAL SIGNATURE

- ▶ Registration of Property- using
- ▶ Digital Signature
- ▶ Esign
- ▶ Execute all or any property transaction docs
- ▶ Power of Attorneys, Cheques

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

NOTIFICATION

New Delhi, the 26th September, 2022

S.O. 4720(E).—In exercise of the powers conferred by the proviso to sub-section (4) of section 1 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following amendments to the First Schedule of the Act, namely:—

2. In the said Schedule,—

(i) for serial number 1 and the entries relating thereto, the following serial number and entries shall be substituted, namely:—

“1. A negotiable instrument (other than a cheque, a Demand Promissory Note or a Bill of Exchange issued in favour of or endorsed by an entity regulated by the Reserve Bank of India, National Housing Bank, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority) as defined in section 13 of the Negotiable Instrument Act, 1881 (26 of 1881).”;

(ii) in the entries relating to serial number 2, after the words, figures and brackets “the Powers-of-Attorney Act, 1882 (7 of 1882)”, the words “but excluding those power-of-attorney that empower an entity regulated by the Reserve Bank of India, National Housing Bank, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority to act for, on behalf of, and in the name of the person executing them.” shall be inserted;

(iii) serial number 5 and the entries relating thereto shall be omitted.

[F. No. 1(3)/2022-CL]

Dr. RAJENDRA KUMAR, Addl. Secy.

INTERMEDIARY UNDER IT ACT

- ▶ The Indian Cyber law has also come up with a unique concept known as “intermediaries”. Intermediary is defined under Section 2(1)(w) of the amended Information Technology Act, 2000 in the widest possible terms.
- ▶ Any person who on behalf of another person receives, stores or transmits any particular electronic record or provides any service with respect to that record becomes an intermediary in India.

INTERMEDIARIES INCLUDE BUT NOT LIMITED TO

- ▶ Telecom Service Providers, Network Service Providers, Internet Service Providers, Web Hosting Service Providers, Search Engines, Online Payment Sites, Online Auction Sites, Online Marketplaces and Cybercafés.
- ▶ Further the law has also stipulated the liability of intermediaries for any third-party data, information or communication link made available by them.

Who is an Intermediary?

- ▶ COMPANY - ENTITIES
- ▶ ASSOCIATION
- ▶ TRUST
- ▶ PROFESSIONAL
- ▶ COLLECTING INFO- IN DIGITAL OR E-FORM, PROVIDING SERVICES, ON ITS OWN OR BEHALF OF ANY PERSON, ENTITY

SEC 67C - IT ACT- INTERMEDIARIES

- ▶ Preservation and retention of information by intermediaries.
- ▶ -(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- ▶ (2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.]

SEC 72 A-CRIMINAL OFFENCE

- ▶ Punishment for Disclosure of information in breach of lawful contract -
- ▶ Any person including an intermediary who, while providing services under a lawful contract, has secured access to any material containing “**Personal Information**” about another person, discloses such information knowingly or intentionally
- ▶ Imprisonment up to 3 years or fine up to 5 lakh or with both (Cognizable but Bailable)

Criminal
Minds



EXPOSURE TO LIABILITIES

- ▶ CIVIL LIABILITIES- DAMAGES BY WAY OF COMPENSATION
- ▶ 5 CRORE RUPEES PER CONTRAVENTION
- ▶ CRIMINAL LIABILITIES
- ▶ 3 YRS - LIFE IMPRISONMENT
- ▶ FINE - Rs.1 lakh- 10 lakhs



Who is liable ?

► Sec.85: Offences by companies

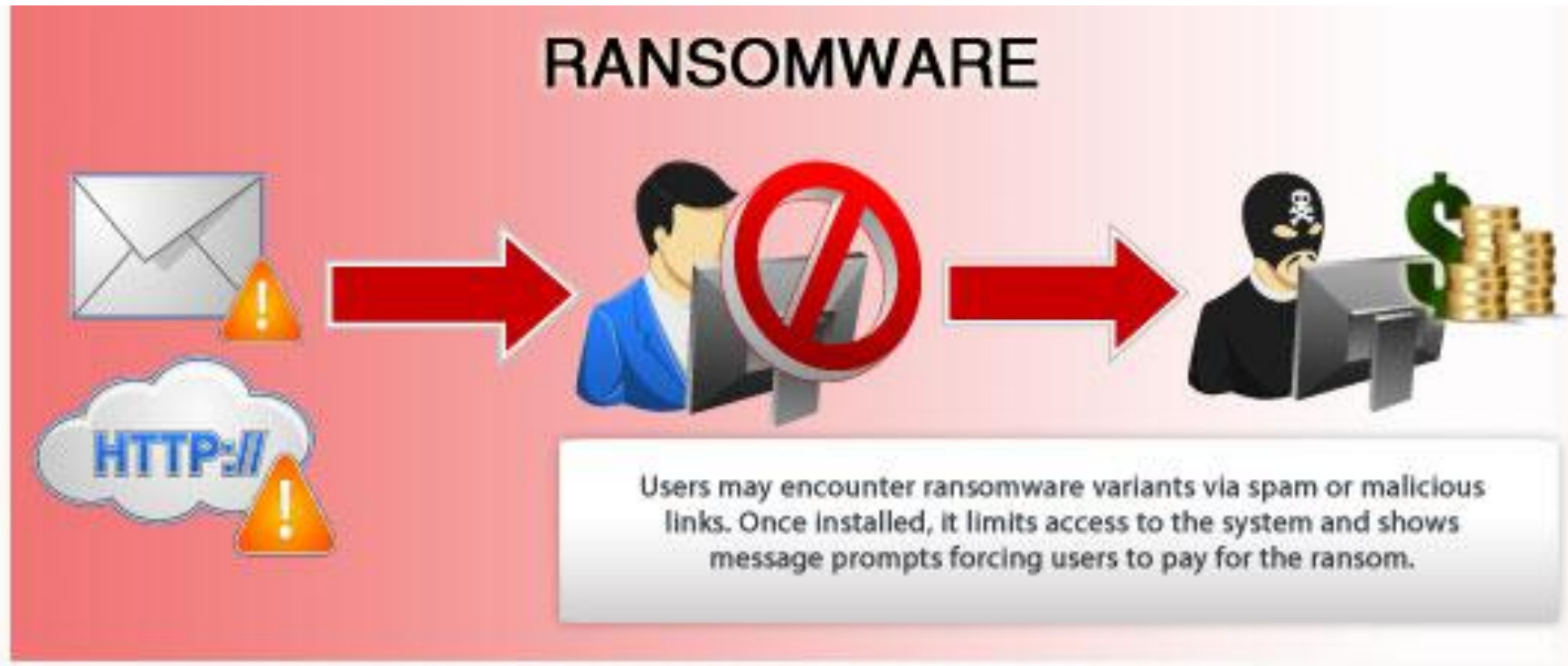
- The company itself, being a legal person;
- The top management including directors; and
- The managers (persons directly responsible for the data)

If it is proved that -

- they had knowledge of a contravention; or
- they have not used due diligence
- that it was caused due to their negligence



RANSOMWARE



CERT-IN GUIDELINES & APPLICABILITY

- ▶ This is in reference to the Guidelines and Directions issued by CERT-In Government of India Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (CERT-In) by way of No. 20(3)/2022 issued on 28th April 2022 under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet for all Body Corporate, Intermediaries, Service Providers, Governmental Organisations, Professionals, Sole Proprietors, Associations including Trusts

WHAT CERTIN GUIDELINES MEAN FOR YOUR ORGANISATION

- ▶ MANDATED LOGS RETENTION AND SECURED MAINTENANCE- ICT SYSTEMS- 180 days
- ▶ REPORTING - CYBER SEC BREACHES- 6 Hours
- ▶ DATA LOCALISATION
- ▶ REPORTING VIA EMAIL, FAX, PHONE
- ▶ POINT OF CONTACT- APPOINTMENT

REPORTING- CYBER SEC BREACHES

- ▶ Targeted scanning/probing of critical networks/systems
- ▶ Compromise of critical systems/information
- ▶ Unauthorised access of IT systems/data
- ▶ Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- ▶ Malicious code attacks such as spreading of virus/worm/Trojan/Bots/Spyware/Ransomware/Cryptominers
- ▶ Attack on servers such as Database, Mail and DNS and network devices such as Routers
- ▶ Identity Theft, spoofing and phishing attacks
- ▶ Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- ▶ Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
- ▶ Attacks on Application such as E-Governance, E-Commerce etc.

- ▶ Data Breach
- ▶ Data Leak
- ▶ Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
- ▶ Attacks or incident affecting Digital Payment systems
- ▶ Attacks through Malicious mobile Apps
- ▶ Fake mobile Apps
- ▶ Unauthorised access to social media accounts
- ▶ Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
- ▶ Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones
- ▶ Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning

LIABILITY - IN CASE OF NON-COMPLIANCE- CERTIN GUIDELINES 2022

- ▶ CIVIL LIABILITY- Sec 43 - IT Act - Upto INR 5 Crores- per contravention
- ▶ CRIMINAL LIABILITY- Sec 85- Top Management, Middle Management and every stake holder responsible in Organisation- Can be jailed
- ▶ COMPANIES ACT 2013- Liability- Sec 134 (3) (n), Section 402
- ▶ Section 70 (B)(7)- One Year of Imprisonment or One Lakh Rupees Fine or Both
- ▶ ISO Certification- cannot be renewed - in case of non-compliance



LIABILITIES..

- ▶ ISMS Audit- Control A 18.1.1
- ▶ Annual Financial Audit- Imprisonment- exist a risk- however remote
- ▶ Non- reporting of complete cyber security incident - Civil & Criminal Liability
- ▶ Manipulation or Tampering of Logs- Sec 463, 468, 469 - IPC- Criminal Liability- Sec 65, 66, 43, 43A, 72- IT Act



LOSS OF REPUTATION, TRUST- BEYOND CALCULATIONS..



IN CASE OF NON- REPORTING-



SOCIAL MEDIA, OTT GUIDELINES 2021



IT RULES 2021

- ▶ PERIODICAL INTIMATION- ATLEAST ONCE AN YEAR-
- ▶ NON- COMPLIANCE:
 - ▶ • PRIVACY POLICY
 - ▶ • TERMS & CONDITIONS
 - ▶ • USER AGREEMENT
 - ▶ • DATA PROTECTION AGREEMENTS



► NOT TO DISPLAY, HOST, UPLOAD, MODIFY, PUBLISH, TRANSMIT, STORE, UPDATE, SHARE the following Information

- That belongs to any other person of which you have no right
- Defamatory
- Obscene, pornographic, paedophilic
- Invasion of Privacy
- Bodily injury, insult or harass- on the basis of gender
- Libelous
- Racially or ethnically objectionable
- Relating or encouraging money laundering or gambling
- Harmful to children



- IP infringement- Trademark, Copyrights, Patents or other Proprietary Rights
- Violates any Law being in force
- Any info- that deceives, misleads the origin of the message- knowingly, intentionally
- Impersonation
- Threatening the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, public order, causes incitement to the commission of any cognizable offence, prevents investigation of any offence, insulting other nations
- Contains Software Virus or any other computer code, file, program designed to interrupt, destroy or limit the functionality of any computer, computer resource
- Any info- patently false, untrue- written or published in any form- intent to mislead, harass a person, entity or agency for financial gain or to cause any injury to any person



- ▶ NON-HOSTING, NON- STORAGE, NON- PUBLISHING- UNLAWFUL INFORMATION-
COMPUTER RESOURCES-
- ▶ • RECEIVING KNOWLEDGE
- ▶ • ORDER - COURT, GOVT.,
- ▶ ❖ SOVEREIGNTY, INTEGRITY OF INDIA
- ▶ ❖ SECURITY OF STATE
- ▶ ❖ FRIENDLY RELATIONS WITH FOREIGN STATES
- ▶ ❖ PUBLIC ORDER
- ▶ ❖ MORALITY, DECENCY
- ▶ ❖ CONTEMPT OF COURT
- ▶ ❖ DEFAMATION
- ▶ ❖ INCITEMENT TO AN OFFENCE
- ▶ ❖ ANY INFO-PROHIBITED BY LAW



ANY INFO- HOSTED, STORED, PUBLISHED

- ▶ ANY INFO- HOSTED, STORED, PUBLISHED-
 - ▶ • REMOVE
 - ▶ • DISABLE ACCESS
- ▶ TIMELINE- WITHIN 36 HOURS- COURT ORDER, GOVT. ORDER



ANY INFO- HOSTED, STORED, PUBLISHED

- ▶ ANY INFO- HOSTED, STORED, PUBLISHED-
- ▶ • REMOVE
- ▶ • DISABLE ACCESS
- ▶ ❖ VOLUNTARY REMOVAL
- ▶ ❖ GRIEVANCES



PROVIDE INFO

- ▶ PROVIDE INFO-
- ▶ • COURT ORDER, GOVT. ORDER- IN WRITING, PURPOSE- SEEKING INFO
- ▶ • TIMELINE- WITHIN 72 HOURS
- ▶ • ASSISTANCE- INVESTIGATION, CYBER SECURITY INCIDENTS
- ▶ PROSECUTION OF OFFENCES, VERIFICATION OF IDENTITY



TECH CONFIG

- ▶ TECHNICAL CONFIGURATION
 - ▶ • NOT KNOWINGLY
 - ▶ ❖ DEPLOY
 - ▶ ❖ INSTALL
 - ▶ ❖ MODIFY



- ▶ TECHNICAL CONFIG- THAT MAY CHANGE OR HAS THE POTENTIAL TO
- ▶ CHANGE THE NORMAL COURSE OF OPERATION - COMPUTER
- ▶ RESOURCE
 - ▶ • DEVELOP, PRODUCE, DISTRIBUTE, EMPLOY- TECHNOLOGICAL
- ▶ MEASURES- PURPOSE - SECURING COMPUTER RESOURCE AND
- ▶ INFORMATION CONTAINED THEREIN

GRIEVANCE- REPORTING & MECHANISM

- ▶ GRIEVANCE - ACKNOWLEDGEMENT
- ▶ TIMELINE- WITHIN 24 HOURS - FROM THE TIME OF RECEIPT OF GRIEVANCES
- ▶ GRIEVANCE - DISPOSAL AND RESOLUTION
- ▶ TIMELINE- WITHIN 15 DAYS - FROM THE TIME OF RECEIPT OF GRIEVANCES
- ▶ ACKNOWLEDGE- COURT ORDERS, GOVT. ORDERS
- ▶ GRIEVANCE OFFICER- ACKNOWLEDGE
- ▶ DETAILS OF GRIEVANCE OFFICERS - SHOULD BE PUBLISHED - RESIDENT INDIAN



SPECIFIC GRIEVANCES-

- ▶ SPECIFIC GRIEVANCES- ELECTRONIC FORM
 - ▶ • NUDITY
 - ▶ • SEXUAL ACTS OR CONDUCTS
 - ▶ • PERSONAL PRIVACY
 - ▶ • IMPERSONATION
 - ▶ • ARTIFICIALLY MORPHED IMAGES
- ▶ TIMELINE- 24 HOURS- REMOVAL, DISABLING ACCESS



DATA RETENTION- IT RULES 2021

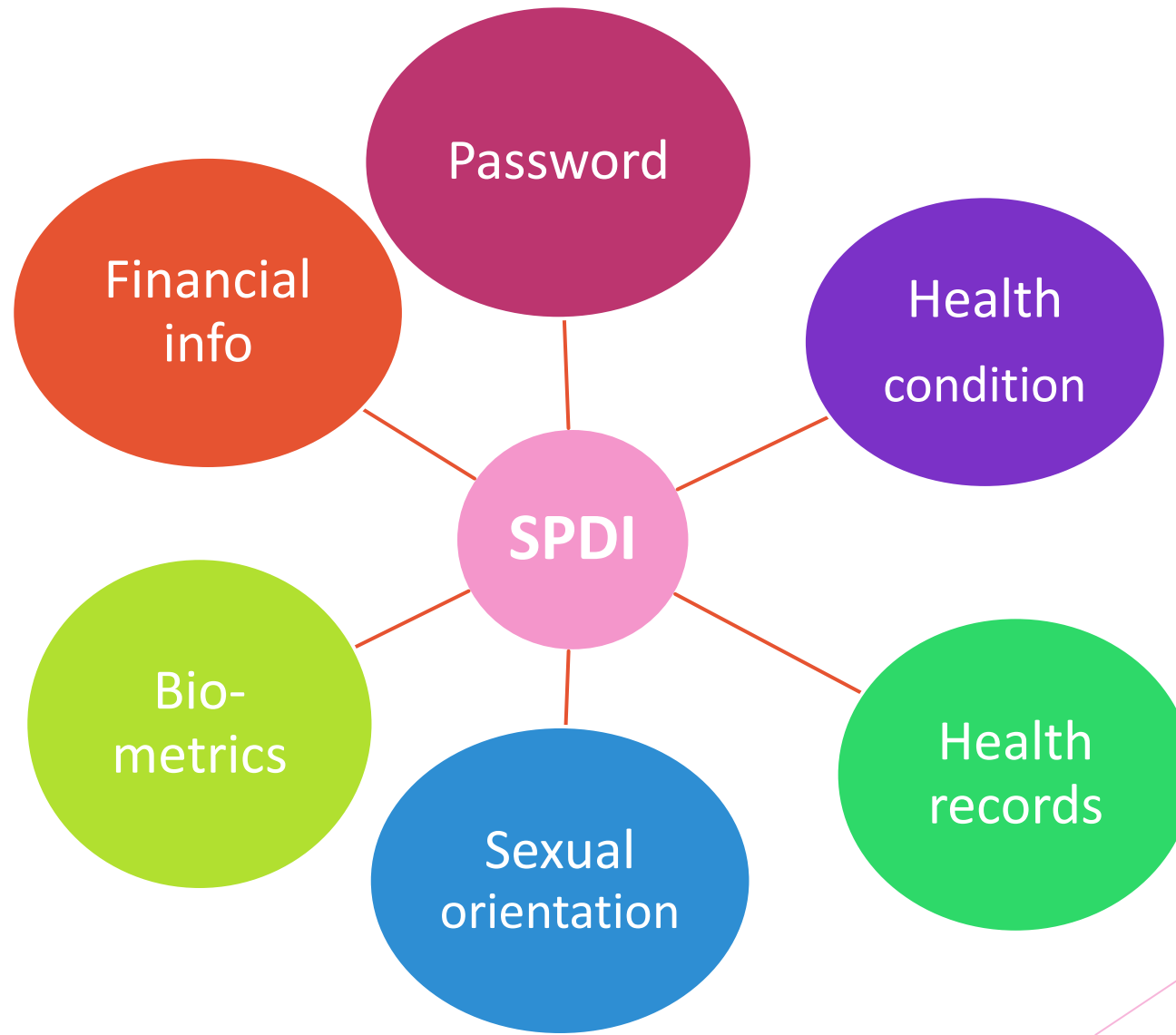
- ▶ DATA RETENTION
- ▶ TIMELINE: 180 DAYS - DATA RETENTION



NON- OBSERVANCE OF RULES

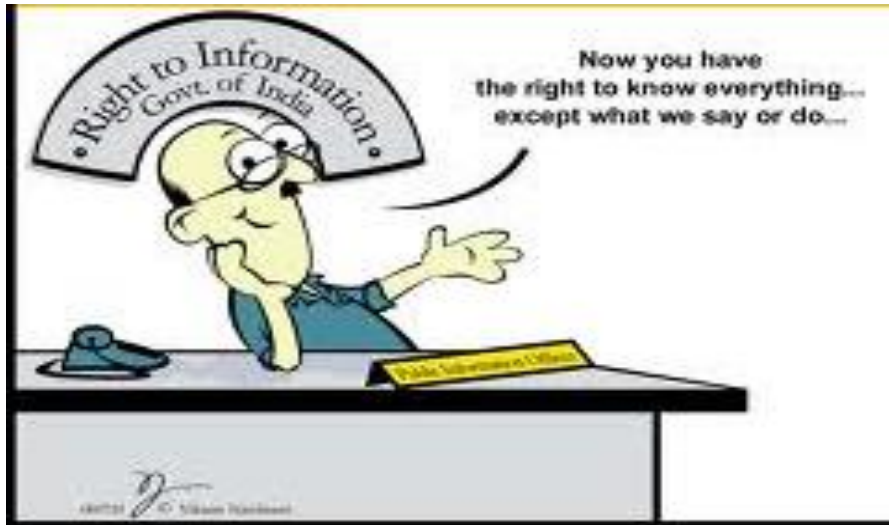
- ▶ RULE 7-
- ▶ SEC 79- IT ACT- NOT APPLICABLE
- ▶ Where an intermediary fails to observe these rules, the provisions of
- ▶ sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary
- ▶ shall be liable for punishment under any law for the time being in force including the provisions of the Act
- ▶ and the Indian Penal Code.

SENSITIVE PERSONAL DATA OR INDORMATION UNDER LAWS



EXCEPTION & damages

- ▶ Any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law will not be regarded as sensitive personal data or information for the purposes of law.



PERSONAL INFO- under IT Rules 2011

- ▶ Sec 2(1)(i)- IT RULES 2011
- ▶ “Personal Information” means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

LEGAL DEFINITION OF COMPUTER

- ▶ Sec 2(1)(i)- IT Act
- ▶ "Computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;



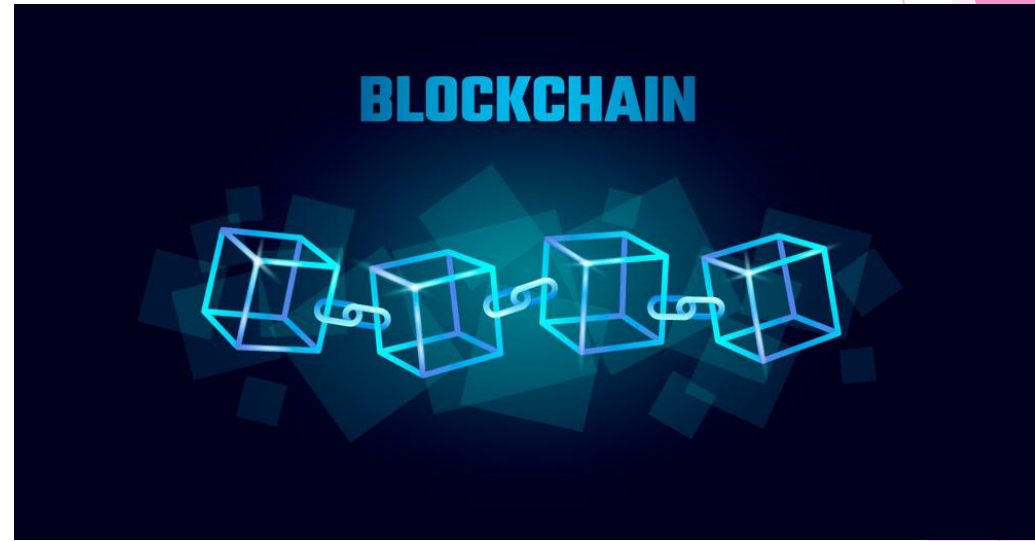
COMMUNICATION DEVICES

- ▶ Similarly the word ‘communication devices’ inserted in the Information Technology Amended Act 2008 has been given an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as iPad or other similar devices on Wi-Fi and cellular models.



BALKANIZATION OF INTERNET





FAKE, FAKE, FAKE ALL AROUND

- ▶ FAKE APPS
- ▶ FAKE MOBILE RECHARGES
- ▶ FAKE VACCINES
- ▶ FAKE NETFLIX SUBSCRIPTION
- ▶ FAKE CHARITIES / DONATIONS
- ▶ FAKE VACCINES, TESTING KITS & GOODS





High speed data
transfer 🤗

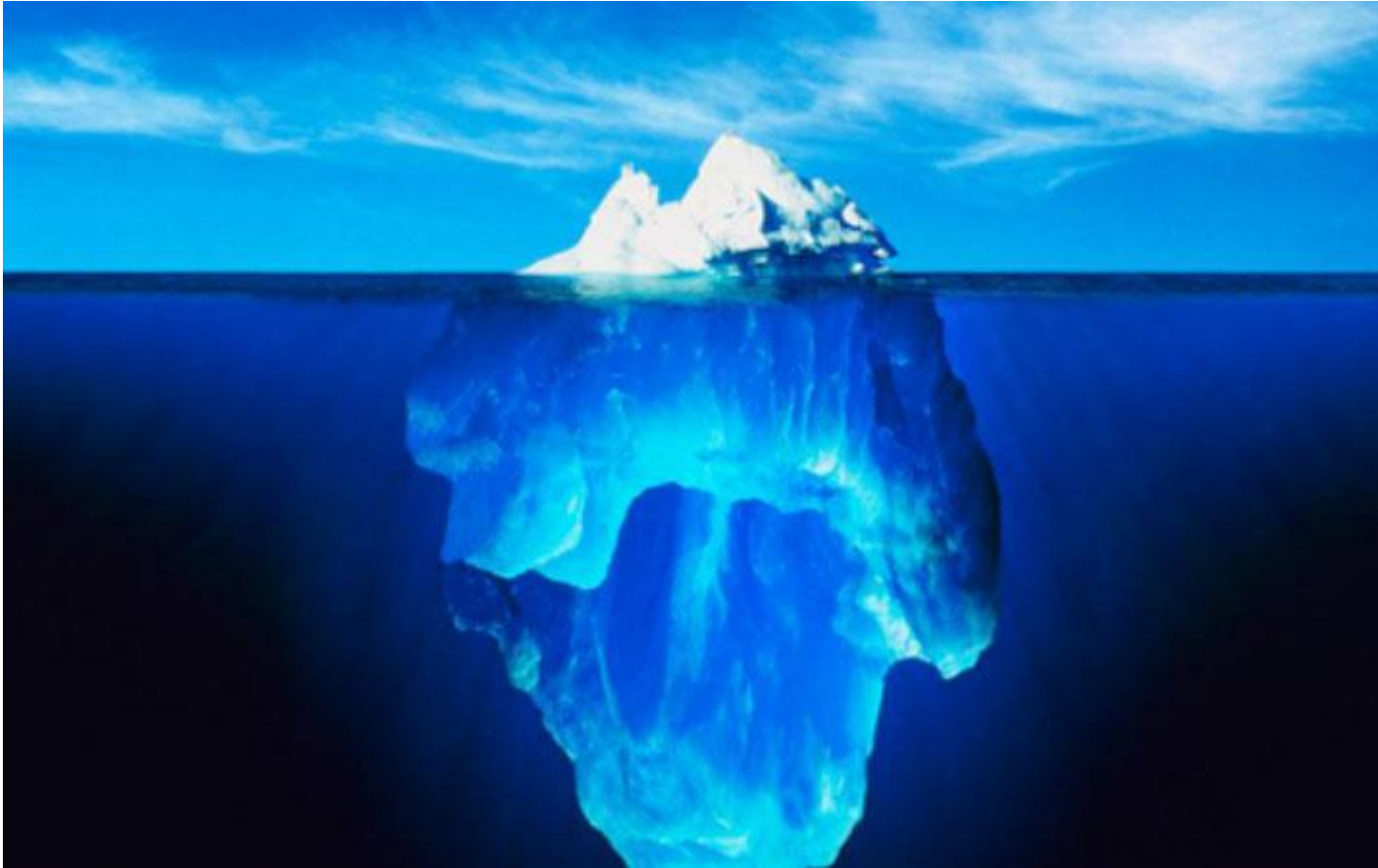
And the Password is "DON'T TELL
ANYONE" 🤗🤗🤗



HIGH SPEED
DATA TRANSFER

And the password is...
'Don't tell anyone'

DARKNET & CYBER SECURITY



NET WE ACCESS



DARK NET

Chennai police book photographer for video tweet on health secretary

TNN | Apr 30, 2020, 08:43 IST

✉️ 🖨️ A- A+



CHENNAI: The cybercrime wing of the city police said an FIR has been registered

A cybercrime store is selling access to more than 43,000 hacked servers

The MagBo portal provides access to hacked servers, with some belonging to local and state government, hospitals, and financial organizations.



By [Catalin Cimpanu](#) for [Zero Day](#) | May 14, 2020 -- 11:52 GMT (17:22 IST) | Topic: [Security](#)



MORE FROM CATALIN CIMPANU

Security
[Joomla team discloses data breach](#)

Windows 10
[How to tell if your device is eligible for the Windows 10 May 2020 update](#)



IFFCO-TOKIO is a leading private general insurance...

Ad IFFCO-TOKIO



Millionaire mom exposes: Make lakhs per month from...

Ad Style & Life

Home > India > News >> Lockdown: 366 Cases In Maha For Social Media Posts

Lockdown: 366 cases in Maha for social media posts

PTI | MAY 10, 2020, 16:56 IST



BUSINESS
INSIDER
INDIA

EXPAND

NO TOBACCO DAY

Like your LUNGS

WITH

NIX IT.

₹49* Only

NIX IT. NIX IT.

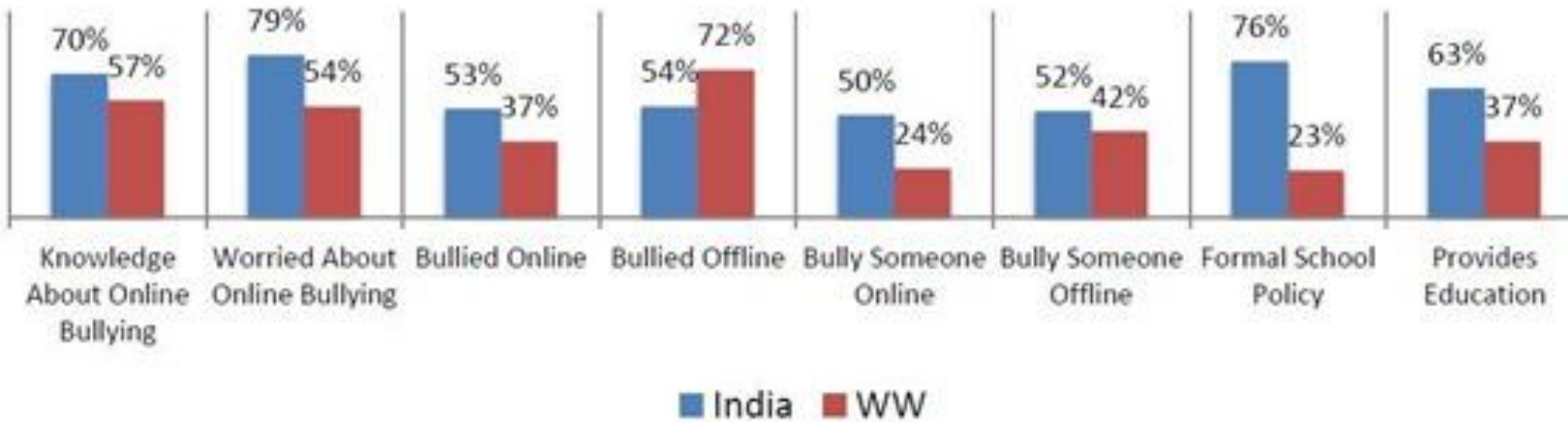
3 MONTHS

SHOP NOW

Smoking is injurious to health.
#Then quitting needed; J. Baner Med. 1980 Sep;2(3):243-51.

CYBER BULLYING

Online Bullying Metrics: India vs. Worldwide Average



Support the Free Press

scroll.in
Monday, June 1st 2020

Home Coronavirus Crisis Food Video The Latest The Reel The Field Trending ▾ Sections ▾

Exchange The Plus

the **Make LEAP**

Students save **60%** on Adobe Creative Cloud [Buy now](#)

INTERNET EFFECTS

In one year alone, cyberbullying of Indian women and teenagers rose by 36%

Meanwhile, conviction rates in this period fell to 25% from 40%.

CYBER-BULLYING IS NOT OK!



CYBER HARRASSMENT

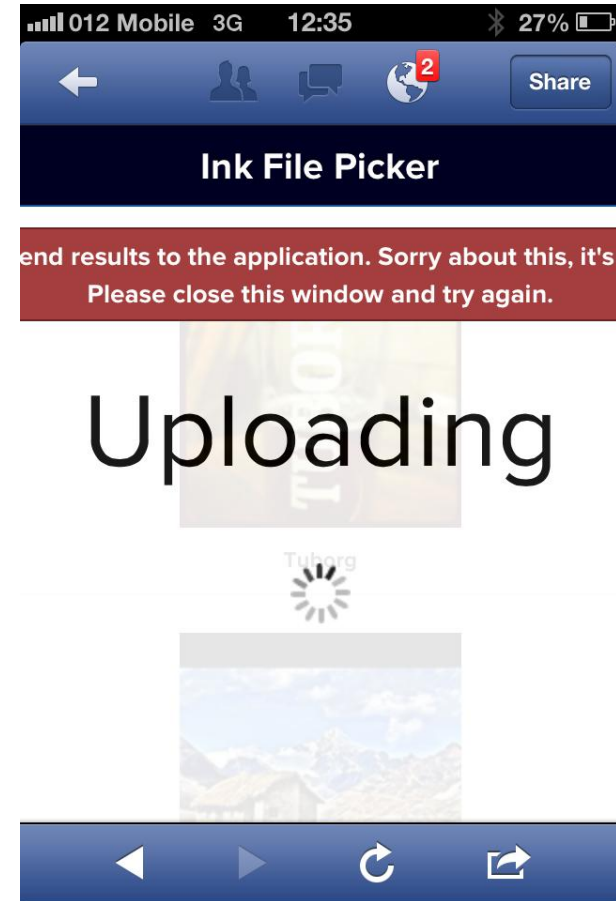


PHISHING



MOBILE UPLOADS

- ▶ UPLOADING PICS FROM MOBILES
- ▶ ESP SMART PHONES
- ▶ LATITUDES & LONGITUDES - CAN BE CAPTURED
- ▶ LOCATION CAN BE TRACED



WHATSAPP

- ▶ NO PRIVACY
- ▶ TERMS & CONDITIONS
- ▶ WHATEVER U POST IS NOT YOUR CONTENT
- ▶ STATUS SUBMISSION
- ▶ AUDIO/VIDEO/IMAGE/TEXT
- ▶ BECOMES INFO IN PUBLIC DOMAIN

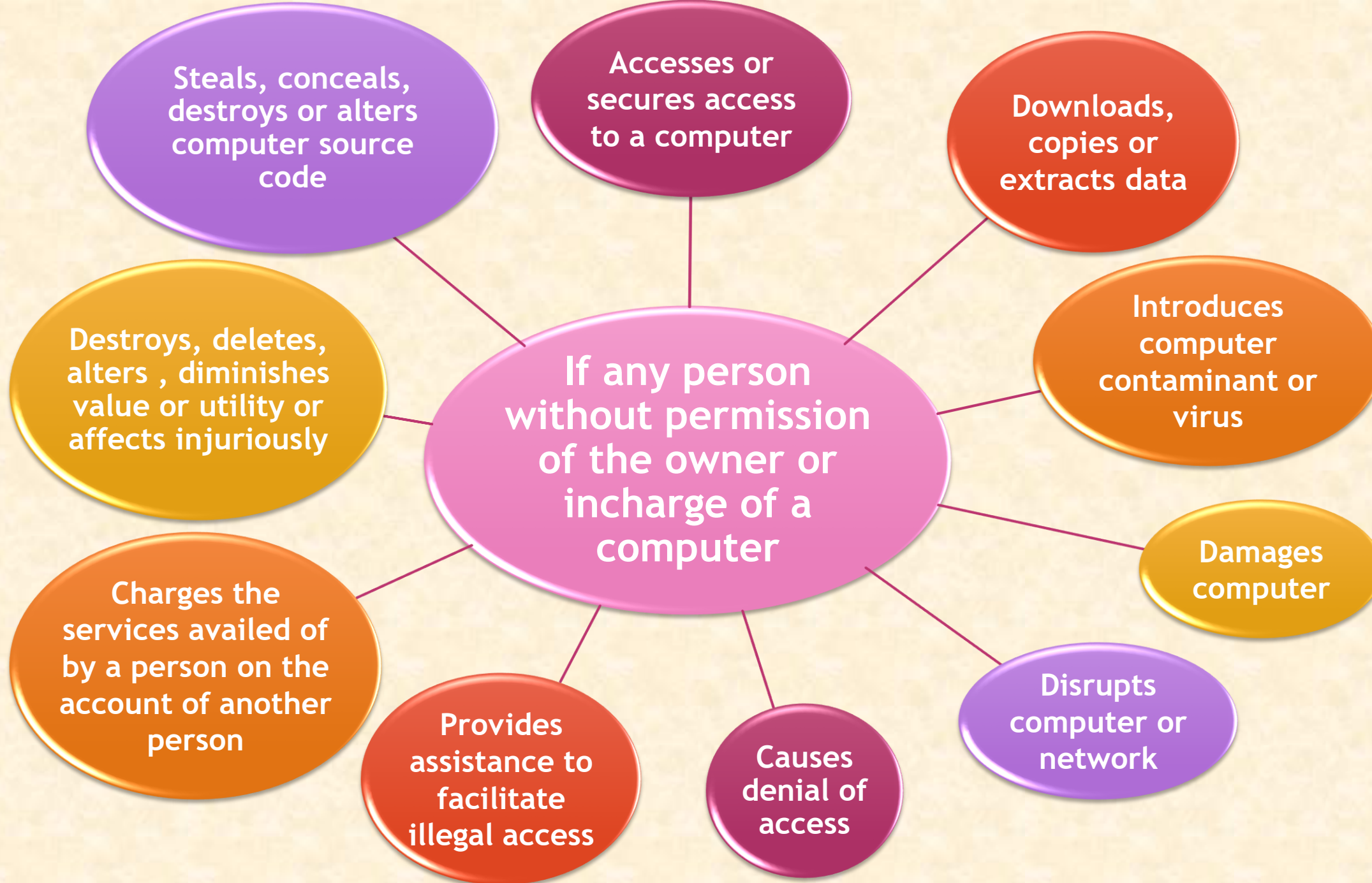


SEC 43- IT ACT

- ▶ **Section 43 - Unauthorized Access**
- ▶ Damages can be claimed by way of compensation



Compensation & Benefits



THEFT OF COMPUTER SOURCE CODE

- ▶ Theft or Tampering of Computer Source Code is defined under Sec 65 of the I.T Act 2000.
- ▶ For the purpose of this section "Computer Source Code " includes :-
 1. Listing of Programs
 2. Computer Commands
 3. Design and Layout
 4. Program Analysis of computer resource in any form

**SOURCE
CODE**



OFFENCES IN RESPECT OF COMPUTER SOURCE CODE



The following are the offences in respect of computer source code maintained by law.

- ▶ Knowingly or Intentionally Concealing
- ▶ Knowingly or Intentionally Destroying
- ▶ Knowingly or Intentionally Altering
- ▶ Knowingly or Intentionally Causing to Conceal
- ▶ Knowingly or Intentionally Causing to Destroy
- ▶ Knowingly or Intentionally Causing to Alter



SEC 66 - IT ACT

- ▶ Computer related offences. -If any person, dishonestly or fraudulently, does any act referred to in section 43,
- ▶ he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five (5) lakh rupees or with both. Explanation. -For the purposes of this section,-
- ▶ (a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);
- ▶ (b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

SEC 66 (B)- IT AMENDED ACT

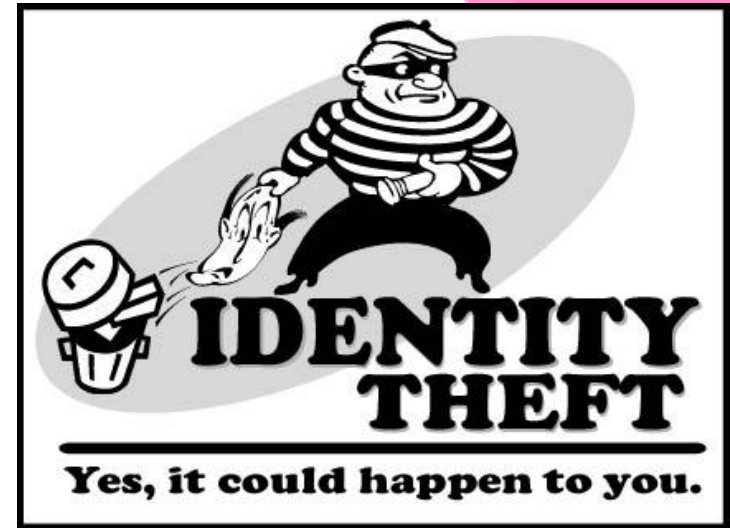


- ▶ Dishonestly receiving stolen *computer resource* or communication device
- ▶ Covers use of stolen Computers, mobile phones, SIM Cards, etc.
- ▶ Also covers “data theft”
- ▶ Punishment - imprisonment up to 3 years and fine



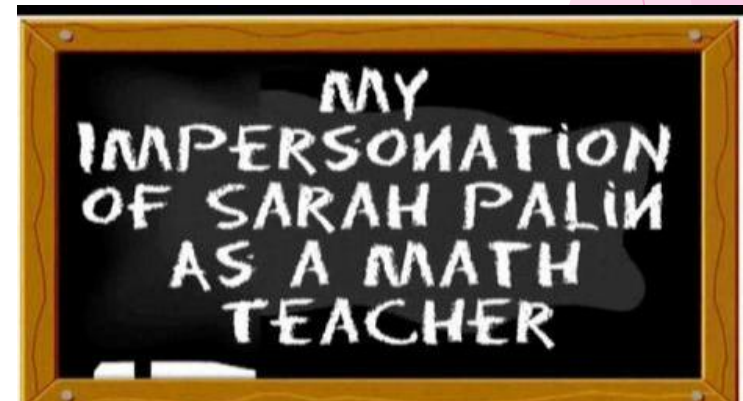
Identity theft

- ▶ Sec. 66 (C)
- ▶ Fraudulently or dishonestly using someone else's electronic signature, password or any other unique identification feature
- ▶ Punishment - imprisonment up to 3 years and fine



Sec 66d

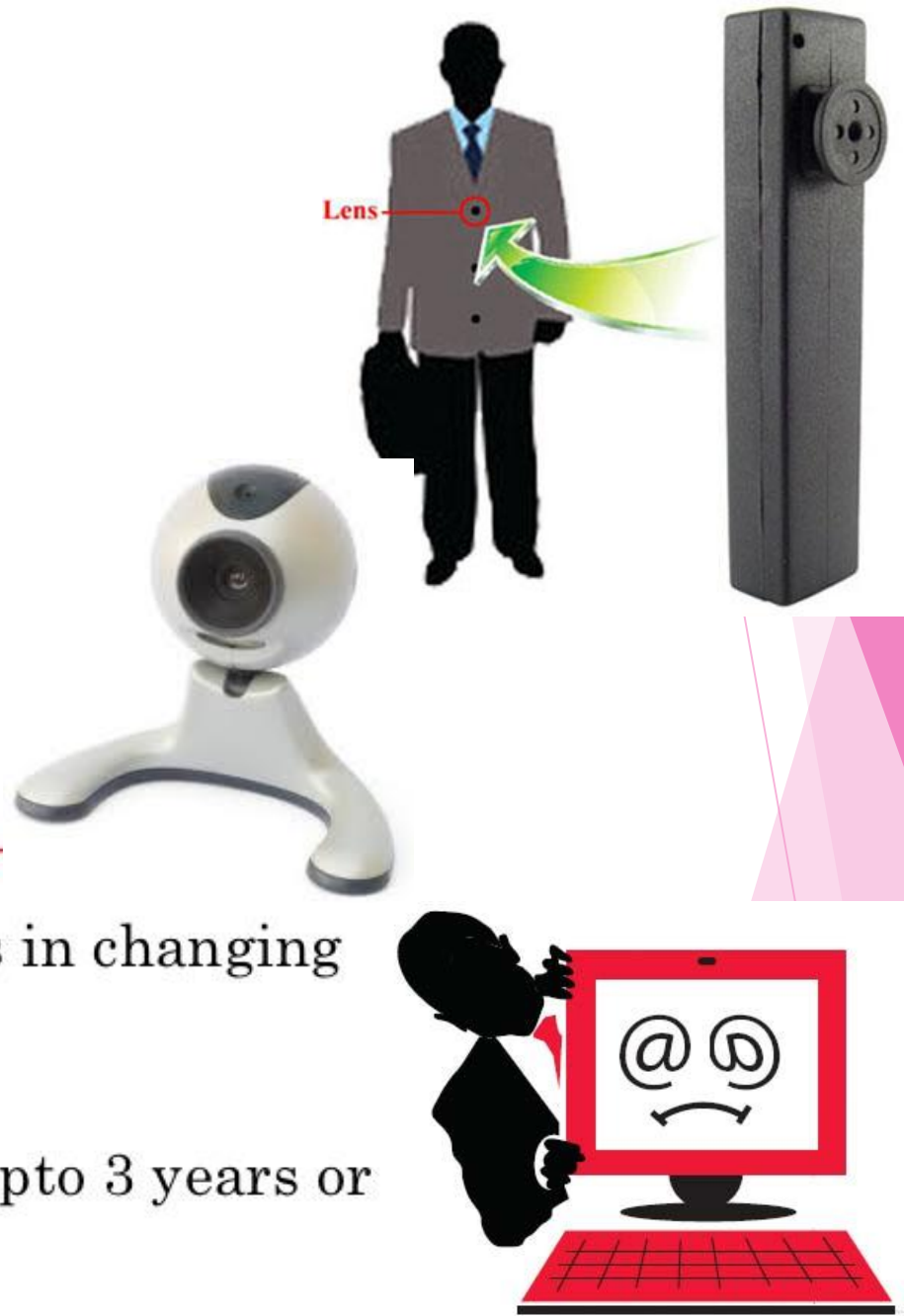
- ▶ Sec. 66 (D)
- ▶ Cheating by pretending to be some other person by using computer resource
- ▶ Sec. 415 and 416 IPC relevant to prove “Cheating” and “Cheating by Personation”
- ▶ Punishment - imprisonment up to 3 years and fine



PERSONAL PRIVACY

Sec. 66 E

- Violation of Personal Privacy
- Popularly known as Voyeurism
- Covers acts like hiding cameras in changing rooms, hotel rooms, etc.
- **Punishment** –imprisonment upto 3 years or fine upto Rs. 2 lakh or both



Sec 70- IT Act- Protected System

businessstoday.in/latest/economy/story/govt-declares-icici-hdfc-npci

Business Today India Today IndiaTodayNE Dailyo Aajtak Campus Aaj Tak GNTTV Ichowk Lallantop

BusinessToday.In

News / LATEST / Economy / Govt declares ICICI, HDFC, NPCI's IT resources as critical information infra [Feedback](#)

Govt declares ICICI, HDFC, NPCI's IT resources as critical information infra

Any person who secures access or attempts to secure access to a protected system in contravention of the provisions shall be punished with imprisonment of a term which may extend to 10 years and shall also be liable for a fine, the Act says.

Performance + Built-in AI [Learn More](#)



Representative image

[Listen to this article now](#) -02:45 1.0x

PTI
Jun 19, 2022, Updated Jun 19, 2022, 10:09 AM IST

The government has declared the IT resources of ICICI Bank, HDFC Bank and UPI managing entity NPCI as 'critical information infrastructure', implying any harm to them can have an impact on national security and any unauthorised person accessing these resources may be jailed for up to 10 years, according to an official notification.

Powered By **VDO.AI**

SEC 72

- ▶ **Section 72 - Breach of confidentiality and privacy**
- ▶ Any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material
- ▶ without the consent of the person concerned
- ▶ discloses such electronic record, book, register, correspondence, information, document or other material
- ▶ to any other person shall be punished
- ▶ with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

SEC 84 (b)- IT Act

- ▶ **84B. Punishment for abetment of offences.**--Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.
- ▶ *Explanation.*--An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

Sec 84 (c)- IT Act

► **84C. Punishment for attempt to commit offences.--**

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence,

► shall,

► where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both

SOCIAL MEDIA POSTS AS EVIDENCE



THINGS TO SECURE A SYSTEM

► WHAT I AM



► WHAT I HAVE



► WHAT I KNOW



► A system is as strong as its weakest link.

CYBER RESILIENCE

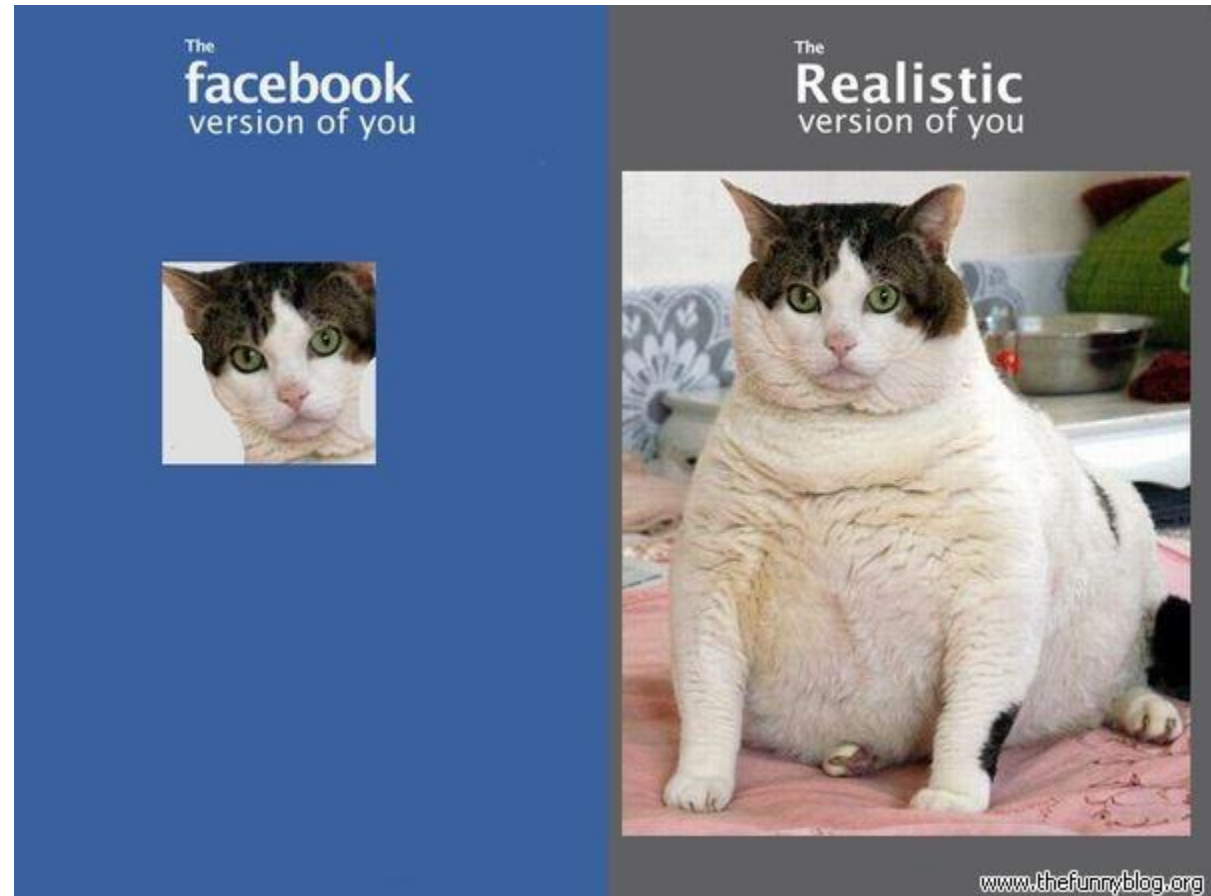


AGENCIES - CYBER SECURITY

- ▶ NATIONAL CYBER SECURITY CO-ORDINATOR - NCSC
- ▶ CYBER AND INFORMATION SECURITY DIVISION, MHA
- ▶ NCIIPC- CRITICAL INFORMATION INFRASTRUCTURE
- ▶ INDIAN CYBER CRIME CO-ORDINATION CENTRE (I4C)
- ▶ DEFENCE CYBER AGENCY



IT IS NOT WHAT IT SEEMS LIKE



CHAT ROOMS



Hi. You sound real cute!!
How old are you and what
do you like doing after school?



I am 14 and a bit of a fitness
fanatic, I often go power lifting
after school.

AN INTERESTING PASSWORD CHANGE



ACTIVE AND PASSIVE LEARNING



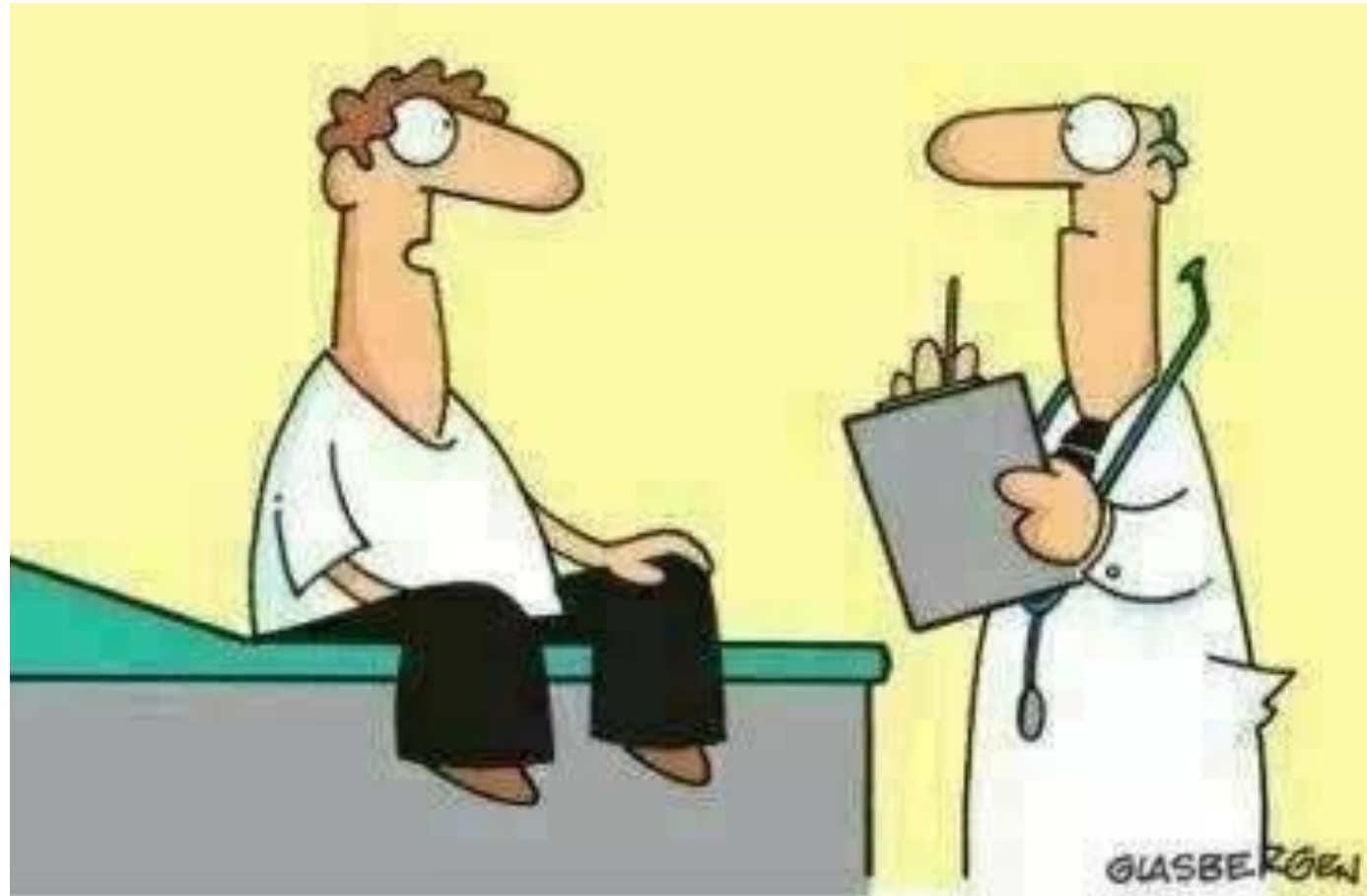
SIZE DOES NOT MATTER



A QUOTE BY FACEBOOK ADDICT

My Parents
should be Proud
of me because
I'm Addicted to
facebook
not to
Drugs !

INTERNET MEDICINE



**"I already diagnosed myself on the Internet.
I'm only here for a second opinion."**



GOD ON FB.....

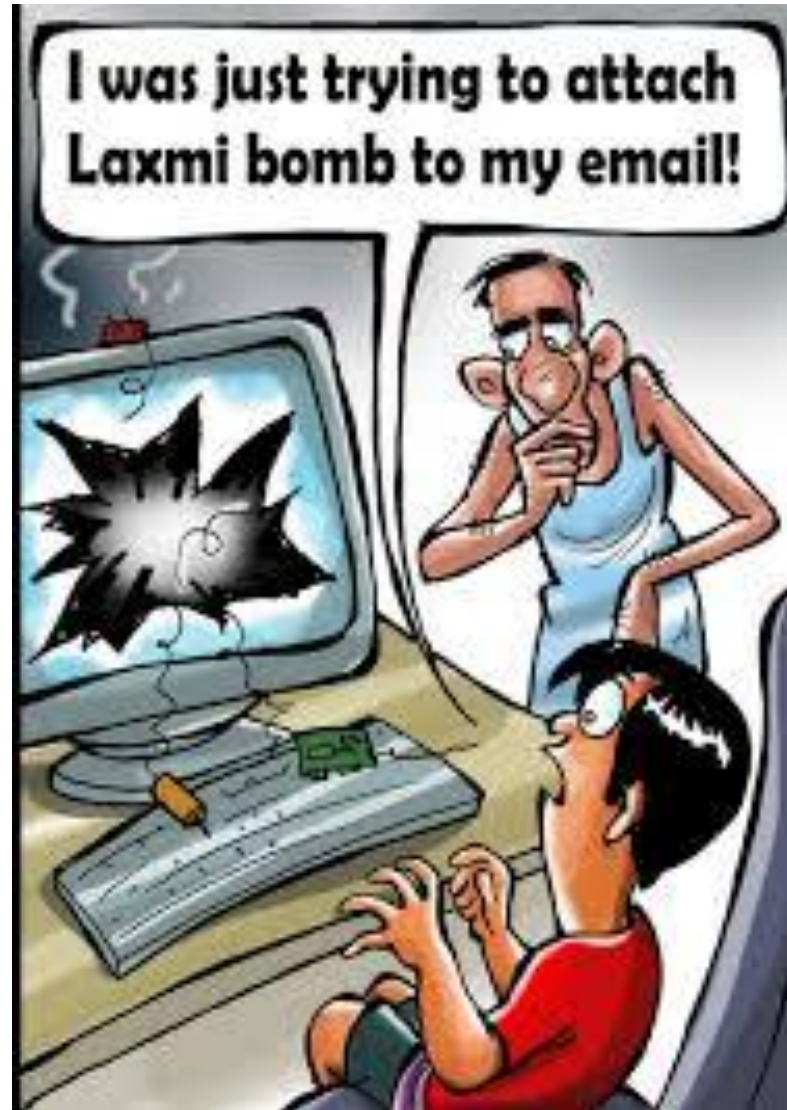


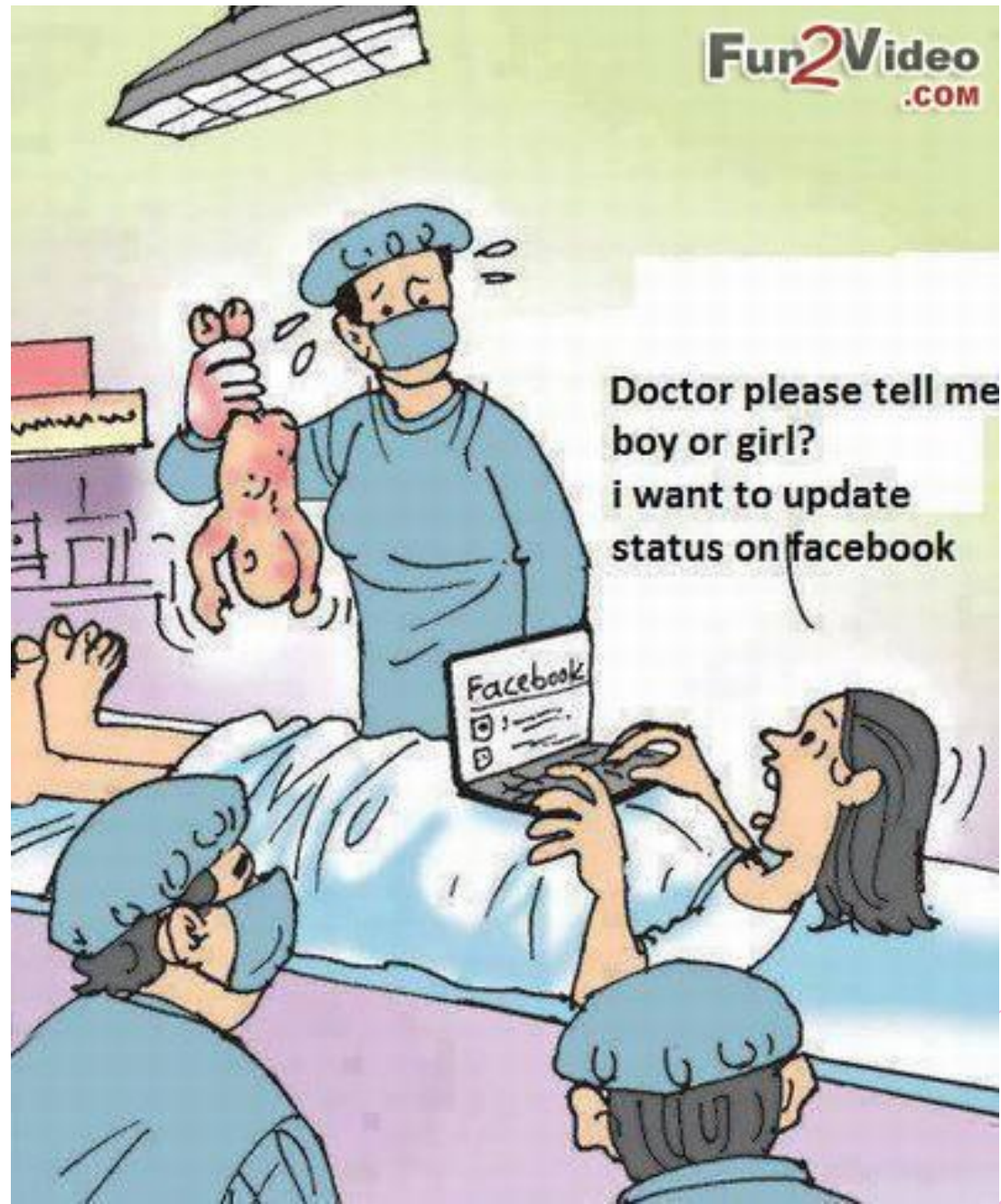
FB STATUS UPDATE...

I forgot to post on Facebook I was going to the gym.
Now this whole work-out was a waste of time...



EMAIL BOMBING...





A password is like a toothbrush



Choose a
good one

Don't share it
with anyone

Change it
occasionally

CYBER WARFARE

- ❖ CAN CRIPPLE CRITICAL INFRA-STRUCTURE
- ❖ MORE DANGEROUS THAN NUCLEAR WAR

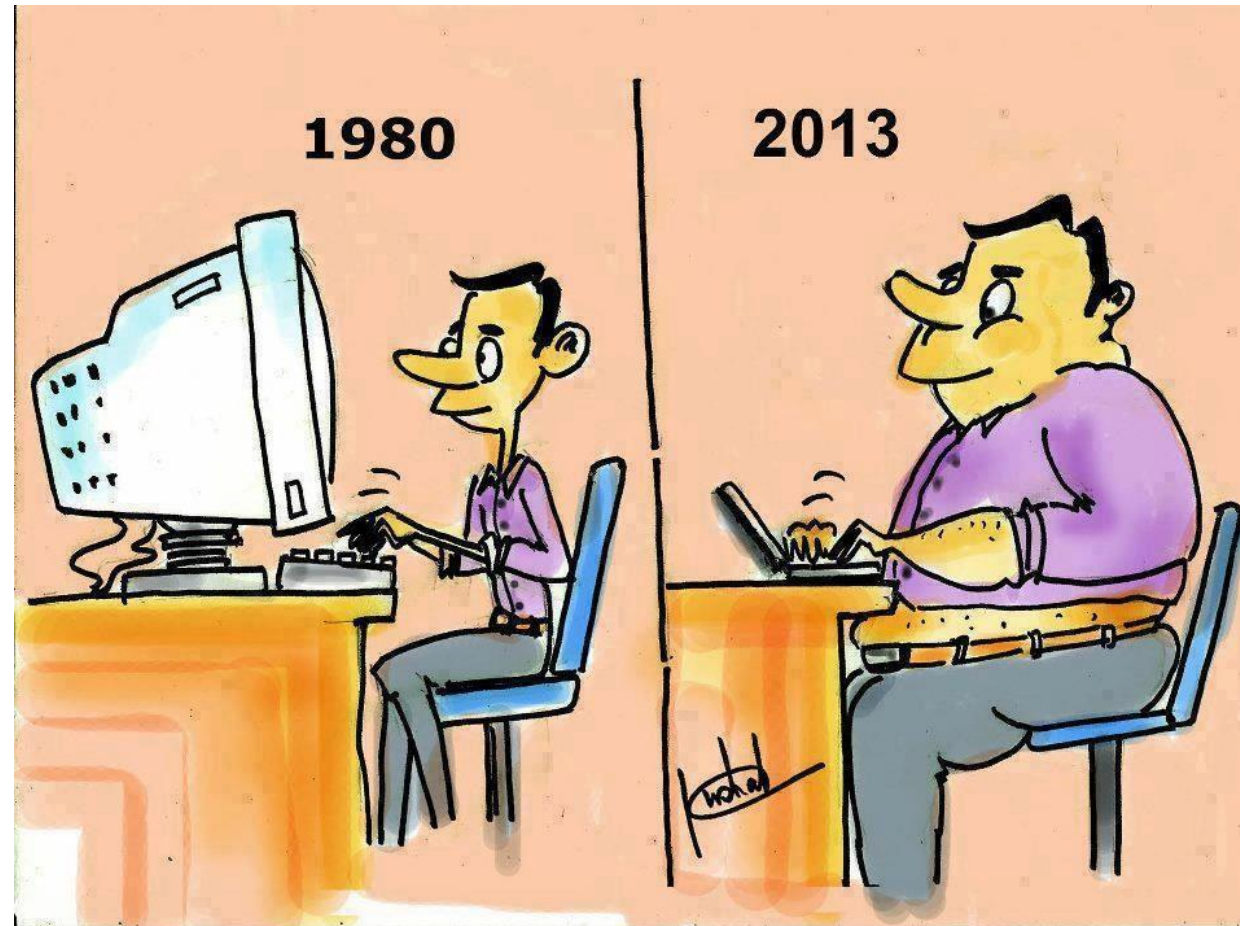


PARADOX OF LAW

- Usually Law EVOLVES, MODULATES, ADAPTS
- Here, We'll have to EVOLVE, MODULATE, ADOPT.
- It is like cutting the leg to the size of the shoe



HOW COMPUTER CHANGED THE LIFE



BE WATCHFUL



NEVER
GIVE UP!









Create Happiness If You Cannot Find It.,



WHAT IS NECESSARY IS ONLY WHAT IS
REQUIRED



