

# THE AWARE CONSUMER

(SUBSCRIBER COPY NOT FOR RESALE)

[www.theawareconsumer.in](http://www.theawareconsumer.in)

Dedicated to  
**NATIONAL  
CONSUMER DAY**  
2021  
on 24th December

## Rising **CYBERCRIME**

– Cybersecurity cannot be  
an afterthought anymore!



### INTERVIEW

Prof. Triveni Singh (IPS)  
SP, Cyber Crime, U.P. Police

### RESEARCH FEATURE

The Shape of Cyber Security  
Laws Around the World

### OUT OF THE BOX

A Pervasive Misinformation Narrative is  
Clouding the Consumers' Minds

**PLUS**

**ROUND UP • MY MARKET • THE PRESCRIPTION**



# NATIONAL ACCREDITATION BOARD FOR TESTING AND CALIBRATION LABORATORIES

**NABL grants accreditation to software and IT system testing laboratories in accordance with ISO/IEC 17025**

**Laboratories testing the following can apply for NABL accreditation in accordance with ISO/IEC 17025**

**Software testing and IT system testing by Accredited labs ensures the safety and security requirements are met**



- Telecom Software / Protocol
- Embedded Systems
- Mobile Devices and Mobile Applications
- e-Governance Application and Solution Evaluation
- Gaming Software, Electronic Gaming Machine, Interactive/ Internet Gaming products and systems (i-Game), etc.
- IOT Block Chain, AI or Drone software / system / application
- Data Analytics Software
- Lottery Software
- E-Procurement System Software
- Process and Control Software
- Web Application and Website
- Linguistics Software
- Sector Specific Software & IT system e.g. Defense/ Railways / Banks / Public Sector etc.
- Testing & Evaluation for regulatory compliance
- Others

NABL 137 document provides additional information



**NABL complies to ISO/IEC 17011 and is a full member and signatory to ILAC and APAC MRA**

**NATIONAL ACCREDITATION BOARD FOR TESTING AND CALIBRATION LABORATORIES (NABL)**  
**NABL HOUSE**  
**PLOT NO. 45, SECTOR 44**  
**GURUGRAM, HARYANA - 122003**  
**EMAIL: [INFO@NABL.QCIN.ORG](mailto:INFO@NABL.QCIN.ORG) | PH: 0124 4679700**







## MESSAGE FROM PUBLISHER & EDITOR

# Consumers Falling Prey to Growing Proliferation of **ONLINE CRIMES**



**WE ARE LIVING** in a digital age. Everything from our communication, shopping and entertainment to even our jobs and education have moved online. We have become dependent on the internet which spells infinite ease of access to almost anything or anywhere in the world at the click of a button. The online ecosphere is not limited to our computers. The increasing use of smartphones and other mobile devices has brought the virtual world right into our pockets.

Just like internet usage is marking its presence in every sphere of our lives, cybercrime is also infiltrating every which realm possible. These are unlawful activities that occur in cyberspace or through the use of cyberspace. A computer is used as a tool to perpetrate the crime or is a target or both.

Think about it – we are seeing the advent of a gamut of new-age crimes by the day. While online banking frauds, data theft and transmitting of viruses first springs to mind, it includes cyber stalking, bullying, pornography, defamation, squatting, ransomware, terrorism and more. In fact, even as we try to protect our online-selves with antivirus software, firewalls and email filters, cybercriminals are finding new and more sophisticated methods to evade our security, invade our activity and violate our privacy.

It is in fact so very easy to commit such cybercrimes. All it takes is some advanced computer expertise, internet access and loads of time on hand. And it is not just vulnerable children or unsuspecting senior citizens who get duped. Cyber fraudsters can net the best of us when we let down our guard even a wee bit, say unthinkingly clicking on a link while the mind is preoccupied with some other work. The faceless perpetrator could be anyone – a stranger gloating on his computer across the world to a colleague sitting in the cubicle right next to you. And it is not just money that we stand to lose, it could be our identity, reputation or even dignity!

On this National Consumer Day, we exhort the government to tighten the law and take other stringent steps to protect us from the growing misery of cybercrimes!



**Prof. Bejon Kumar Misra**

Publisher & Editor  
bejonmisra@theawareconsumer.in



# CONSUMER ONLINE FOUNDATION

THE FIRST

AND ONLY  
ORGANISATION  
**CERTIFIED**  
AS PER  
INTERNATIONAL  
STANDARD  
**ISO 9001:2015**  
FOR

CONSUMER  
COMPLAINTS  
REDRESSAL SERVICES



*A proud moment for us  
to share with our  
well wishers and supporters*



PROF BEJON KUMAR MISRA  
Founder – Consumer Online Foundation

PRAFULL D. SHETH

Editorial Board Member

# WHY ARE PROPOSED E-COMMERCE RULES LYING IN COLD STORAGE?

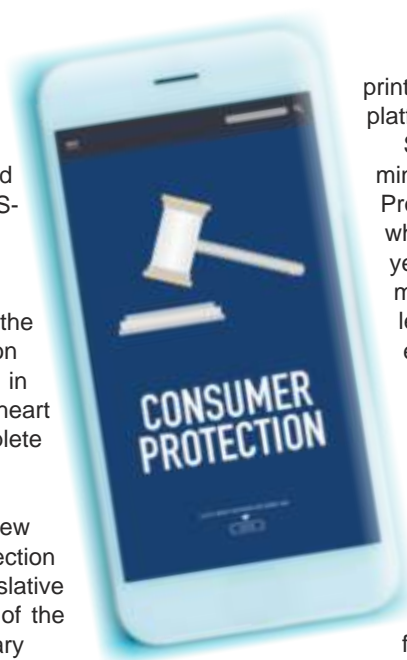


## WITH NATIONAL CONSUMER

Day 2021 just round the corner, I cannot help but hark back to this same time last year. While the world was grappling with the deadly SARS-CoV-2 virus just like it is now, the National Consumer Day 2020 celebrations were marked by an unrestrainable cheer on account of the recently passed Consumer Protection Act, 2019. The gaiety was subdued in view of the circumstances, but the heart could not stop rejoicing in the complete overhaul of the old and outdated legislation.

The new CPA truly heralded a new era in the history of consumer protection in India with a ground-breaking legislative and regulatory framework in favour of the consumers. It introduced revolutionary concepts like product liability, instituted strict penalties for misleading advertisements and even embraced e-filing of consumer complaints.

The true turning point was the broadening of the definition of the consumer to finally bring e-commerce transactions under legal purview. This brought the hope that the gullible customers will no longer be trapped by levies, penalties and other charges that surface after the online transaction is complete, not to mention getting duped by the fine



print of online retailers and e-commerce platforms.

Subsequently, the consumer affairs ministry released the draft Consumer Protection (E-Commerce) Rules 2020 which was followed by another one this year to amend the rules with some much-needed additions to tighten the legal norms on the e-commerce entities. However, it seems to be overcompensating the delay by marginalising e-commerce platforms which will only skew the competition. Isn't the outlawing of flash sales characterised by deep discount offers a needless killjoy that deprives consumers of both choice and price value?

Even after suggestions flowed in from various stakeholders, the authorities seem to be adopting delaying tactics by extending the deadline for comments. The rules are further embroiled in internal dissent from other ministries which also purport that the proposals are going beyond the aim of protecting consumer interests!

With no clear timeline for implementing the new rules in view, it is high time the government starts giving top-most priority to consumer welfare once again! ■

## 16

### RESEARCH FEATURE

#### THE SHAPE OF CYBER SECURITY LAWS AROUND THE WORLD



Cybercrime is a growing concern for all countries at all levels of development. It is actually a global menace as illegal cyber activities are not limited by geographical borders.



## 25

### HORIZON

#### CONSUMERS SHOULD TAKE OWNERSHIP OF THEIR ONLINE LIVES



Our growing reliance on digital tools signals an imperative need to equip ourselves with the knowledge and skills of not only how to use technology, but also how to behave responsibly while staying safe in the online realm.



## 31

### INTERVIEW

**Prof. Triveni Singh (IPS), SP, Cyber Crime, Uttar Pradesh Police**

## 38

### MY MARKET

#### E-COMMERCE: ARE CONSUMERS ACTUALLY GETTING WHAT THEY PAID FOR?



Online sellers often make false or misleading statements regarding a product's characteristics or capabilities.



## 41

### OUT OF THE BOX

#### A PERVERSIVE MISINFORMATION NARRATIVE IS CLOUDING THE CONSUMERS' MINDS



News spreads quickly in the age of digital technology and social media; fake news spreads even more rapidly!



## 46

### IN FOCUS

#### HOW CAN CONSUMERS TAKE BACK CONTROL OF THEIR PERSONAL INFORMATION?



A robust data protection and privacy regulation is critical to ensure security in the storage and transfer of data!

Owner, Printer, Publisher & Editor:  
Prof. Bejon Kumar Misra

#### EDITORIAL CONSULTANTS

Prafull D. Sheth  
Bina Jain  
Suman Misra  
Dr. Manisha Kukreja Batla  
Dr. Alka Mukne  
Pyush Misra  
Payal Agarwal  
Shashank D. Sudhi  
Dr. A. Raj

DESIGNER: Galaxy; Yellow Palette

DESIGN CONSULTANT: Maanav Khaitan

#### WEB DESIGNER:

Manish Mohan  
Ebrahim Bhanpurawala

#### MANAGER CIRCULATION

S. K. Venkatraman

#### Published at:

B - 306, 1st Floor,  
C.R. Park, New Delhi-110019

#### Printed at:

M/s. Swastika Creation  
19, D.S.I.D.C. Shed, Scheme 3,  
Okhla Phase II, New Delhi - 110020

For any queries, please contact us at  
contact@theawareconsumer.in  
Phone: 9311044424

Total number of pages - 64, Including Covers

Material in this publication may not be reproduced in any form without the written permission of the Editor & Publisher.

DISCLAIMER: The views expressed in this magazine are solely those of the author in his/her private capacity and do not in any way represent the views of the Editor & Publisher.





DR LEE HADLINGTON  
SENIOR LECTURER AT DE MONTFORT UNIVERSITY

We think of cybercriminals as kids in their bedrooms just trying it out, but these people are doing this as a business, so it's no surprise that they research what works and what doesn't.

# ROUNDUP



**OCTOBER**  
**NATIONAL CYBER SECURITY AWARENESS MONTH**  
**#STAYCYBERSAFE**

## MeitY Observes National Cyber Security Awareness Month

All through October every year, the government focuses on increasing cyber security awareness as part of the National Cyber Security Awareness Month (NCSAM). This is a concerted attempt to bring attention to the importance of cyber security and how to stay safe and secure online.

### DATA BRIEFING

Indian Government data recorded  
**1.16**  
million cyber security cases in 2020, a 3x spike from the previous year.



OCTOBER 2020  
NATIONAL CYBER SECURITY AWARENESS MONTH  
#STAYCYBERSAFE

# BE A CYBER CHAMPION

May the Cyber Force be with You!

Share your thoughts using  
#StayCyberSafe



**THE MONTH OF** October is globally marked as Cyber Security Awareness Month every year with a view to educate both the public and private sector to increase cyber resilience. There is a different theme every year focusing on specific challenges in the cyber world and identifying opportunities for behavioural change.

The theme for 2021 is 'Do Your Part, #BeCyberSmart' with the overarching aim to empower both individuals and organisations to own their role in protecting their part of the cyberspace. After all, it is only when everyone does their part that our interconnected world can become safer and more resilient for everyone. This includes raising community awareness, educating vulnerable audiences, training employees and implementing stronger security practices.

In India, under the recommendations of the National Security Council Secretariat (NSCS), Government of India, the Information Security Education and Awareness

(ISEA) wing of the Ministry of Electronics and Information Technology (MeitY) (in association with CERT-IN, NIC and C-DAC) organises many mass awareness activities, webinars and workshops through various modes as part of the National Cyber Security Awareness Month. Some of them include cyber security tips on best security measures, awareness videos on cyber security topics and alerts on cyber threats along with quizzes, crosswords, newsletters and more. Few of the topics covered include different types of malware attacks, how to identify fake messages on social media platforms and other trending cyber security concepts.

India jumped from 47 to 10 in the new rankings of the Global Cyber-security Index released in June 2021.

There are varied programs for both the general public and the technical cyber community. Some activities are targeted at educating and motivating the netizens to be cyber aware and

secure. For instance, online short sessions were hosted all through the month on the MyGov platform on how to secure mobile devices, personal data, digital payments and password and wi-fi security to help the end-users. Then there were sensitisation and awareness campaigns in multiple Indian languages on cyber security and privacy. The participants won prizes and e-certificates.

Workshops were organised to train/upgrade the technical knowhow of various stakeholders working in banking, insurance, capital markets, power sector, cyber security and data science researchers along with professors and lecturers. In fact, any interested persons can enrol for the programs to gain the required information and knowledge to successfully shield themselves against various cyber threats and dangers lurking in the cyber space.

India is in the final stages of clearing a National Cybersecurity Strategy! 🇮🇳



# IRDAI Champions Cyber Insurance Cover for Individuals

Just like there are different types of insurance options to protect us against the risks of theft, damage or illness to our health, home, vehicles, etc. the new-age consumer also needs cyber insurance to compensate for financial losses arising out of digital frauds, identity theft and other unforeseen events in the cyber world.



Retail cyber insurance products to be in the offing soon

**ONE OF THE** main pitfalls of the growing digitalisation is cybercrime. Indeed, all of us are exposed to severe risks and threats every time we are online. While phishing attacks, fraudulent transactions and other security breaches are booming due to the pandemic-fuelled heightened digital traffic, cyber insurance covers are mostly limited to banks and other corporate entities. Only a few big players like Bajaj Allianz, HDFC ERGO and ICICI Lombard extend insurance against internet frauds to individuals.

The Insurance Regulatory and Development Authority of India (IRDAI) recently constituted a working group which reported that cyber risks have risen by 500% since March 2020. Recognising that individuals too need cyber risk protection just like

corporates, the IRDAI released model cyber insurance policy guidelines in September this year. The document titled 'Guidance Document on Product Structure for Cyber Insurance' provides the salient features, coverage and suggestions on product structure for cyber insurance. It also proposes simplifying existing products while expanding their scope of coverage.

India is one of the most cyber attacked nations in the world with about 4 million malware detected every day. National cyber security coordinator, Lt. Gen. (retd) Rajesh Pant said, "One of the reasons for this is that we have a large attack surface with 1.15 billion phones and more than 700 million internet users".

The apex insurance regulatory body expects general insurers to adopt these guidelines while providing insurance coverage against cybercrimes like:

- Theft of funds from bank accounts, credit/debit cards, mobile wallets
- Identity theft
- Unauthorised online transactions
- Email spoofing
- Hacking of social media accounts
- Malware attack
- Phishing
- Cyber stalking/bullying
- Ransomware
- Data breach

The policy will not only provide financial compensation for first-party losses from the cyber fraud, but also

cover legal expenses involved in prosecuting the scamsters and defending oneself against claims made by third parties who have been adversely affected by the impersonation. The policy will chip in to reimburse the costs for data restoration and even for reputational damage from identity theft.

The premiums are kept affordable and multiple devices can be covered under a single cover. The coverage can be extended to family members too, but the premium will obviously increase.

As per the IRDAI norms, consumers insured against cybercrimes will face zero liability for:

a) Contributory fraud/negligence/deficiency on the part of the bank even if it is not reported by the customer.

b) Third party breach even if the deficiency lies not with the bank but elsewhere in the system provided the customer notifies the bank within 3 working days of receiving the communication from the bank regarding the unauthorised transaction.

The customer will bear limited liability for:

a) Losses due to customer negligence (like sharing payment credentials) till the time the unauthorised transaction is reported to the bank.

b) Losses due to unauthorised transactions where the responsibility lies not with the bank but elsewhere in the system and the customer delays in notifying the bank – i.e., 4 to 7 days after receiving the communication from the bank regarding the unauthorised transaction.

In addition to this, the consumers should pay attention to the fine print to understand the conditions and sub-limits of the policy. For instance, phishing and email spoofing coverage is often restricted to only 15% to 25% of the sum insured. Other reimbursements may be limited to 25% to 50% of the overall policy limit. It is better to look for 100% coverage, especially for theft of funds and identity. ▶

# WhatsApp Stays on the Beat for Consumer Grievances

WhatsApp is the messaging platform of choice with more than 400 million users in India. This makes it ripe for both abuse and misuse.



**THE MINISTRY OF** Electronics and Information Technology (MeitY) issued the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 that came into effect from 26th May this year. The guidelines require all social media platforms to have a grievance redressal mechanism and name a grievance officer who will register a grievance within 24 hours and redress it in 15 days.

However, WhatsApp had appointed a grievance officer in India way back in 2018 itself. Users can reach out to the WhatsApp grievance officer and register a complaint through the Contact Us link under the Help section in the Settings menu. Complaints can also be registered via email at [grievance\\_officer\\_wa@support.whatsapp.com](mailto:grievance_officer_wa@support.whatsapp.com). Or they can be sent by post to Mr. Ashish Chandra at Post Box No. 56, Road No. 1, Banjara Hills, Hyderabad - 500034, Telangana.

In addition to this, WhatsApp is also taking active steps to curb the fake news being propagated on the app. Being an end-to-end encrypted platform to allow users to exchange messages privately, the company cannot directly moderate the content in circulation. Instead, it has introduced measures like 'frequently forwarded messages' (messages which have been forwarded more than five times) can be forwarded only to one person/group at a time.

Even the MyGov Corona Helpdesk can be reached via WhatsApp for emergency contacts, symptoms, advice on how to be safe, official alerts from the authorities, etc.

Following the rollout of the rules, Facebook and Twitter have also appointed their grievance officers in India for filing and redressing complaints from consumers on violations and other issues. ▶

# Bridging the Skill Gap in **CYBER SECURITY**

It is not just death and taxes, even cybercrime has become a doomed certainty of the modern world. And cybersecurity professionals are crucial for helping avert the varied risks of cyber attacks.

**There is a crunch of cybersecurity talent for protecting systems, infrastructure and people**

**A PHISHING SCAM** can rob someone of their entire life savings. A ransomware attack can bring a business to its knees and leave hundreds of people unemployed. To add to this, cyber attacks are ever-evolving with web application breaches, reconnaissance, cyber espionage, DDoS and more.

Laws and policies alone cannot avert these disastrous cybercrimes. Even security solutions can be effective only when they are manned by the right hands. Therefore, what we need is cybersecurity professionals to protect the digital world and prevent such things from happening.

With cybersecurity featuring high on the agenda of big and small organisations alike to defend themselves against the ever-looming threats, the industry is in dire need of skilled professionals.

In fact, the whole world is facing a huge cybersecurity skills shortage. According to the 2020 ISC2 Cybersecurity Workforce Study, the global shortage of cybersecurity professionals already exceeds 3.12 million. According to another estimate, the shortage of cybersecurity workforce in India is 9% higher than the global average.

The State Of Cybersecurity in India 2020 report values the Indian cybersecurity industry at \$6.7 billion. Around 96,000 cybersecurity personnel are currently working across enterprises in India and close to 11,000 positions

related to cybersecurity are still available to be filled. Other reports reckon that there will be about 1.5 million job vacancies in cybersecurity by 2025 in India alone.

The government is taking several initiatives to build a robust cybersecurity infrastructure, like launching a specialised cyber forensics university, developing the National Mission on Quantum Technologies and Applications and setting up more institutes for higher education. MeitY is focusing on skilling security leaders in government entities across the nation in cybersecurity. The Data Security Council of India (DSCI) has launched the 'CyberShikshaa' programme to create a pool of skilled women security professionals in the country. These programmes are in association with Microsoft. Even companies themselves are looking to tackle the skills gap by training their own security personnel to be alert for ongoing threats and detect impending attacks.

However, we need more educational institutions and training programmes to train professionals on emerging technologies in cybersecurity. Corporate businesses also need to make much more investments in cybersecurity training.

Individuals looking to build a successful career, change careers or to advance their skills can opt for cyber training and be a part of the cybersecurity success story! ▶

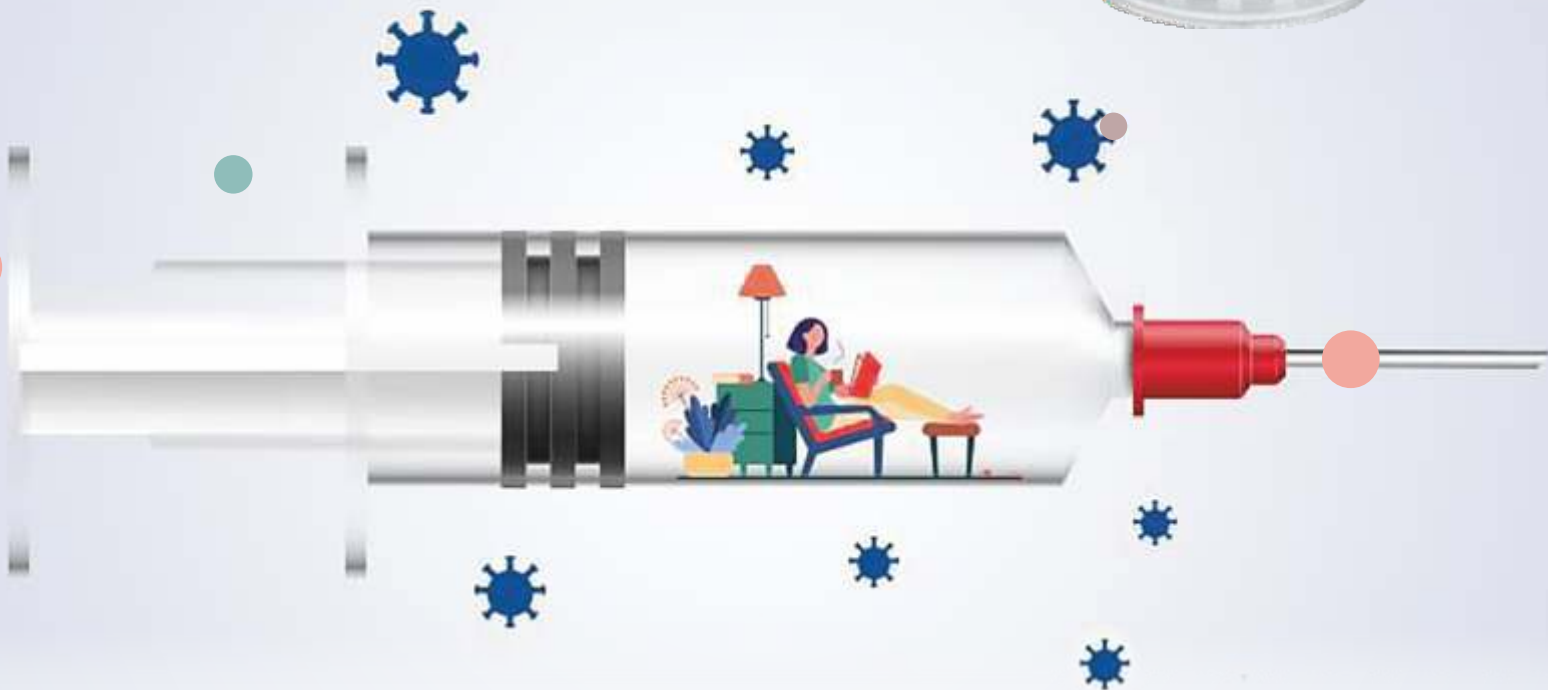




#LetsBeatCorona

# DISPO VAN

THE TRUSTED BRAND  
PROMOTING PATIENT SAFETY



## STAY IN, STAY SAFE!

[www.hmdhealthcare.com](http://www.hmdhealthcare.com) • [info@hmdhealthcare.com](mailto:info@hmdhealthcare.com)



**Rajiv Nath**

- Mg. Director@ HMD
- Forum Coordinator@ AIMED

*“Not every war is won  
on a battlefield.  
Some wars can also be won  
sitting at home.”*

#StayHomeStaySafe

**Consumers, Beware**

# Maintaining Digital Privacy and Safety is in our Hands

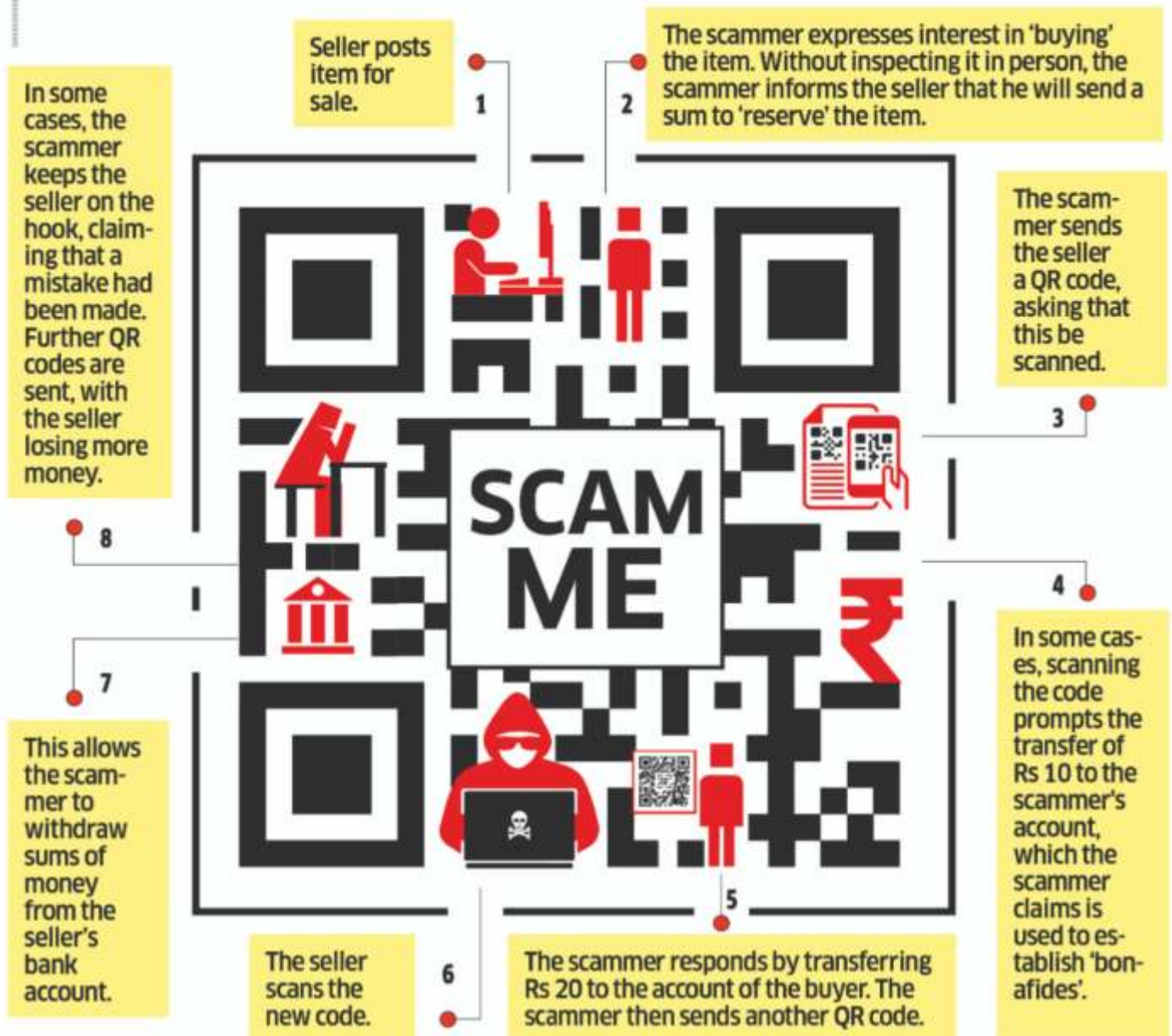
The digital world is making things more and more convenient. Passwords get autosaved; credit card information gets auto-filled; mobile numbers, addresses and other information are always handy; allowing for one-click checkouts. Given our growing reliance on the internet, most of us seem to be operating on 'autopilot' which is akin to playing into the hands of cybercriminals. A proactive approach is crucial for steering clear of potential privacy and security holes.



*The whole world is moving online and mobile with our data synced across devices – this 'connected' ease can translate into grave security risks too!*

## SCAN QR CODE, LOSE MONEY

The Unified Payments Interface (UPI) is a system that merges several banking features and merchant payments into a single unified payments system. The system's QR Codes were meant to ease the process of carrying out financial transactions. Instead, they have become manna for fraudsters who are exploiting the technology to con victims out of money. The problem is compounded by the fact that some payments platforms do not specify what the code has been generated to do - to pay another person or receive money from another individual.





**There are very many ways in which we can become a victim of illegal cyber activities.  
Adequate precautions are essential for safeguarding our personal information.**

**YOU GET AN** SMS/email from the bank that your account has been blocked and you should immediately update the KYC/PAN card/Aadhaar card details through a link to continue availing the services. Little do you suspect that the message has not actually come from the bank and is the work of scrupulous fraudsters. No sooner that you click on the link and provide the details, money gets siphoned from your account and you become another gullible victim of a phishing scam!

Microsoft's 2021 Global Tech Support Scam Research report in association with YouGuv covering tech support scams and their impact on consumers in 16 countries reveals that consumers in India experienced a scam encounter rate of 69% in the last 12 months and lost Rs.15,334 on average. What is particularly alarming is that almost half of the surveyed consumers (48%) were tricked into continuing with the scam (an 8 point increase from 201 and 3 times higher than the global average of 16%). One in three (31%) continued engaging and eventually lost money (an increase of 17 points compared from 2018). Surprisingly, the millennials aged 24 to 37 proved to be the most susceptible to these scams!

'The total volume of phishing emails and other security threats relating to the COVID-19 coronavirus now represents the largest coalescing of cyber attack types around a single theme that has been seen in a long time, and possibly ever' - Sherrod DeGripio, Senior Director of Threat Research and Detection at Proofpoint, a leading cybersecurity service provider.

There is no end to the types of tricks being perpetuated online. It's a veritable minefield of debit/credit card frauds, e-commerce frauds, investment frauds, email spoofing, website spoofing, hacking, identity theft and other illegal cyber activities designed to gain unauthorised access to your computer/mobile phone to steal money, pilfer data or spread malware.

You may reason that you are always on your guard and such things cannot happen to you. But think again - if a website shows that your password is wrong or has expired, wouldn't you click on the link that is conveniently provided to change or update the password? Would you bother to go directly to the website by entering the URL in the browser?

Following are some tips on how to be safe now rather than sorry later:

- Be careful when filling forms and passwords online. Create secure passwords with a mix of alphabets, numbers and symbols and change them periodically. Skip birthdays, nicknames and other easy combinations; they may be easy to remember, but will also prove to be as easy to crack. Change the default passwords on devices and do not use the same password across accounts. It is advisable to use a reliable password manager tool to create unique passwords.

- Do not disclose unnecessary personal information on websites. It is better to cancel the transaction or leave the site, especially if it is not clear why the solicited information – like your mobile number, address, pet's name or even favourite book - is required.
- Avoid oversharing on social media - refrain from posting regular updates about your whereabouts. Your casual comments or posts may end up providing the answers for the security questions in the password reset tools. Also update the privacy settings to limit who can see your personal information and activities.
- It is better to avoid syncing your social media accounts and also refrain from signing up for third-party websites with your social media credentials. A security breach into a social media account can compromise the safety across the other websites and apps.
- Stop blindly trusting unsolicited messages from banks, utility companies or other corporates with links or attachments, no matter how legitimate they appear. Be particularly wary of emails that transmit an 'urgency' to take a particular action. While at it, do not download pictures or videos from unknown sources. Make it a habit to check the sender's email address and ignore/delete the suspicious or unwarranted ones. Go directly to the domain to check the veracity, if required.
- Check the name of the websites and look out for misspellings and other tell-tale signs. Do not enter personal information if the URL does not begin with 'https' or does not have the lock symbol next to it.
- Free public wi-fi networks should be used with caution as they have very few security measures. Never shop online when on free wi-fi as others using the same network can easily access your activity.
- Close old email addresses, social media accounts and other online accounts you no longer use and delete the personal details if possible.
- Always wipe out all the data from old computers and mobile phones before disposing them.
- You can literally lock the door and place an alarm by installing a good antivirus software, spyware and firewall to keep virus and other malware at bay. Update the patches on a regular basis to ensure all round protection.

Frequent change of password for your online accounts acts like a vaccine for viruses! – State Bank of India

## Conclusion

On the eve of the National Consumer Day 2021, let us all pledge to stay on our guard when online. Prudent caution and constant vigilance will go a long way in keeping us safe and secure. In fact, it is better to be over-sceptical, you may miss out on something but your data will stay private at least! ▶

# The Shape of Cyber Security Laws Around the World

Cybercrime is a growing concern for all countries at all levels of development. It is actually a global menace as illegal cyber activities are not limited by geographical borders. While more and more countries are enacting cyber laws, the world still has a long way to go both in terms of conviction of attacks and protecting consumer rights in cyberspace.



**OUR LIVES HAVE** become increasingly dependent on technology on the one hand and many disturbing things are happening in cyberspace on the other. The rate of online crimes is increasing along with the growth in online activities. Latest reports predict that global cybercrime costs will grow by 15% per year over the next five years, reaching US \$10.5 trillion annually by 2025 (from US \$3 trillion in 2015).

The increasing incidence of cybercrimes opens a two-fold challenge for law enforcement agencies - managing both cybersecurity threats and the aftermath of cybersecurity incidents. Worldwide, governments have been instituting cybersecurity legislation, issuing guidelines and establishing bodies to regulate the cyber landscape.

The United Nations Conference on Trade and Development (UNCTAD) Global Cyberlaw Tracker is the first ever global mapping of cyberlaws. It tracks the state of e-commerce legislation in the field of e-transactions, consumer protection, data protection/privacy and cybercrime adoption in the 194 UNCTAD member states. The following maps (on pages 17 & 18) indicate which countries have or have not adopted legislation along with those that have a draft law pending adoption. When information about a country's legislation adoption was not readily available, 'no data' is indicated.

It is notable that since 2000 the UNCTAD eCommerce and Law Reform Programme is supporting developing countries in Africa, Asia and Latin America to develop legal regimes to tackle the issues of information and communication technology so as to generate trust in online transactions and offer legal protection for users.

Let us take a closer look at cyber laws in some countries:

#### United States of America - The

USA is the world leader in cybercrimes and also has the strongest cyber laws in place. The first effective law - *The Computer Fraud and Abuse Act (CFAA)* - was established in 1984 which was replaced by the *National Information Infrastructure Protection Act (NIIA)*. Strict definitions and punishments for cybercrimes are in place in the form of penalties and imprisonment.



**United Kingdom** – The primary cybercrime legislation in the UK is the *Computer Misuse Act 1990 (CMA)* to handle most of the malicious attacks or offences

happening in cyberspace. This is supplemented by the *Data Protection Act 1998* and now 2018 which ensures that all types of private, confidential or business information is handled in a safe, fair and lawful manner. It regulates how the information gets stored and also how it is used by organisations, businesses or the government. The National Cyber Security Centre (NCSC) was formulated to support businesses, governmental agencies and public departments with guidance on incident response and recovery.

**European Union** – As part of the Digital Single Market strategy, the EU Cybersecurity Act complements the NIS (Network and Information Systems) Directive and strengthens the European Union Agency for Cybersecurity (ENISA) apart from establishing a cybersecurity certification framework for products and services.



**Australia** – In Australia, cybercrime is codified by the *Criminal Code Act 1995* which was amended in 2001 by the *Cybercrime Act 2001*. Provisions of the Act are consistent with the terms of the Council of Europe Convention on Cybercrime 2000. The responsibility of investigation and response is with the Australian Federal Police (AFP). The Australian Cyber Security Centre (ACSC) was established in 2014.

#### Singapore - The starting point

for tackling cybercrimes in Singapore is the *Computer Misuse Act* which was initially adapted from United Kingdom and Australian legislation and was most recently amended in 2013. The main focus is on computer integrity crimes with provisions to deal with crimes that have been facilitated by computers including unauthorised access, use or modification of computer, computer materials and computer services. It is supplemented by the *Cybersecurity Act* and the *Personal Data Protection Act* which set out the obligations of organisations regarding cybersecurity arrangements. The Cyber Security Agency of Singapore (CSA) was set up in 2015 to provide centralised oversight of national cybersecurity functions and work with sector leads to protect the critical information infrastructure.



**China** - China started recognising and penalising cybercrimes way back in 1997 with the 'Computer Information Network and Internet Security, Protection and Management Regulations' with

imprisonment for hacking, sabotaging data and propagating viruses. Since 2010, the Chinese government maintains complete internet control in the country with many of the popular websites like Google, Facebook and YouTube banned within the borders. The latest *Cybersecurity Law* requires all foreign companies to store their essential data of use within the country itself while allowing the government to conduct checks on the company networks and data. This is heavily criticised for excessive coercion, control, and repression.



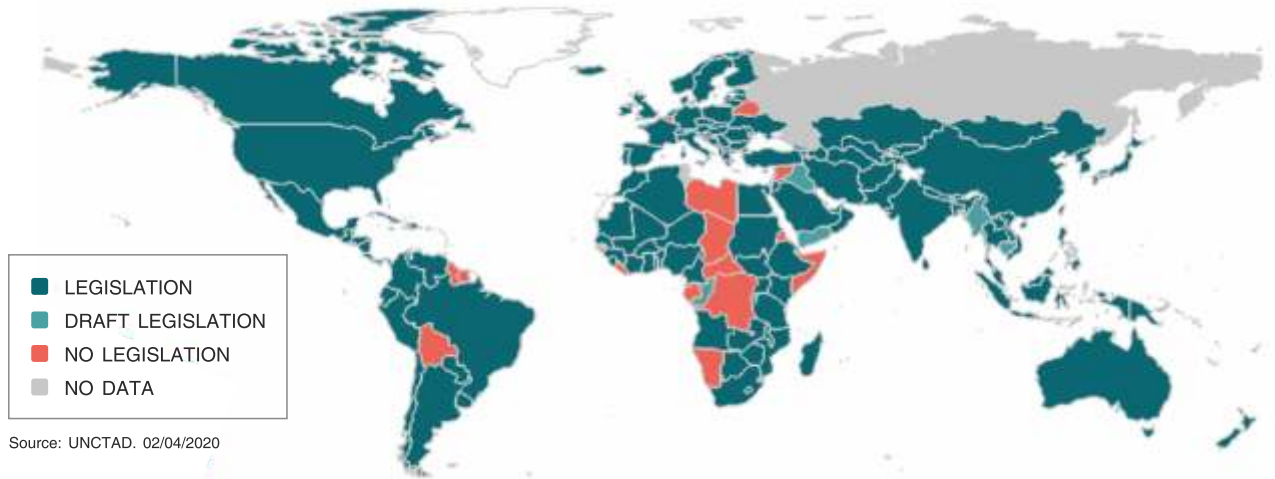
**80%**  
COUNTRIES WITH  
LEGISLATION

**5%**  
COUNTRIES WITH  
DRAFT LEGISLATION

**13%**  
COUNTRIES WITH  
NO LEGISLATION

**2%**  
COUNTRIES WITH  
NO DATA

## Cybercrime Legislation Worldwide



154 countries (80%) have enacted cybercrime legislation: Europe has the highest adoption rate at 93% while Asia and the Pacific are the lowest at 55%.

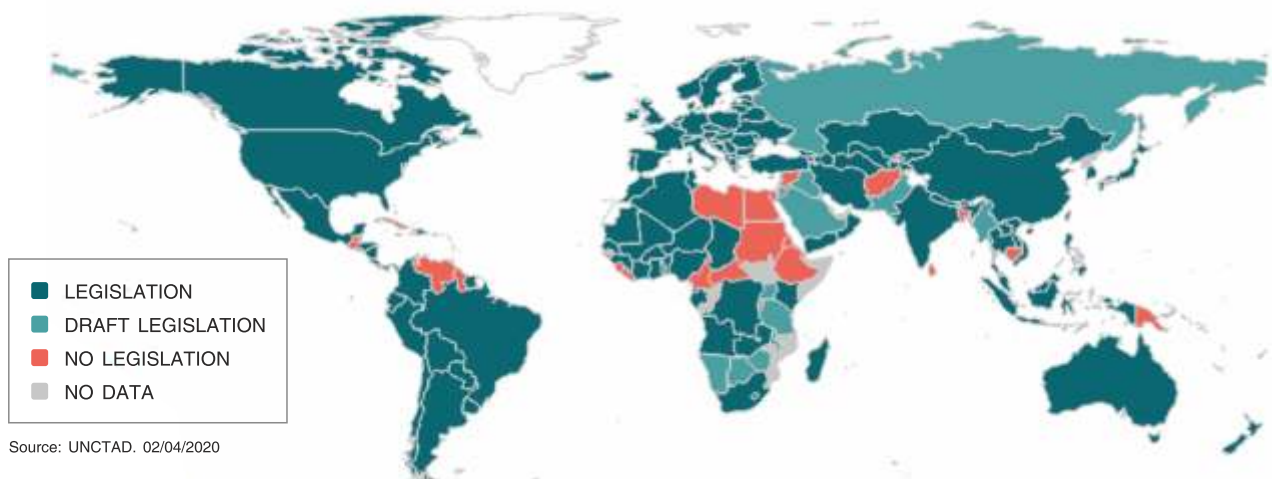
**66%**  
COUNTRIES WITH  
LEGISLATION

**10%**  
COUNTRIES WITH  
DRAFT LEGISLATION

**19%**  
COUNTRIES WITH  
NO LEGISLATION

**5%**  
COUNTRIES WITH  
NO DATA

## Data Protection and Privacy Legislation Worldwide



128 countries (66%) have legislation in place to ensure data security and privacy. Africa and Asia show a similar level of adoption with 55% of countries having adopted such legislations of which 23 are least developed countries.

**82%**  
COUNTRIES WITH  
LEGISLATION

**6%**  
COUNTRIES WITH  
DRAFT LEGISLATION

**4%**  
COUNTRIES WITH  
NO LEGISLATION

**8%**  
COUNTRIES WITH  
NO DATA

### E-transactions Legislation Worldwide



158 or 82% of the countries have instituted e-transaction laws that recognise the legal equivalence between paper-based and electronic forms of exchange. Of these 158 countries, 68 are developing or transition economies and 30 are least developing countries. It is notable that almost all European countries (44 out of 45) and 91% of the Americas have e-transaction laws. In Africa, the incidence of e-transaction legislation is only 61%.

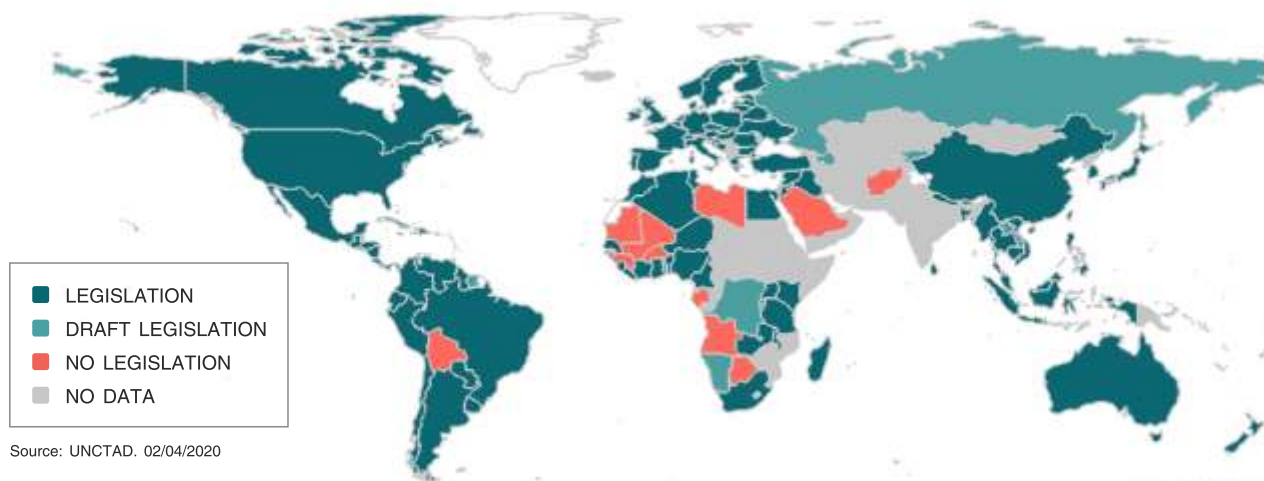
**56%**  
COUNTRIES WITH  
LEGISLATION

**6%**  
COUNTRIES WITH  
DRAFT LEGISLATION

**9%**  
COUNTRIES WITH  
NO LEGISLATION

**29%**  
COUNTRIES WITH  
NO DATA

### Online Consumer Protection Legislation Worldwide



The prevalence of laws to protect consumers online is the lowest with many developing and transition economies still lacking such legislations related to e-commerce. Data on online consumer protection regulation was available only for 134 countries of which 110 have adopted the requisite legislation: Europe 73%, Americas 72% and Africa 46%. Data could not be obtained for as many as 57 countries.

While most of the countries have or are on the path of instituting cybercrime laws, many of them are allegedly moving towards techno-authoritarianism. Indeed, laws that should protect people from online criminal activities are actually found to be undermining human rights and can prove to become detrimental to the normal life of consumers.

### International Cyber Crime Treaties

The ReVIL or Sodinokibi ransomware campaign - one of the most sophisticated ransomware attacks - took the world by storm for many months. The cyber criminal gang disabled the IT systems of many leading corporates, forcing them to shut down for several days. It even threatened to publish compromising information on then US president Donald Trump unless the ransom demand was paid.

Even the United Nations was subject to a grave cyber attack in April 2021 by another group which targeted users within the network through stolen user credentials purchased on the dark web for long-term intelligence gathering. The unbelievable WannaCry hacking attack way back in 2017 that shook the world by crippling computers across 150 countries is still fresh in our memories.

Closer home, the Israeli spyware, Pegasus is believed to have spied on at least 300 Indians, including two serving Ministers, three opposition leaders and one constitutional authority apart from several journalists and business persons. This sophisticated spyware actually infected the devices even without the victim clicking on any link or message. What followed was intense spying on messages, chats and pictures which were stealthily transferred along with other data to a master server.

These are just a few examples of the pervasive nature of this ubiquitous problem. Alas, government agencies, defence and high tech companies and multinational businesses around the world continue to be the prime targets of gigantic and extremely sophisticated cyber attacks.

The Budapest Convention is the first multilateral cybercrime treaty for

addressing cybercrime by harmonising national laws. Developed by the Council of Europe, it came into force in 2004 and has been ratified by 65 countries (as of December 2020) including governments in Asia, Americas and the Pacific. For years, it has been considered the gold standard, serving as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between the parties to the treaty. While India declined to adopt the Convention over concerns about sharing data with foreign agencies, we have been reconsidering the stand since 2018.

Prompted by Russia since over a decade, the U.N. General Assembly adopted a resolution in December 2019 to establish an open-ended ad hoc inter-governmental committee of experts (representative of all regions) to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. It will take into consideration the existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes.

A three-day organisational session was held in May 2021 to agree on an outline and modalities for the further activities to draft a global comprehensive

cybercrime treaty. Following this, the General Assembly adopted a resolution for 'Countering the use of information and communications technologies for criminal purposes'. The ad hoc committee will convene at least six sessions of 10 days each, the first of which will be held in New York from 17th to 28th January 2022. The

negotiations are expected to conclude in 2023 after which the committee will present a draft convention to the General Assembly at its 78th session.

### Conclusion

Both devices and people are vulnerable to dangerous attacks in the cyberspace. Governments have to strike the right balance between addressing the increasing threat of cybercrime and protecting the rights of its people. ▶



**Between March and April 2020, India has witnessed a staggering 86% increase in cyber-attacks. Women are both disproportionately targeted by online violence and suffer serious consequences as a result.**

Some of the mindful companies are using ingenious means to help employees avoid social engineering scams and maintain information security while at it. Multinational professional services company, Accenture has a policy where 'spoof' phishing mails are randomly sent to employees every month. Employees who fail to recognise the attack and repeatedly click on the link/attachment have to complete specific learning assets, enroll for training or consequences program. Recurrent failures can even lead to salary cuts and job loss!

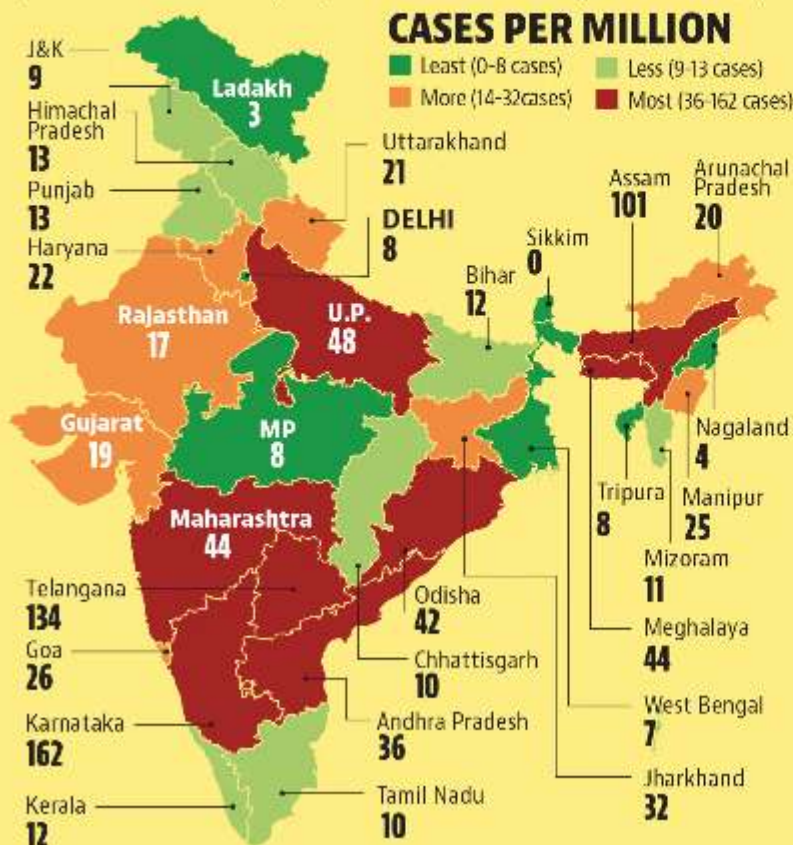


## Not Just Work and Studies; Even Crime Surges Digitally During The Pandemic

India reported a whopping 50,035 cybercrime cases in 2020, showing an increase of 11.8% over the previous year as per the 'Crime In India 2020' report by the National Crime Records Bureau (NCRB).

### Vulnerable digital space

Number of cases filed last year under sections dealing with cyber crime rose to 50,035 from 44,735 a year before as more people moved to working from home, spending more time with digital tools



### RATE OF CRIME

State	Cases filled in 2020	Change from 2019
Uttar Pradesh	11,097	-2.8%
Karnataka	10,741	-10.6
Maharashtra	5,496	10.7
Telangana	5,024	86.7
Assam	3,530	58.2
Odisha	1,931	30.0
Andhra Pradesh	1,899	0.7
Bihar	1,512	44.0
Rajasthan	1,354	-23.2
Gujarat	1,283	63.6
Jharkhand	1,204	10.0
Tamil Nadu	782	103.1
West Bengal	712	35.9
Madhya Pradesh	699	16.1
Haryana	656	16.3
Kerala	426	38.8
Punjab	378	55.6
Chhattisgarh	297	69.7
Uttarakhand	243	143.0
Delhi	168	46.1

Status check on cybercrimes in the country in 2020

**THE NCRB, UNDER** the Ministry of Home Affairs, functions as a repository of information on crime and criminals. It collects and analyses crime data as defined by the Indian Penal Code and special and local laws in the country. Headquartered in New Delhi, the agency publishes the annual 'Crime in India' report with comprehensive statistics of crime that provide insight into the law and order situation across the country. The report also serves as a crucial tool for investigators in linking crime to the perpetrators.

According to the 68th edition of the crime report released in September this year, a total of 66,01,285 cognisable crimes - comprising 42,54,356 Indian Penal Code (IPC) crimes and 23,46,929 Special and Local Laws (SLL) crimes - were registered in 2020. With the year marked by months of national lockdown, the number of traditional crimes like theft, burglary, robbery and assault on women dropped by about 2 lakhs. Even violent crimes registered an overall decline of 0.5%.

On the other hand, the rate of cybercrime incidents per lakh population surged from 3.3% in 2019 to 3.7% in 2020. Of the 50,035 cybercrime cases reported in 2020, there were 4,047 cases of online banking fraud, 1,093 cases of OTP frauds, 1,194 cases of credit/debit card fraud, 2,160 cases of ATM fraud, 578 cases of fake news on social media, 972 cases of cyber stalking or bullying of women and children, 149 cases of fake profiles and 98 cases of data theft.

Among states, the maximum cybercrime cases were reported in Uttar Pradesh (11,097) followed by Karnataka (10,741), Maharashtra (5,496), Telangana (5,024) and Assam (3,530). Most of the states reported an increase in the number of reported cases in 2020. It is only Sikkim which recorded zero cases of cybercrime in the last year. Vis-à-vis 2018, the cases have increased four times in Bihar and Telangana, three times in Tamil Nadu and Manipur and two times in Odisha, West Bengal, Karnataka and Chhattisgarh.

Looking at the city-wise breakup of the reporting of cyber offences, Bengaluru leads the rankings followed by Hyderabad, Mumbai and Lucknow. While the top 20 major cities of India together contribute over one-third of the cybercrimes across the country, the number of reported cases there rose by only 0.8%.

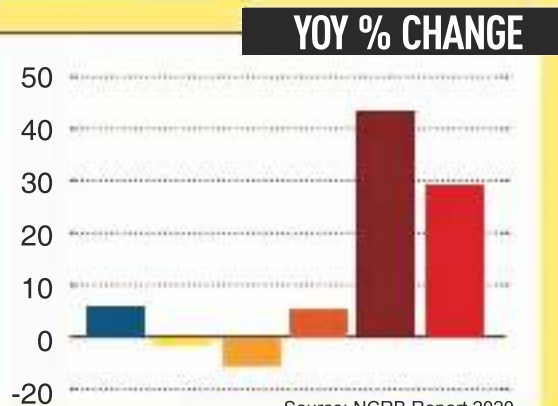
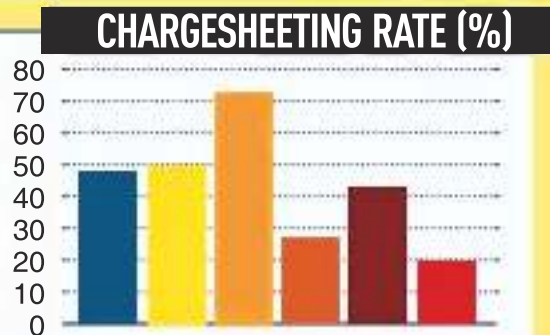
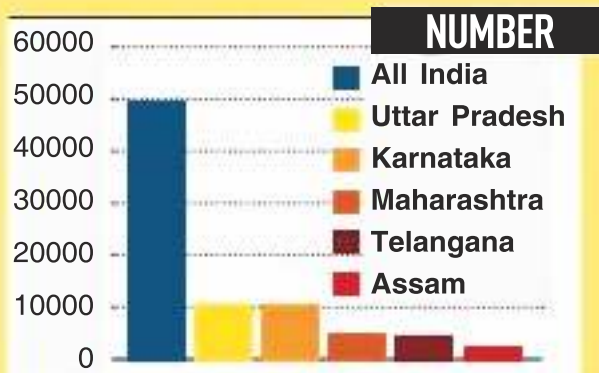


of cybercrime cases reach the stage of being chargesheeted (across India).



of cases, damage can be controlled if public are informed early (But no proper system exists yet).

## Numberwise CYBER CRIMES IN 2020



Source: NCRB Report 2020

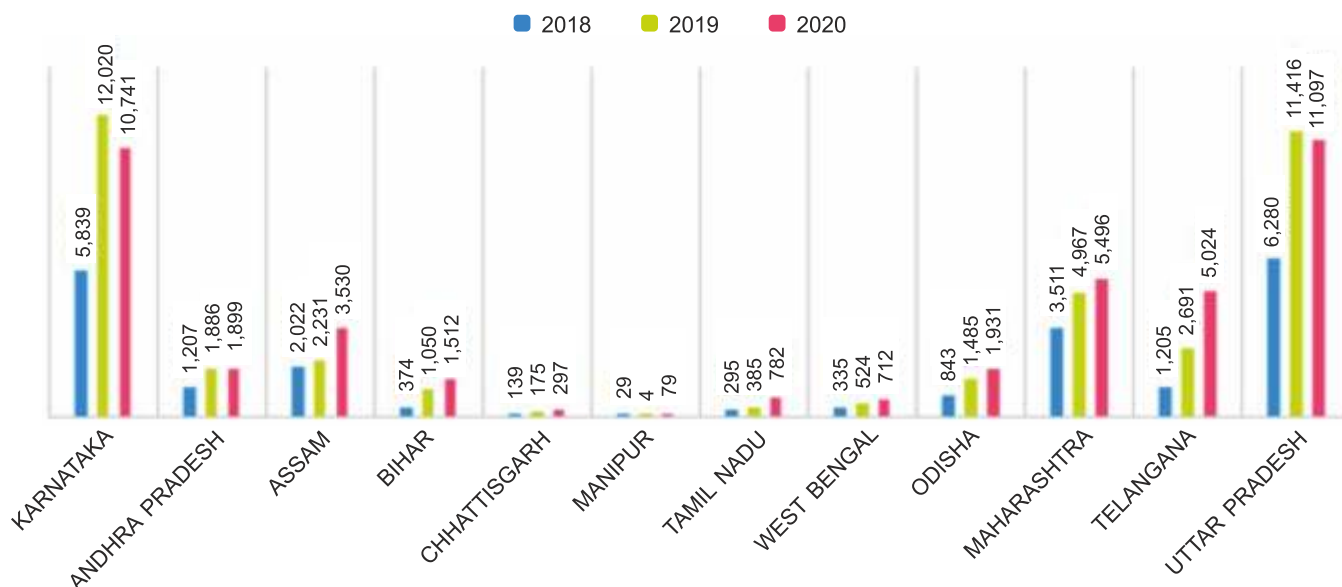
It is notable that more people are being targeted in smaller cities with most of the sharp jumps being seen in Telangana, Assam, Bihar, Odisha and Jharkhand as compared to 2019. However, this could also hint at deep disparities in reporting of cases between regions.

### Most Commonly Recorded Crimes in Indian Cyberspace

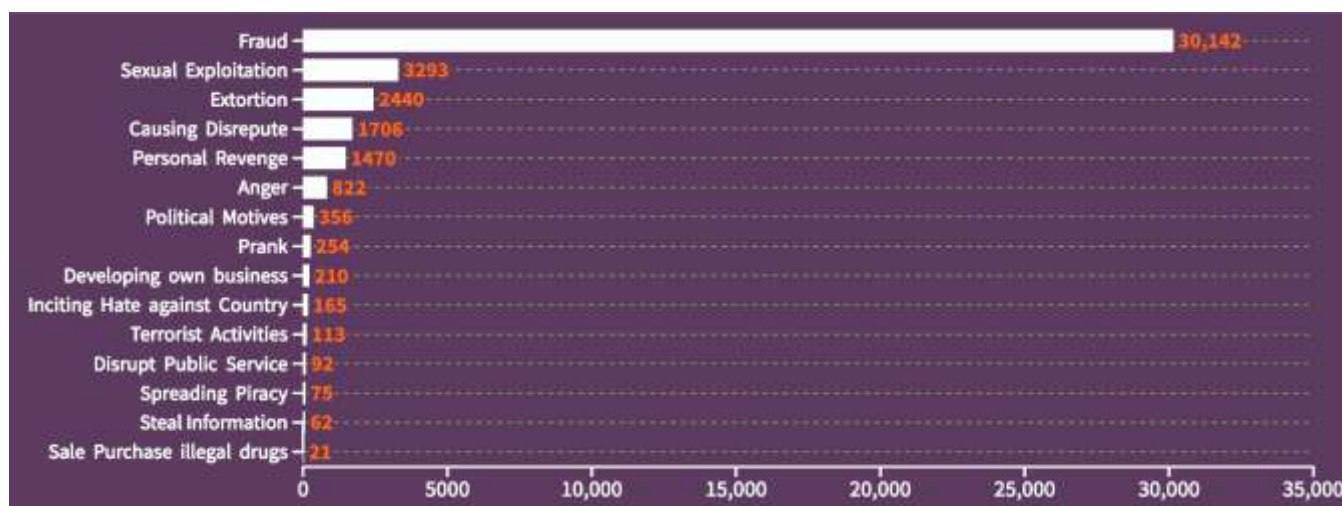
When it comes to the intent behind the cybercrime:

- Fraud was the key motive in 30,142 or 60.2% of the total cases.

## STATE-WISE CYBER CRIMES RECORDED IN INDIA



## CYBER CRIME BY MOTIVES IN 2020



Source: NCRB | 'Other' motives not mentioned: 8,814

- Sexual exploitation ranked second with 3,293 cases or 6.6% of the total.
- Extortion accounted for 2,440 cases or 4.9% of the total.
- The intent to cause disrepute was the overriding factor in 1,706 cases.
- Personal revenge made up for 1,470 cases.

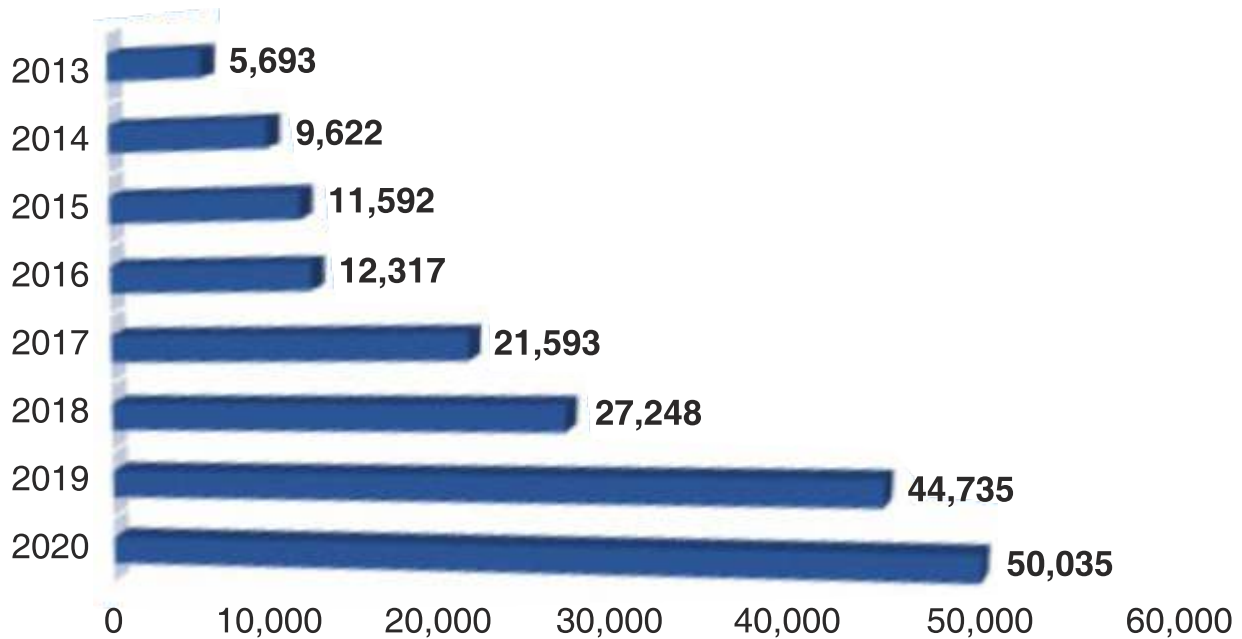
These five motives together accounted for 78% of the total cybercrime cases reported in 2020. Karnataka, Uttar

Pradesh and Telangana together made up 62% of the cases reported with fraud as the motive. Online sexual exploitation was reported mostly in Maharashtra, Uttar Pradesh and Assam. Cyber extortion was reported the most in Uttar Pradesh, Assam and Odisha.

Uttar Pradesh topped the charts for the highest reported crimes of forgery and privacy violation, Karnataka for identity thefts, Bihar for credit/debit card and ATM frauds, Telangana for online banking frauds, OTP frauds, cyber blackmailing and fake news on social media and Jharkhand for online gambling.



## CYBER CRIME REPORTED IN INDIA



### Year-on-Year Increase

The number of cybercrime cases rose from 44,735 in 2019 to 50,035 in 2020 (an increase of 11.8%) which is mostly attributed to the fact that more people moved to working and studying from home apart from spending more time with digital tools during the pandemic. However, it should be noted that the figures stood at 27,248 in 2018 showing an increase of nearly 85% in 2020. Moreover, the cybercrimes reported to the police have jumped almost nine fold from 2013 to 2020 with the numbers standing at just 5693 in 2013.

Again, the authorities caution that the data doesn't necessarily indicate more crime; it can even signal better reporting in the past few years!

### Just the Tip of the Iceberg

The overall numbers pertaining to cyber offences look huge, but the fact remains that they may still not represent the real picture. The ground reality is actually much more overwhelming as most of the cyber attacks tend to go unreported. Companies do not want to compromise their reputation and business on account of the data and security breaches. Filing a complaint will open up their data to the authorities and can cause privacy and other issues, that too without any assurance that the investigators can successfully track and apprehend the miscreants.

Indeed, the disposal of cybercrimes also cuts a sorry picture in the NCRB report with the charge-sheeting rate standing at 47.5% and the pendency rate at 71% at the police level. The judiciary did not perform any better with

the conviction rate standing at 68% and the pendency rate at 89%.

Many individuals hesitate to report the cyber offenses as they are either not aware of the cyber cells and other reporting facilities or do not want to get embroiled in the long-drawn-out legal drama. Cyber security experts uphold that almost every second person has been targeted by a cyber scamster!

To add to this, the sources of cybercrimes are also spreading wide. Jamtara in Jharkhand was once considered the epicentre of cyber frauds, but now there are many more hotbeds like Bharatpur in Rajasthan, Gwalior-Chambal region in Madhya Pradesh, Palgar in Maharashtra and Noida in Uttar Pradesh. The perpetrators are also spreading to neighbouring areas like Deoghar in Jharkhand, Agra and Meerut in Uttar Pradesh, Nuh in Haryana and other places in Maharashtra as well.

Police officials from at least 22 states have visited the Bharatpur cyber police post since January 2021 to trace cyber criminals who are duping and cheating their residents.

### Conclusion

The spikes in cybercrime will continue unabated until the authorities work dedicatedly and with sophisticated measures to investigate, apprehend and punish the culprits. Immediate crackdowns are the need of the hour to keep the cyber offenders from escaping the clutches of the law! ■

## Consumers Should Take Ownership of their Online Lives

Our growing reliance on digital tools signals an imperative need to equip ourselves with the knowledge and skills of not only how to use technology, but also how to behave responsibly while staying safe in the online realm.



*The internet is a valuable tool. But it is important to watch out for potential hazards as bad actors are constantly trying to cause us harm for their personal gain.*

**AN IAMAI KANTAR** ICUBE 2020 report estimates that 323 million or 67% of urban India is using the internet while the number stands at 299 million or 31% of the rural population. It further stated that by 2025 there will be more internet users in rural India than in urban India. According to Statista, there are over 340 million Facebook users in India as of 2020 – 'If India's Facebook audience were a country, then it would be ranked third in terms of largest population worldwide'.

Kerala has declared internet as a basic human right and that all citizens should have access to wi-fi!

However, does the soaring internet usage mean that the internet population is equally savvy about how to actually surf online, etiquette practices and safety protocols? Another study pegs that only 25% of the female social media users in the country are aware of cybercrime!

Take Mr. Verma, a real estate broker for example. When his office air conditioner was not cooling properly in the middle of the summer, he did not think twice before looking up the company's customer care number on Google. On calling the listed number, he was puzzled when there was no proper response to his query; his complaint was apparently registered but he did not get any automated confirmation message from the company or any other follow-up. An hour later, he was in for a huge shock when Rs. 5.6 lakhs were siphoned off his bank account. Alas, Mr. Verma was just one of the naïve folks who fell prey to the ingenious online frauds!

be it communication or financial transactions. Posting anything online becomes a permanent record that can come back to haunt us later. And we have to be especially vigilant for suspicious content and not open links or messages that are from unknown or untrustworthy senders.

Additionally, there are a lot of subliminal messages and misinformation out there. Tracking cookies are covertly latching onto each and every thing that we are doing online. Then there is the digital footprint and online identity that everyone is talking about.

Do not take your data or information about you that is stored online for granted. Reading privacy policies and managing privacy settings is essential for safeguarding our online privacy. In fact, be wary about the kind of personal information you are sharing online.

In short, digital literacy is about being aware of the inherent dangers of digital technologies and protecting ourselves with both technological safeguards and good practices.

## Reporting Cybercrimes

Cyber predators are using latest technologies and innovative ideas to gain access to our data and use it to withdraw money, blackmail, stalk, harass or other crimes. We are quite susceptible to falling victim to cybercrime even despite our best efforts to stay safe online. In such a case, do not let embarrassment or fear of defamation keep you from reporting the offence.

## The intersection of technology and literacy is about making informed choices when operating online

Digital internet tools like search engines, email programs, social media platforms and online videos have made our life much easier and more enjoyable. But digital literacy is important for knowing how to properly find, create, consume and share the digital content at our disposal. This covers a broad range of skills – from using appropriate keywords to search on Google, navigating the results and clicking on the hyperlinks and graphics for a more interactive experience to creating YouTube videos, posting views in the comments section of blogs and using the Share button on Facebook.

That's not all either! Digital literacy also includes being able to evaluate what you find in an online space – like assessing the objectivity, authenticity and accuracy of the content, reliability of a website, repercussions of posting offensive or hateful content online and copyright issues when using other people's pictures, images or videos. This calls for becoming critical consumers online to be able to gauge the legitimacy of online information which will also become key for identifying 'fake' or 'scam' content peppering our emails, social media feeds, instant messaging chats and pop-ups. Above all, it is crucial to always be conscious of your personal security while surfing the internet.

## Appropriate Internet Behaviour

As a rule, we have to be as respectful and watchful in our online interactions as we would be in the real world –

It goes without saying that cybercrime victims should report even suspected offences as soon as possible. As Anyesh Roy, Deputy Commissioner of Police, Delhi Police's Cyber Prevention, Awareness and Detection (CyPAD) Centre observes, "In case of cyber frauds, timely reporting of the crime is the key. Almost all the cases, where the victims' money was retrieved, were reported within 24 hours of the crime. The chances of recovering the cheated money are certain till the illegal transactions don't become irreversible, meaning the amount is either withdrawn in cash or reaches a stage where it is immediately not possible for the concerned financial institution to block the account."


The authorities are becoming more cognizant of cybercrimes and devoting more resources to responding to the threats. There are dedicated cybercrime cells that use sophisticated tools to investigate the crime and apprehend the criminals. Here it is not just about bringing the nefarious elements to justice but also keeping them from harming other innocent victims in a similar manner!

## Conclusion

While the government should educate and prepare technology users to protect themselves, we ourselves have to become digital citizens who can use technology appropriately, thus becoming better internet users by being aware of and identifying the potential risks and proceeding with caution at all times. ▀



## Towards a Safe and Secure Cyber Ecosystem



Like all good things, the cyberspace also requires regulation to safeguard it from potential abuse. The Information Technology Act, 2000 is the national legislation governing everything to do with technology, computers, ecommerce and e-communications.

*The Information Technology Act 2000 is a remarkable milestone in ensuring safe internet access to the citizens of the country*

**IT IS HUMAN** tendency to find ways to exploit and misuse every good thing; technology is no exception. The founders of the internet could never have envisaged the sneakily creative methods that miscreants will come up with to violate the cyber cosmos and perpetuate wrongdoings.

Increasing computerisation made it paramount to protect the rights of innocent and unsuspecting internet users. In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-Commerce to spearhead legal uniformity on a global footing. This was designed to recognise electronic records and accord it the same treatment as paper communication and records. The UN General Assembly endorsed it as the backbone for national cyber laws and recommended that all member States should favourably consider the said Model Law.

## Safeguarding the Cyberspace

The Indian Ministry of Commerce swung into action to draft an e-commerce law and with the passing of the Information Technology Act 2000, India became the 12th country to legitimise cyber regulations.

The principal focus of the new Act was 'to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies'.

However, it was not only restricted to providing legal inclusiveness to e-commerce, registering electronic records with the government and granting legal recognition to digital signatures. The policymakers attempted to account every miniscule action or transaction happening on the world wide web at that time along with the reaction in the global cyberspace while prescribing appropriate legal implications and penalties for various offences and contraventions.

The Act also made amendments to the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

While this legal framework finally ensured that an information is not denied legal effect, validity or enforceability just because it is in an electronic format, there were still quite some glaring loopholes and omissions in the legislation. A major amendment led to the Information Technology Amendment Act, 2008. Some of the salient features introduced for further empowering and protecting the internet consumers include:

- Focus on data privacy
- Attention to information security
- Reasonable security practices to be followed by corporates
- Redefine the role of intermediaries

- Inclusion of cybercrimes like pornography, cyber terrorism and voyeurism

It also introduced Section 69 to invest the authorities with the power to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource in expedient circumstances, subject to compliance of procedure. Under section 69A, they can also block any websites from public access in the interest of sovereignty and integrity of the nation.

Furthermore, Section 75 expressly states that the Act will cover offences or contravention committed outside India, in cases where this involves a computer or a computer network located in India.

The controversial Section 66A penalised publishing of offensive, false or threatening messages/emails to mislead or deceive the recipient about the origin of such communication. This was actually a vague section prime for misuse. It was purported to violate the fundamental right to freedom of speech of the citizens and was struck down by the Supreme Court in 2015 as unconstitutional.

## Case-Free Adjudication

A remarkable feature of the Indian IT Act is the civil remedy in the form of adjudication – the victim does not have to file a police complaint or approach other investigating agencies. The Government of India appoints an adjudicator - officer not below the rank of a director to the central or state government – with specific powers and procedures to adjudicate civil offences related to cybercrime and data theft. However, consumers are not aware of such a useful provision and fail to take advantage of the same.

The Act also established the Cyber Appellate Tribunal (CAT) with appellant jurisdiction guided by the principles of natural justice.

## Driving the Fight Against Cybercrime

The Ministry of Communications and Information Technology was initially responsible for IT policy, strategy and development of the electronics industry. In 2016, the Ministry of Electronics and Information Technology (MeitY) was carved out as a standalone ministerial agency for promoting e-development in the country through e-governance and securing the cyberspace. Among other activities, it operates the Indian Computer Emergency Response Team (CERT-In) - the National Nodal Agency for collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cybersecurity incidents, emergency measures for handling cybersecurity incidents etc.

The Central Government also has a dedicated Cyber And Information Security (C&IS) Division which set up the Indian Cyber Crime Coordination Center ('I4C') in 2020. It comprises of seven distinct agencies including the National Cyber Crime Reporting Portal (<https://www.cybercrime.gov.in/>) to facilitate victims/complainants to report cybercrime complaints online. These are dealt with by the police or other law



### List of offences under the IT Act and the corresponding penalties:

Section	Offence	Penalty
65	Tampering with computer source documents - Concealing, destroying, altering any computer source code; fabricating electronic records or committing forgery	Imprisonment up to three years, or/and with fine up to Rs. 200,000
66	Data theft and other computer system related offences	Imprisonment up to three years, or/and with fine up to Rs. 500,000
66B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to three years, or/and with fine up to Rs. 100,000
66C	Identity theft by using others' password or electronic signature	Imprisonment up to three years, or/and with fine up to Rs. 100,000
66D	Cheating by personation using computer resource	Imprisonment up to three years, or/and with fine up to Rs. 100,000
66E	Privacy violation - Publishing or transmitting private images of others without their consent	Imprisonment up to three years, or/and with fine up to Rs. 200,000
66F	Acts of cyberterrorism that threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorised to access the computer resource or attempting to penetrate or access a computer resource without authorisation (including computer contaminant)	Imprisonment up to life.
67	Publishing or transmitting obscene material in electronic form	Imprisonment up to five years, or/and with fine up to Rs. 1,000,000
67A	Publishing images containing sexually explicit acts	Imprisonment up to seven years, or/and with fine up to Rs. 1,000,000
67B	Publishing pornography or predating children online	Imprisonment up to five years, or/and with fine up to Rs. 1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs. 1,000,000 on second conviction.
67C	Failure by intermediaries to maintain records for specified duration	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
69	Failure/refusal to decrypt data in case of specific extenuating cases or for investigation of an offence	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to Rs. 500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to Rs. 100,000.



enforcement agencies. Almost 2 lakh complaints were lodged in 2020 itself.

The portal also hosts a Citizen Financial Cyber Frauds Reporting and Management System for immediate prevention of money loss with a designated helpline number – 155260 which is operational in some states as of now. The Delhi Police's Cyber Prevention, Awareness and Detection (CyPAD) Centre revealed that the Delhi Police received a total of 3,112

complaints of cyber financial frauds on this helpline between April and August 2021. Nearly Rs. 14 crore was siphoned off from the accounts of the victims (whose complaints were found to be genuine after verification). About 10% of the defrauded amount (Rs.1.42 crore) was returned as the cyber cell officials quickly blocked the suspects' accounts through the concerned banks, online wallet firms and payment gateways after receiving the complaints.

The National Cybercrime Threat Analytics Unit (TAU) is a platform for analysing all pieces of puzzles of cybercrimes. It produces cybercrime threat intelligence reports and organises periodic interaction on specific cybercrime centric discussions. Other agencies include National Cybercrime Forensic Laboratory, National Cybercrime Training Centre, Cybercrime Ecosystem Management Unit and National Cyber Crime Research and Innovation Centre.

Several states are setting up dedicated cybercrime units to ensure proper handling and quicker disposal of cybercrime cases. The Delhi Police has set up a separate wing for cybercrimes and has a cyber fraud detection unit in every district. Telangana too has a dedicated cybercrime investigation department while Rajasthan is set to have a cyber police station in every district. Kerala is forming a new cyber police battalion and Karnataka has made cybercrime detection training mandatory for police personnel in the state. The latter has started registering cyber financial fraud cases as a Cybercrime Incident Report (CIR) which is referred to a particular control room to coordinate with the Reserve Bank of India to freeze the beneficiary's accounts within just two hours.

The National Cyber Coordination Centre (NCCC) was set up as a multistakeholder cybersecurity and e-surveillance agency in 2014. The first phase is operational to scan the country's web traffic round the clock to detect cybersecurity threats and other malicious activities in real time and fend off such domestic/ international threats in a timely manner. The NCCC Director is now vested with the requisite powers to block any online content.

The National Cyber Security Policy 2013 laid down several strategies for protecting the public and private



*With growing digital sophistication,  
no law anywhere in the world  
can be completely comprehensive in  
controlling and preventing cybercrime*

infrastructure from cyber-attacks. But it failed to get implemented properly and has even become outdated now. Another new National Cyber Security Strategy (NCSS) is in the works to ensure cyber awareness, safety through cyber audits, preventive measures, action during cyberattacks and remedial measures.

Many state police departments are organising awareness workshops for their personnel about common online

frauds that have increased during COVID-19 with specific sessions on Internet Protocol Detail Record (IPDR) analysis and cryptocurrency fraud. The government is issuing public alerts and advisories for consumers to beware of counterfeit products, phishing attacks and spread of misinformation.

*"I dream of a Digital India where cyber security becomes an integral part of our National Security!" – Prime Minister, Narendra Modi*

## Calling for a New Paradigm of Regulation

Technology is upgrading very fast and is so our dependence on the same. Smartphones and internet technology have become ubiquitous which throws new challenges for the authorities.

*The world had changed considerably in the last few years. The IT Act was last amended in 2008 and the issues that the country is dealing with have changed considerably. A new legal framework that does justice to all these developments and strengthens India's cybersecurity and adjudication process needs to be put in place - Ajay Sawhney, Secretary, MeitY*

The MeitY is working on revamping the regulatory framework of the IT Act to better deal with the massive shifts in modern technologies and other emergent challenges while also harmonising it with the provisions of the Personal Data Protection Bill, 2019. The aim is to make the law more responsive and accountable to the consumers.

## Conclusion

It is not just about the government, the lawmakers and the regulators anymore. Even other stakeholders like the internet service providers, banks, e-commerce portals and other intermediaries have to make prudent efforts to ensure that technology is used for legal and ethical business growth and not for committing crimes. Last but not the least; even consumers have to be conscious of their information security and online safety while ensuring compliance with the laws. ■

**“If you have a case of a wallet being snatched with just Rs 100 in it, you will likely see far greater activity in police stations, than if you report a cyber theft worth crores!,,**



**PROF. TRIVENI SINGH** (IPS), SP, Cyber Crime, Uttar Pradesh Police is currently in charge of investigating cybercrime cases as well as providing administrative and technical supervision to 18 cybercrime police stations located at all commissionerates in the state of Uttar Pradesh.

He has investigated more than 200 types of cybercrimes, arrested thousands of criminals and solved cases involving thousands of crores of fraudulent money. An online fraud of Rs 3,700 crore by Ablaze Info Solutions, Jamtara's fake calls network, gang duping people by stealing bank details and cloning SIMs and gang of job scammers are just some of the notable cases that he has solved successfully.

Prof. Singh has been honoured with several distinctions like President Medal for Gallantry by The President of India, Certificate of Honor by Director, CBI and India Cyber Cop of the Year Award, 2012 by DSCI-NASSCOM. He has also co-authored two books with Amit Dubey, a cyber security expert and crime investigator – Hidden Files: Tales of Cyber Crime Investigation and Hidden Files – Unlock sharing his experiences of nabbing criminals and busting gangs.

We present a curated interview of 'India's First Cyber Cop', Prof, Triveni Singh's comments in various conferences and other forums about the latest trends in cybercrimes, police mitigation strategies and what we should do to stay safe.

**Q Cybercrime is on the rise as the criminals consider themselves to be safe. What is the reason for this and how can we create effective deterrents?**

Cybercrime is the fastest growing industry with almost zero investment. Cyber criminals in India using fake SIMs and mobile phones are running a multi-crore fraud syndicate. With the bare minimum investment, they are churning out a huge profit. Calling fraud, social media fraud, financial fraud, online cheating are some of the most common crimes.

With the advent of the COVID-19 pandemic, India's cyber police have been riddled with fraud websites and scamsters running phishing sites in the name of Indian central government's PM Cares Fund, as well as UPI accounts that are fraudulently promoted. Alongside these scams, cyber criminals have increased the volume of scams linked to the moratorium on credit cards and loans advised by the Reserve Bank of India (RBI).

Through the national cybercrime reporting portal run by Ministry of Home Affairs, UP police have got over 70,000 cases. It also includes some very technical and sophisticated crime like ransomware attacks and attacks on critical infrastructure.

While the cyber police has seen increased reports in recent times, there is still a long way to go. Corporate India must come forward and report any cyber incident to the police. This will not only help in catching the criminals, but data sharing and attack analytics will help in preventing future crimes. Companies should take responsibility for the data leak, cyber-attacks or any other cyber incidents to help the country control complicated cybercrime cases. Corporate India should not engage with criminals or pay the ransom. Instead, they should immediately contact police or other designated government agencies

**Q What are the challenges that Cyber Crime Departments face?**

The key complication lies in not having enough trained IPS officers who can understand new technologies, and lack of proper, consumer-facing awareness campaigns. Training the task force to deal with technologically advanced tasks is a major obstacle presently affecting the Indian cybercrime departments. We need intensive training and workshops to train them about the process, threats and technology. In reality, the police department is given training for 2 to 3 days at the least which cannot be sufficient to understand how a criminal can bypass the entire system.

I will give you a very interesting example. A 17 year old boy came to my office and offered that he can give me whatever I want for free – be it hotel accommodation, flight tickets, insurance, mobile recharge. He spoke about three companies – a general insurance company, mobile company and telecom provider. I invited the CEO and CTOs of these very companies to my office. The boy hacked into their database and created a health insurance for himself for Rs. 10000, booked a mobile phone in his name and recharged the CTO's phone for Rs. 1000 without giving any money! For all three, he had compromised the payment gateway which he revealed

that he did by installing Fiddler and data tamper application on his system! This shows that the modus operandi of the crimes has gone so technical that it is beyond the technical knowledge, understanding or even the imagination of our department.

Despite a steep rise in cybercrime, phishing attacks and online frauds, cyber police still get comparatively lower importance to other task forces. If you have a case of a wallet being snatched with just Rs 100 in it, you will likely see far greater activity in police stations, than if you report a cyber theft worth crores! While you have a significantly large task force in standard police forces, cybercrime departments often have five or six officials working through thousands of reported cases. As a result, the case resolution time also continues to increase.

**Q Which cybercrime techniques do you consider the most complicated and dangerous?**

Earlier it used to be email compromise, social media fake accounts, OTP fraud and wallet fraud. Now there is a paradigm change in the cybercrime landscape. Lot of ransomware attacks are happening – like that on Haldiram food chain or chartered accountants where their entire system was locked and they got a message demanding money in Bitcoin saying that until the payment is done, they will not give the decryption code.

Unfortunately, the law enforcement agencies are not equipped to handle these kind of cases. In some cases, the victim paid the ransom but still did not get their file decoded. Since we are not able to solve the cases, people think we are not taking interest in the cases. But the problem is that we don't have the capability, tools or technology skills to work on these cases. In fact, even top hackers or corporates cannot decipher the key or decrypt the file.

When we try to investigate the Bitcoin cases, the blockchain technology is such that there is perfect anonymity and we cannot resolve who is the sender and receiver. In almost all high profile cases we find ourselves handicapped because of cryptocurrency. There is no fool-proof solution for a ransomware attack and tracking Bitcoin or cryptocurrency which is taken by hackers to decrypt the locked data.

**Through the national cybercrime reporting portal run by Ministry of Home Affairs, UP police have got over 70,000 cases.**

The data of insurance, banking and healthcare industry is easily available on the dark web. You just have to pay the premium and anyone can find data related to any corporate sector. From where does this come – either insiders share the data or criminals hack into the system. In either case, a data breach has happened.

What's more, even call centres have all the data of insurance companies about the bonus, premium, name, age, address and mobile number which can be used to





PROF. TRIVENI SINGH (IPS), SP, Cyber Crime, Uttar Pradesh Police



befooled thousands of people. We have arrested more than 600 call centre employees and recovered over Rs 4,000 crore from such online frauds.

Tracking any VOIP call is very difficult for the police because it is international and we usually do not get proper cooperation in this regard.

Then there is the popup industry which is a malware. They send millions of emails - suddenly you get a popup that your computer or mobile phone has been infected with malware and you should call the number to delete the virus and resolve the problem. This is a VOIP call that lands into India itself and the person says that he is from Microsoft or other tech-support company and calls for payment of \$70 to \$80 to remove it.

**Q What do you think is the most efficient way to tackle cybercrime and what is needed to achieve this?**

I would suggest law enforcement, cyber experts and corporates can come together on the same platform to exchange ideas and data in real-time to crack such cases. Not only technical officials, but top to bottom level employees of a company should follow cyber hygiene to stay safe in the digital world.

**Q The IT Act 2000 has become out of date and is being considered inadequate in many cases. While the Ministry is working on revamping the Act, what kind of changes and additions do you consider are necessary?**

The legal position is that any outsider cannot be a part of the investigation as it has to be done completely by the law enforcement officers. Recently, the government has made a provision so that we can outsource to around 30 to 40 cyber experts who are posted in every police station. They deal with the cyber forensic work like image analysis and preserving of data and can testify in the court as an expert. But the investigation has to be done by the police officer only.

Many a times there is a confusion whether a case is a crime or not. A person was using an application to get

railway tickets immediately and was arrested. Even CBI was working on this case, but the inspector had to leave him as no criminal offence was made against him. On investigating further, we found that they were using manipulation and spoofing tools to manipulate the IMEI number, IP address and MAC address to feed the debit/credit card details which is an offence under IT Act Section 66C and D. Then we booked it as a case of impersonation as they were playing with the source code of the device and changing IP address which is an identity theft.

But in such technology cases, even senior officers always face the question whether it is a crime or not and that's why most of the officers do not take the lead as the issue is so complicated that they think it is better to leave the matter. My suggestion is that there should be a different technology vertical in the law enforcement agencies who will have knowledge of cyber law, intellectual property law and cyber forensic tools/technology to investigate the case.

**Q What do you expect the government should do to promote cyber safety among the public?**

We are appealing for increased support from state and central governments to raise greater awareness regarding cybercrime and ways to deal with it. We also need regulation of online services such as website registrations and payment gateway integration, in a bid to ensure that a website domain is registered with legitimate documentation, which would later help the police in tracking down the perpetrators of online crime activities.

My department is also running campaigns to raise awareness about such attacks, but cyber police around the country still appear to have relatively limited resources at hand, as a result of which cyber cells are facing considerable setbacks in terms of expanding operations in the scale that they should be. There needs to be a greater push from official departments in order to scale up cybercrime tracking operations in India. An early bout of prevention is better than scurrying for cures later! ■





**Pyush Misra**  
Trustee,  
Consumer Online Foundation

## Pre-empting the Dark Side of the Digital Surge with Cybersecurity Readiness

“The COVID-19 pandemic is unleashing a new pandemic in its wake – that of cybercrimes! Indeed, malicious entities are having a field day due to the unprecedented reliance on digital resources and the growing cyber victim pool. What is India doing to keep this in check and protect its citizens?”

– *Pyush Misra*

The pandemic has  
exposed the inherent  
weaknesses of our  
cyber laws





**AS WE VERY** well know, the COVID-19 pandemic has led to a colossal surge in the use of digital technologies. Just prior to this, in January 2020 itself, India had already become the second largest internet user base with 560 million internet users (AIM Research and Jigsaw Academy report).

The forced lockdowns have not only increased the reliance on internet networks, but also caused significant shifts in usage patterns and behaviour. In the 'new normal', employees are working from home, meetings are conducted via audio-video conferencing and even students are studying online. It is not just social interactions, but even our shopping, healthcare, entertainment and other activities have also moved to the cyber realm. Digital payments have grown exponentially, with even the uneducated and rural folks taking to this medium.

The pandemic is moving the world towards increased technological innovation and online collaboration, but cybercrime is also on the rise, with a 600% increase in malicious emails during the current crisis - Izumi Nakamitsu, U.N. disarmament chief

### Ripe for the Picking

Even as we adapt to the extraordinary changes in the way we work and live, we have to consider that our precarious digital habits are making us more susceptible to cyber frauds. The increased online activity is perfect for scammers who do not hesitate to take advantage of the growing vulnerabilities to extract both money and sensitive information. Adolescents and teenagers are spending more and more time on streaming platforms, gaming sites, social media and other youth networks – they are prime targets for the threat actors proliferating the web.

Right at the onset of the pandemic, the cyber fraudsters did not hesitate to play on the fear of COVID-19 to target vulnerable people and health services. Coronavirus-themed online scams (like online sales of counterfeit drugs, fake donation links) and phishing campaigns (fraudulent websites posing as COVID-19 resources or leads for hospital beds/oxygen cylinders) had a field day for months.

The healthcare infrastructure and medical research facilities were also not spared. Many hospitals and test centres faced ransomware attacks - important patient data was taken with the threat of not returning unless the ransom amount (usually in cryptocurrency) was paid. Even the PM CARES Fund has been one of the targets of the malicious hackers with sham versions defrauding people of their money.

Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19 - Jürgen Stock, Secretary General, INTERPOL



“The COVID-19 pandemic has accelerated the shift towards a more digital world. Changes we make now will have lasting effects when the world economy starts to pick up

again. This survey offers valuable insights that can inform our digital strategies and policies, as we turn the page from pandemic response to recovery.”

– **Mukhisa Kituyi**  
Secretary-General of UNCTAD



The Norton Cyber Safety Insights Report, April, 2021 states that nearly 330 million people (across ten countries including India) have become victims of cybercrime in the past year and more than 55 million people were victims of identity theft. Set up in 2020, the I4C reporting portal had received 3,17,439 reports of cybercrime incidents and 5,771 FIRs as of 28th February, 2021.

Both the numbers and the methods continue to rise with cybercriminals developing more advanced modus operandi to prey on the heightened dependency on the internet.

## Ensuring Secure Functioning in Cyberspace

India has been characterised by large scale lapses in digital security and part of the blame rests at the door of our fragile cyber laws once again. The government is aware of the escalating scams, frauds, intrusions, security breaches and other threats which is compounded by the fact that scores of people are using digital applications for the very first time during the pandemic.

Measures are being taken to educate the authorities and alert the consumers. The government's strong stand against Zoom forced the provider to upgrade the security measures. Yet, the efforts appear to be mostly haphazard

and reactive. The lack of proper enforcement coupled with minimal penalties fail to daunt the offenders. If caught, they will be imprisoned for a few years at most, which is not a very effective deterrent.

It cannot be denied that the Information Technology Act, 2000 has many grey areas and has proved to be inadequate when it comes to cyber-squatting, spam mails, ISP's liability in copyright infringement, etc. It is also silent on the software backup maintained by corporates and public sector undertakings in overseas locations and the subjective legal jurisprudence on them. Similar is the case of downloading updates and upgrades for operating systems and other software of foreign origin which can involve spyware. Various cybersecurity



breaches faced by big corporates and healthcare organisations find no mention in the law and have to be handled under the sections of hacking and online fraud.

There are many other gaps on account of the new and developing cybercrimes for which the law needs to stretch its arms. Emergent technologies like Artificial Intelligence and Machine Learning, quantum computing, ransomware and cryptocurrency barely existed in 2008. Electronic financial services and online gambling also call for separate policies to tighten the grip. Territorial

jurisdiction and preservation of online evidences need to be addressed urgently.

Strengthening the cyber security infrastructure and invoking stringent punishments is the need of the hour. The government has to take a proactive approach by developing a robust multi-lateral system of law, technology and public policy that is transparent, centralised and also affords smooth coordination between the state agencies to nab the perpetrators. There is a need for strong enforcement with accountability of officials as well.

## Conclusion

With cybercriminals using the latest inventions to initiate innovative troubles, lawmakers have to go the extra mile by refining and upgrading the laws on a continuous basis to stay well-equipped to deal with cyberwarfare. ▀

**The Norton Cyber Safety Insights Report, April, 2021 states that nearly 330 million people (across ten countries including India) have become victims of cybercrime in the past year and more than 55 million people were victims of identity theft.**

# E-Commerce

## – Are Consumers Actually Getting What They Paid For?



“Online sellers often make false or misleading statements regarding a product's characteristics or capabilities which induces consumers to make a decision they otherwise might not have made.”

– **Advocate Shashank Sudhi**

**A MAN ORDERED** wireless earphones online - the product description clearly mentioned bluetooth and wireless with quick charging, impressive playtime and connectivity; the images were in tune with the title of the product and even the price charged on the portal was as expected for wireless headphones in the market. Imagine the customer's bewilderment when he opened the package to find regular wired headphones!

A woman saw a Facebook page selling earrings and ordered long dangles with coloured stones for Rs. 1200 only to receive small and plain studs by courier a week later.

Another customer was impressed by a listing for a lace wig with human hair. The product description emphasised on 100% virgin human hair with complete details about the length, cap size, density and more. Customer reviews enthusiastically proclaimed the natural texture, thickness and glossiness of the wig which was

identical to real hair. Yet, on delivery, it was found that the wig was made of synthetic hair and did not even feature a lace front!

This is just a preview of the blatant misrepresentation and cheating happening online. All of us have read umpteen stories of customers getting bars of soap instead of an iPhone, books instead of a Dell laptop or a handkerchief instead of a shirt. Then there are instances of an order for a Sony or Samsung smart TV turning up as an un-branded, non-smart television that is also much smaller in size!

The harangued online shopper sends desperate emails to the customer care department and calls the toll-free number to file a complaint. You have to click pictures of the product, keep it in original packaging and have all the order details handy. If it is an established e-commerce portal, the product will be replaced or refunded, but only after expending time and effort in complaints and follow-ups.



But God save you if it is a new seller or relatively unknown online player! You will most likely be redirected from one customer care executive to another or hear empty consolations like 'We regret the inconvenience', 'The management is looking into the matter' and 'We will refund the money as soon as possible'. There is no communication whatsoever even after endless promises of 'will get back in 7 working days'.

A steady lack of response means that the only recourse is to file a consumer complaint with the District Consumer Forum or approach a consumer protection organisation for redressal. And justice, if any, may be a long time coming.....

## Dissatisfaction and Cheating Abound in E-Commerce

Online shopping is the new way of doing things – it brings the convenience of shopping from a screen without having to step out and brave the traffic and crowds to reach and shop in a store or deal with a salesperson. A few clicks open up a mind-boggling array of choices from around the world, that too with unbelievable prices or other offers.

However, the infinite ease often comes back to haunt the online shoppers in more ways than one. Mis-selling is rampant in cyberspace with many retailers misrepresenting their wares in the product listings or setting false expectations. Dr. Pratima Narayan, a lawyer working on consumer law and e-commerce, observes, "The most common complaints are about not getting a refund or replacement, late delivery and misleading promotions."

## Where does the problem lie?

When it comes to buying something over the internet, the product listing becomes the primary source of information. It contains a description of the product such as the features and benefits along with the price and why it is worth purchasing. This is supported by images and/or videos to provide a pictorial view of the size, colour and other details.

It goes without saying that the words and pictures should clearly and accurately represent what the vendor is selling. While slight variations are acceptable, gross misrepresentation is obviously not.

Yet inconsistencies abound in the form of deceptive images, titles,

characteristics, size, colour options, prices, etc. The unsuspecting consumer is misled by the fraudulent presentation and may even get tricked into buying the said product. And when you don't get what you expected, be it in terms of size, colour or the product itself, it makes for a decidedly unpleasant e-commerce shopping experience!

That's not all either. Apart from product-based deception, e-tailers also indulge in fake reviews for their products which again delude the consumers in terms of what to expect from the purchase. To add to this, even some of the online shopping portals are jumping onto the misleading bandwagon through malpractices of false advertisements and claims in terms of quality, quantity, services, prices and discounts on the products.

## On the regulatory front

Unfortunately, the Consumer Protection Act, 1986 has long been silent on e-commerce issues; online portals and merchants were playing the field by their own rules as they were out of the purview of the law which was enacted when the human race could not even dream of virtual shopping!

Yet, the authorities have given credence to the beleaguered consumers on occasion. In 2015, a consumer court fined online shopping website Flipkart for delivering the wrong product and refusing to process the refund claim after the grace period, even though the company argued that it was only an intermediary between buyers and sellers and could not be held responsible. In 2019, the e-commerce portal Home Shop 18 was directed by the National Consumer Disputes Redressal Commission to compensate a complainant by paying Rs. 16,000 for the unfair trade practice of misleading advertisements of 'free gift vouchers' without specifically mentioning the terms and conditions in the

main advertisement. The portal's contention that the vouchers were 'voluntarily' provided and that the terms and conditions were on the website were overruled by the consumer forum.

However, such resolutions are few and far between. Consumers often find that nobody responds to their calls/emails and they cannot find the refund/return options on the website either. And it does not make sense to expend the time and effort of filing a consumer case for small and paltry amounts.

**Online shopping is the new way of doing things – it brings the convenience of shopping from a screen without having to step out and brave the traffic and crowds to reach and shop in a store or deal with a salesperson.**





**The Consumer Protection Act, 2019 has been enacted with a view to widen the scope of consumer rights and cover the field of e-commerce, direct selling, tele-shopping and other multi levels of marketing in the age of digitization.**

The newly enacted Consumer Protection Act, 2019 has finally broadened the definition of the consumer to bring e-commerce transactions into the fold, thus holding online platforms accountable to their customers. The law also institutes provisions for dealing with false and deceptive advertisements, be it online or offline.

Advertising Standards Council of India (ASCI) released draft guidelines this year for advertising by influencers on Facebook, Twitter and other social media platforms to enable consumers to 'easily recognise promotional content on digital platforms'.

The Consumer Protection (E-Commerce) Rules 2020 require e-commerce entities to ensure that the product and service listings are consistent with the actual characteristics and usage conditions of such products or services. They cannot permit any display or promotion of misleading advertisements on their platform.

Further, the e-commerce players will not be allowed to refuse to take back the goods purchased in case a product is found to be fake or defective, is delivered late or is even found to be different from its accompanying description in the cyberspace.

However, the rules seem to be in cold storage with no signs of being legislated.....

### What You Can Do As A Consumer?

- Steer clear of new or unknown e-commerce companies; research them properly and avoid the purchase if in doubt.

- When buying from a website for the first time, it is better to opt for cash on delivery.
- Comb through the fine print and pay special attention to the Terms of Use and Privacy Policy before making a purchase.
- Get a clear picture of the cancellation, return and refund policies
- Check whether the customer care details like address, email and phone number of the e-commerce company are available
- Do not order in a hurry, take the time to understand the product and warranty description.
- Beware of claims like no exchange or refund, handling charges for refund, etc.
- A trick is to take a screenshot of the product/service you purchased, in case the company changes the price or product description later.
- Before making the payment, check for encryption key – a small key symbol – in the payment portal to ensure that the transaction is secure.
- Do not tamper with or use the product if it is not to your satisfaction. Take pictures immediately and call the customer care number or send an email to file a complaint.

### Conclusion

Misleading e-commerce practices should not be allowed to spoil the online shopping experience anymore. This calls for strict regulation with stringent action. ▶



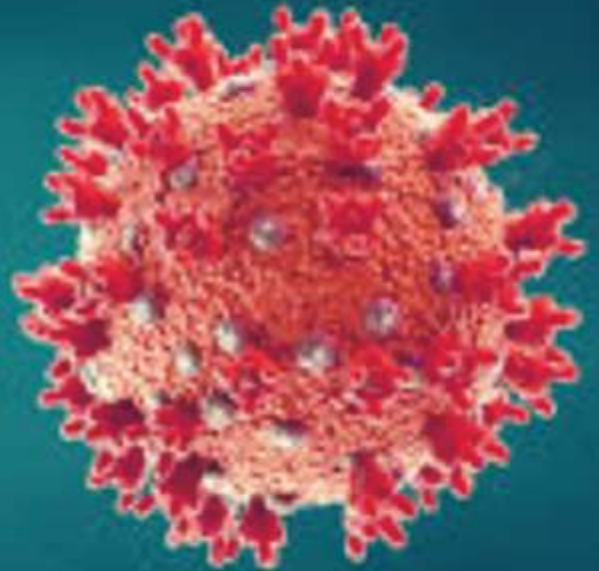
# A Pervasive Misinformation Narrative is Clouding the Consumers' Minds

“News spreads quickly in the age of digital technology and social media; fake news spreads even more rapidly! Indeed, misleading information abounds on social media that can even turn dangerous at times. Stringent measures are necessary to control this digital menace!”

– Payal Agarwal

## FAKE CURES

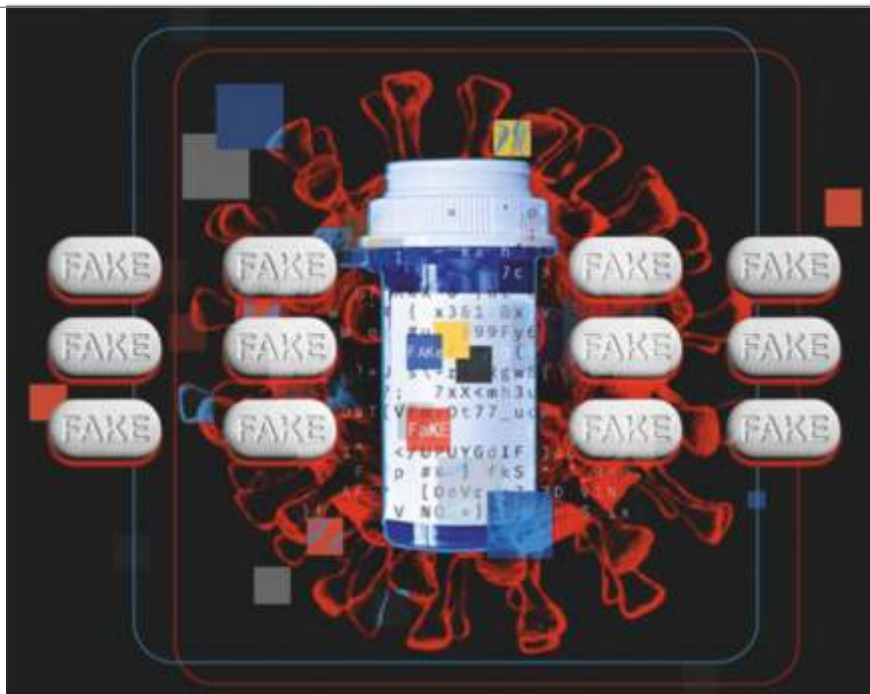
- 'A few drops of lemon juice in the nose will cure COVID-19!'
- 'The heat of summer will kill the SARS-CoV-2 virus!'
- 'Keeping bundles of cloves, cardamom, camphor and mace in the pocket keeps coronavirus at bay!'
- 'Eating spicy food can reduce COVID-19 symptoms!'
- 'A halved onion kept in the corner of the room will catch the COVID-19 germs!'
- 'Drinking alcohol will keep coronavirus at bay as sanitizers also contain alcohol!'
- 'If you are able to hold your breath for 10 seconds or more without coughing or feeling discomfort, you do not have COVID-19!'





# out of the box

\\ A PERVERSIVE MISINFORMATION NARRATIVE IS CLOUDING THE CONSUMERS' MINDS



*The internet has become a tool for spreading both information and falsehood like wild fire. How do we separate factual news from fiction on social media?*

**THESE ARE JUST** some of the fake cures and stories that went viral on social media and messaging platforms in the early stages of the COVID-19 pandemic. The deadly virus was spreading exponentially, but the rumours around it were way faster. The problem with such nuggets of gross misinformation is that people not only believe and act on them, but also keep sharing them in their circles. This ends up encouraging superstitions and unscientific health practices that actually have no evidential proof.

While some of the remedies may be ineffective, some may turn harmful as well. Consider this: A careless comment from then U.S. President, Donald Trump that injecting disinfectant into the body can clean the lungs and fight COVID-19 caused widespread deaths for the next two months due to the spike in intake of bleach, household cleaners and other

disinfectants by the American public! This is just one of the unproven treatments that he thoughtlessly promoted during his tenure.

The scourge of fake news has not been confined to quick-fixes, preventive remedies and cures alone. The COVID-19 misinformation with religious and political overtones was responsible for propelling interreligious discontent too. The

baseless claims made people angry with the government and many even started believing that a particular religious community was responsible for spreading the virus.

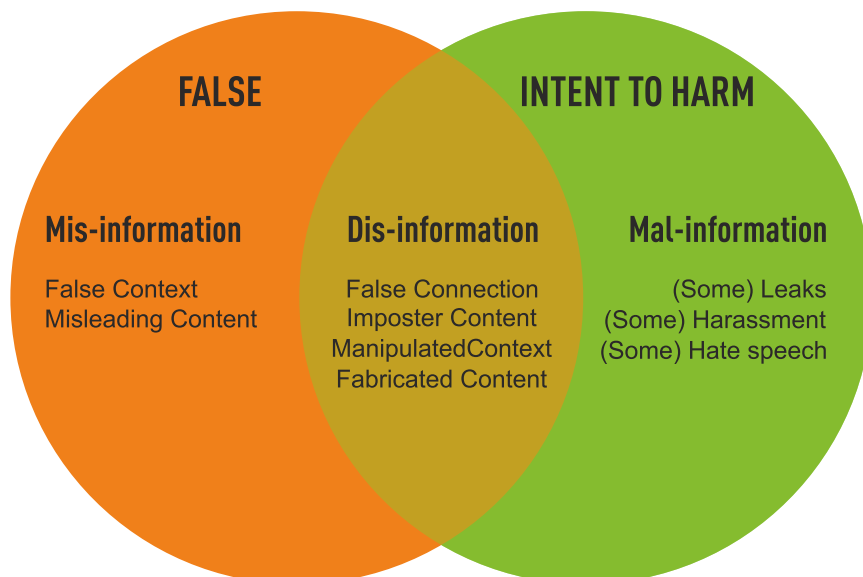
Opportunists have also been taking advantage of the anxiety, fear, panic and desperation among the public to peddle counterfeit preventions, treatments, medications, vaccines, testing kits and more right from day one.

Conspiracy theories have been abounding - from the SARS-CoV-2 virus being purposely created as a biological weapon in a lab in China to the U.S. army introducing the virus in Wuhan to 5G mobile networks causing COVID-19 to even COVID-19 being a hoax or part of an elite plan by Bill Gates to control the world population. *I am sure most of you will vehemently support the first one even while knowing it is mere media speculation, thus giving credence to the sweeping effects of fake news!*

That's not all either.

Many people overreacted to the 'COVID-19 forwards' by unnecessarily hoarding goods while there were dangerous underreactions which made people negate the risks of the virus and prompted unwillingness to comply with the public health guidelines – some

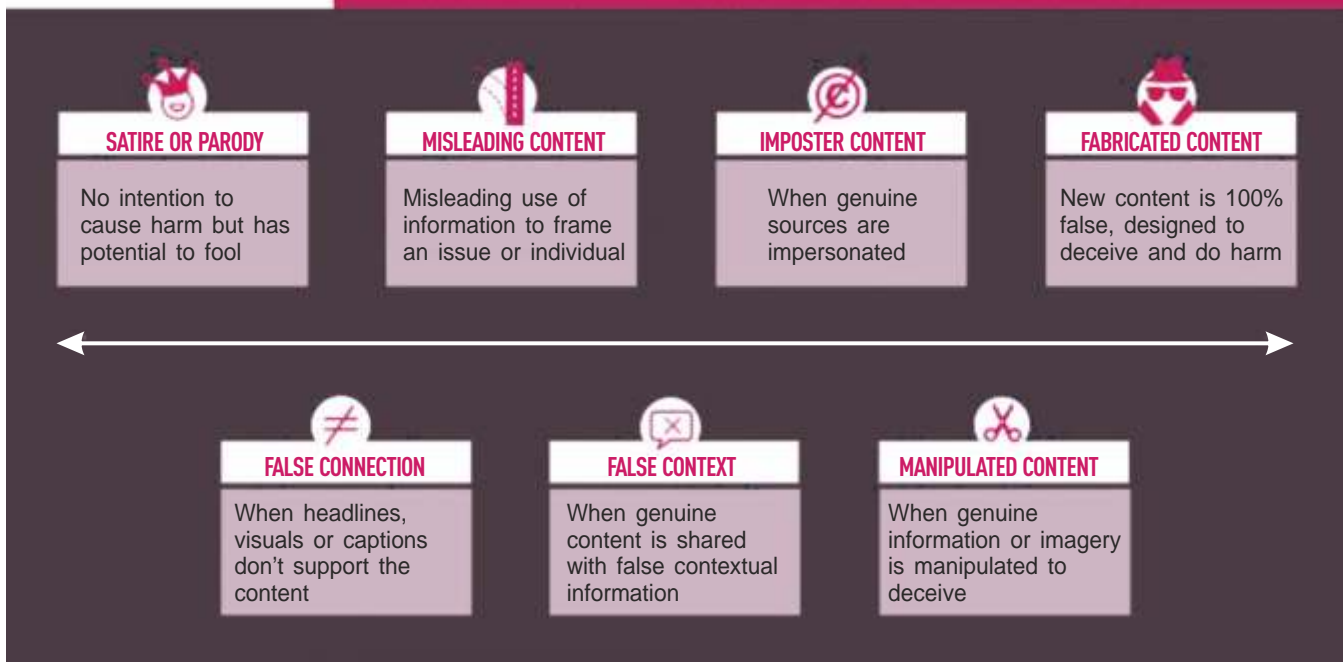
## Misinformation, disinformation, and malinformation



A 2020 Cornell University study found that US President Donald Trump has been the world's biggest driver of Covid-19 misinformation during the pandemic!

## FIRSTDRAFT

## 7 TYPES OF MIS- AND DISINFORMATION



refused to wear masks, some did not practice social distancing while others refused to stay indoors during the lockdowns – thus inadvertently spreading the virus.

The phony stories doing the rounds now range from the vaccine generating magnetic properties in the human body, causing infertility among women and altering human DNA to the jab being used to implant microscopic chips in people to monitor them. This kind of gross misinformation is triggering vaccine hesitancy across the world – sceptical people refuse to get the life-saving shots, thus increasing the potential risks to the population. To add to this, most people are not even aware that a lot of the information out there is actually wrong.....

Indeed, while technology and social media proved to be exceptionally helpful tools for keeping people safe and informed, the sad fact is that the COVID-19 misinformation that was spreading on these same channels not only complicated the health communications and public health responses, but actually claimed many lives too. Recent research

published in the American Journal of Tropical Medicine and Hygiene reveals that in the first 3 months of 2020, nearly 6000 people around the globe were hospitalised and at least 800 people may have died because of coronavirus misinformation.

The World Health Organization warned the public about an 'infodemic' - an overabundance of information, both online and offline, dominated by fake news and misinformation - of the deadly new disease on social media in February 2021 itself. The international health agency stated that, "The coronavirus disease is the first pandemic in history in which technology and social media are being used on a massive scale to keep people safe, informed, productive and connected. At the same time, the technology we rely on to keep connected and informed is enabling and amplifying an infodemic that continues to undermine the global response and jeopardises measures to control the pandemic."

## Prevalence of Misinformation

A recent international study on 'Prevalence and Source Analysis of COVID-19 Misinformation in 138 Countries' revealed that India (15.94%), the US (9.74%), Brazil (8.57%) and Spain (8.03%) are the four most misinformation-affected countries. The researchers analysed 9,657 pieces of misinformation that originated in 138 countries from January 2020 to March 2021. They were fact-checked by 94 organisations to understand the prevalence and sources of misinformation in different countries.

As expected, the internet accounts for 90.5% of the COVID-19 misinformation. Social media (85%) happens to be the biggest producer of misinformation with Facebook alone generating 66.87% of the misinformation among all social media platforms.

The study further stated that at 18.07%, India produced the largest amount of social media misinformation. This was followed by Brazil (9.17%) and the US (8.61%). It was suggested that our higher

internet penetration rate and increasing social media consumption coupled with lack of internet literacy among the users is responsible for the gamut of social media misinformation.

Misleading information surges when a crisis first appears and reliable data isn't readily available  
- author of the study,  
- Md Sayeed Al-Zaman

## Is Fake News a New Phenomenon?

Time was when we got our news primarily from newspapers and television. The information from journalists and media houses was mostly reliable and we never doubted the veracity of the claims. But today news is not only read online, but also ceaselessly liked, commented and shared on Facebook, Twitter and WhatsApp, which end up acting as easy vectors for dubious facts.

The sheer scale of fabricated information that is influencing people's views, pushing specific agendas and creating confusion today is unimaginable. While misinformation – be it intentionally wrong or mistakenly created - has reached an unparalleled scale during the ongoing pandemic, fake news is not a new spectacle. It has just gained more traction during the last couple of years with the growing use of the internet and social media.

False stories about politics, economy and the environment are often used to misinform and deceive the readers. It is believed in many circles that the 2016 US presidential election and even the Brexit referendum was influenced by misinformation spread by other countries. Lynching of innocent people by angry mobs fuelled by inflammatory online posts is an example that hits closer home. We have also seen fake news spread like wild fire and play out unending controversies over the Citizenship Amendment Act in the beginning of 2020.

This is because people not only tend to blindly believe the unverified information; they often fail to properly understand the underlying possibilities and just share the said news without paying much attention. Indeed, sharing anything online is so quick and easy, it can even become viral within no time. This plays into the hands of anti-social elements who deliberately attempt to disseminate wrong information and manipulate behaviour – the particularly active anti-vaxxer movement being a prime example!

## Decoding the Ecosystem of Fake News

Fake news is much more than simply false news stories designed to mislead the readers. Some may have a bit of truth, but lack contextualising

details like verifiable facts or sources. Some may include basic verifiable facts, but the language may be deliberately inflammatory or present only one viewpoint by deliberately avoiding other pertinent details.

As we drown in the tsunami of fake news, the irony is that we tend to take even the genuine pieces with a pinch of salt. It has become incredibly difficult to trust news generating from government sources, reliable institutions and scientific findings too – thoughts like Is this reliable? Could it be bogus? cross the mind more than once for sure! In fact, during the COVID-19 pandemic, we have witnessed first-hand that credible news failed to stand up to the unverified information that was overflowing online.

## Flattening the Infodemic Curve

Authorities and institutions around the world are taking active steps to counter the sharing of misinformation on social media. WHO Director-General, Dr Tedros Adhanom Ghebreyesus observed that, "Public trust in science and evidence is essential for overcoming COVID-19. Therefore, finding solutions to the infodemic is as vital for saving lives from COVID-19 as public health measures...."

The WHO launched the 'Reporting Misinformation' in August 2020 that





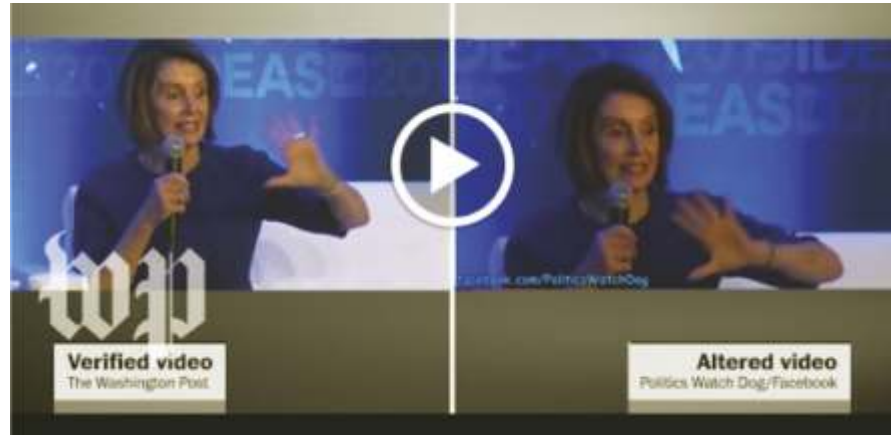
not only galvanised people to verify information, but also showed them how to report misinformation to various social media platforms. The WHO Myth Busters pages regularly clarify the circulating misinformation at <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters>. Many media agencies have also established fact-checker websites to publish articles dismantling false claims about COVID-19.

The Indian government is endeavouring to bring regulation and accountability along with content moderation in the online world. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were notified in February 2021 to regulate the social media intermediaries and online news and current affairs websites. It includes a code of ethics along with a three-tier content regulation mechanism under the Information Technology Act, 2000 - self-regulation by the entities, self-regulation by the applicable entities and oversight by the central government. Social media and streaming platforms are now required to take down contentious content quicker, appoint grievance redressal officers and assist in investigations as well. This has been partly stayed by the Bombay High Court in August.

Meanwhile, Google and Facebook have instituted reporting and flagging tools to tackle fake news. WhatsApp has also added safeguards restricting the spread of chain messages and directing users to accurate online information. But the fact remains that they need to do much more to curb the spread of inaccurate and harmful information that is proliferating in the cyberspace.

### Being Social Media Smart – Nipping Misinformation in the Bud

As consumers, we should also be more aware about false narratives circulating around us. Truth discernment will come when we undertake a critical evaluation by



**A video of US House of Representatives Speaker Nancy Pelosi was slowed down to make her appear drunk. This side by side video was created by the Washington Post.**

Archived on 6th September, 2019.

checking whether the source of the story is credible and reliable. Look at the name of the website and if it is unfamiliar, check the 'About' section or find out more about the author. Eyeball more than just the headline; make it a practice to check the entire article as many fake news stories use sensational or shocking headlines to grab attention.

If a story seems shady, check whether it contains verifiable facts or quotes. Also, find out if other reliable websites/news outlets are reporting on the same information. It is a good idea to check the date, timeline or publishing information as many old pictures and videos are often used to circulate fake news.

Last but not the least; take your own biases into consideration as

personal views or beliefs can often colour judgment about the information. Always think twice before sharing anything on social media – evaluate the news carefully and only share genuine ones. Even if you don't have the time or inclination to verify the same, at least don't click on the Share or Forward button!

And when you spot something that seems fabricated or misleading, it is your duty to not just refrain from forwarding it to others but also report it to the hosting social media platform or the authorities.

### Conclusion

The epidemic of fake news is breeding uncertainty and fuelling distrust. We have to fight the virus on the one hand and misinformation on the other as the latter is affecting a lot more people than the virus itself! This calls for digital media literacy coupled with critical thinking skills when navigating the internet. As Rajneil Kamath, a publisher at fact-checking portal, <https://newschecker.in/> remarked, "People get cheap internet-based tech on their smartphones, but they don't have the necessary education on how to assess the veracity of claims made in the messages!" ▶

A WHO tweet advised – 'False information on #COVID19 is spreading & putting people in danger. Make sure to double-check everything you hear against trusted sources. For accurate information on #coronavirus find official advice from your country's public health authority & WHO.'

## How Can Consumers Take Back Control of their Personal Information?

Given the sheer amount and frequency with which we are sharing our personal information, the possibility of identity theft is becoming greater and greater. A robust data protection and privacy regulation is critical to ensure security in the storage and transfer of data!



*In today's connected world, people are sharing more and more of their personal information online, that too in ways that were not even imaginable earlier*

**TODAY, ALMOST EACH** one of us owns a smartphone, uses the internet and has a social media account. In addition to this, we are constantly using different apps, doing online banking, shopping over the internet, wearing fitness trackers and what not. Do we ever pause to think about the amount of personal information that we are inadvertently disclosing in the process?

Indeed, every time we download a new app or sign up on a website, we are sharing some pertinent details about ourselves with a private or public entity. That's not all either – even in the physical domain, when we book a doctor's appointment or open a bank account, a chunk of our personal information is slipping into their hands.

This is definitely the age of a data economy. Apps, social media platforms and other websites all need to collect and store our personal data to provide the seamless services that we take for granted. But the hitch here is that this ends up revealing details like your name and where you live to your thoughts, habits and life in general. In fact, almost everything about you is out there, just waiting to be exposed and misused. And it can be exploited in ways that you can never even imagine!

## Elements of Personal Data

The U.S. General Services Administration defines Personal Identifiable Information (PII) as, 'Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.'

The critical pieces of data that we knowingly or unknowingly reveal include:

- Basic information like full name, address, birth date, mobile number and email address
- Personal identification numbers like Aadhaar number, PAN number, passport number, driving license number, vehicle registration number, etc.
- Health and medical records, insurance details and more
- Financial data including bank account and credit/debit card numbers
- Personal characteristics like photographs or handwriting
- Biometric data of retina scan, voice signatures and fingerprints
- Technology information like Internet Protocol (IP) and MAC address that becomes a consistent link

This kind of information is regularly collected by apps, websites and other platforms and we share the details without a second thought. Apart from this, every time we are online, all our activities are being stealthily tracked and recorded through cookies. Our Google searches and Facebook posts are constantly giving away a little about us – be it our interests, what we need or where we are. The harsh fact is that our online behaviour can even slip leads about our racial or ethnic origin, sexual orientation, political opinions, religious beliefs, etc.

This way our information tumbles into hands that we are not even aware of, leaving us with much less privacy than we can ever realise. In fact, with increasing technological



## Data Privacy

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete the data



## Data Security

Measures that an organization is taking in order to prevent any third party from unauthorized access.

---

*Data privacy defines who has access to data; data protection provides tools and policies to actually restrict access to the data*

developments, novel and intrusive ways of collecting and processing personal information are coming to the fore.

## The Risks are Manifold and Growing

It is not as if the online platforms are purposely collecting the data for potential misuse. Businesses need it to meet our needs like delivering products/services and more. However, this sensitive data is stored on the company computers, servers and in the cloud. It can easily fall into the wrong hands who can exploit it in myriad ways to cause harm, loss or other damage.

A malicious attack by criminal elements to access personal details is known as a data breach and the leaks can blow into a massive violation of user privacy. Financial and healthcare companies, apart from government organisations, are the prime targets of such cyber attacks. Criminals use this personal data to harass users, defraud them or commit identity theft. This can lead to fraudulent charges on your credit card, bank account being flushed out or even criminal activities being conducted under your name.

However, the fact remains that violation of personal data is not always from external hackers. There are insider threats from employees who might inappropriately access the data. Then there is the risk of unintentional exposure by someone who has access to the data. Something like careless disposal of computer equipment or other data storage media can also compromise the privacy of the consumers.

It's not just about negligence here, some entities even exploit user data for personal gain, even to the extent of selling it to third parties for advertising and other purposes.

## Importance of Data Protection

This is where data protection comes into the picture. Indeed, businesses derive great value from the data that they collect from their consumers. However, companies should be aware that this is borrowed data and it is their



primary duty to safeguard it at all costs and keep it from getting exposed in any manner.

This calls for a robust data security policy as any kind of breach can weigh the company down heavily in terms of financial liabilities, loss of reputation, impact on business and more. According to the Cost of a Data Breach Report 2020 (Ponemon Institute), the average total cost of a data breach is USD 3.86 million. Research also reveals that 69% people consider that strong privacy and security practices help preserve trust in the company.

Data protection is nothing but safeguarding of personal information by organisations to ensure that it does not get compromised, corrupted or lost. It includes a set of standards, strategies and measures that are instituted to prevent unauthorised access by third parties as well as intentional or unintentional disclosure, alteration or deletion of the data. The arsenal for protecting the integrity and availability of data encompasses technological weapons like data loss prevention (DLP), access control, encryption, tokenisation, hashing, network security and other practices.

## Concerns of Data Privacy

With the huge amount of sensitive data being shared across the globe, the apprehensions of private individuals are no longer just limited to whether their information is being properly handled and kept accessible to approved parties only. As consumers we do demand and appreciate transparency about how a business is storing and using our data. But we are also feeling the need to maintain control over when, how and to what extent our personal information is shared with others. And organisations should ensure that our privacy requests are carried out in full faith.

Therefore, data privacy is the public expectation of privacy which is defined by the ability to decide whether or not we want to share some information, who to share it with, for how long and so on. The control over personal data incorporates the right to be left alone and also to modify the information when needed.

Today, privacy is what 'organic' or 'cruelty-free' was in the past decade - Gartner's Predictions for the Future of Privacy, 2020

## Data Protection Regulatory Framework Is What Enforces Data Privacy

The challenge of data protection is intensified by the fact that data is inherently borderless and accessible. Authorities are also recognising the need for regulations that will bring accountability measures for organisations processing personal data. For instance, the European Union has stepped up to the plate by enacting the General Data Protection Regulation (GDPR) which is considered the most comprehensive and ground-breaking data protection law. With strict access controls over the personal data of individuals, this regulation has made user consent a key aspect of data use and collection.

Authorities in other countries are also following suit

with their own data protection and privacy regulation – California has the California Consumer Privacy Act (CCPA) while South Africa has its own Protection of Personal Information Act (POPI Act). Brazil's General Law for the Protection of Personal Data and the UK's Data Protection Act are quite similar to GDPR. Japan, Australia and Singapore have also instituted stringent data privacy regulations.

India is taking much longer with the Personal Data Protection (PDP) Bill, 2019. In the works since 2017 under the aegis of the Ministry of Electronics



*Data Protection Regulatory Framework Is What Enforces Data Privacy*

and Information Technology, the Bill aims to control the collection, processing, storage, usage, transfer, protection and disclosure of personal data of Indian residents. It is primed to bring a comprehensive overhaul in data protection which is governed by the Information Technology Act, 2000 till now. Some of the key features of the bill include:

- Notice and prior consent for the use of individual data
- Limitations on the purposes for which data can be processed by companies
- Restrictions to ensure that only data necessary for providing a service to the individual in question is collected.
- Requirements for data localisation
- Appointment of data protection officers within organisations
- Creating of a Data Protection Authority of India for protecting the interests of data principals, preventing misuse of personal data and ensuring compliance with the new law.



*The need for data protection and privacy laws is increasing as the amount of data created, stored and used continues to grow at unprecedented rates.*

Recent amendments to the draft Bill have also incorporated the Right to Be Forgotten which allows private information about a person be removed from internet searches and other directories under certain circumstances.

The Bill is mired in heavy opposition from various corners about the overregulation and blanket powers to the government and is likely to be on hold till it manages to balance the competing interests of the different stakeholders.

However, the Indian legislature did manage to amend the IT Act to include Section 43A and Section 72A, which subject financial services, telecoms and other regulated sectors to obligations of keeping customer personal information confidential and using them for prescribed purposes, or only in the manner agreed with the customer. It also prescribes the right to compensation for improper disclosure of personal information.

Over the past year, the Indian government has banned many Chinese apps on more than one occasion. The ban is not over the political skirmish but is emanating from the illegal data collection practices of the said apps. It has been enforced under Section 69A of the IT Act for collecting extensive information of users – like data from users' clipboard, GPS locations, IP and MAC addresses, wi-fi access point names - without their explicit permission. Some were even setting up local proxy servers on users' devices to transcode media.

However, the recent Twitter account blockages has brought the same section under criticism for lack of proportionality and operational transparency!

Rather than leaving everything to the authorities, we as individuals can take some simple steps to protect our data from misuse.



*The PDP Bill will empower Indians to know how their data is being used, by whom and why*

- Always lock the mailbox to keep thieves from stealing the physical mail.
- Shred all documents that contain personal information, like receipts, bank and credit card statements, before disposing.
- Secure the wi-fi network and other devices with passwords to keep others from monitoring your online activity.
- Check the privacy settings on your social media accounts.
- Don't share your Aadhaar or PAN number just because someone asks for it. Find out if they really need it and how they plan to protect it.

## Conclusion

What netizens need is a robust, transparent and permission-based data privacy law. Meanwhile, the best data privacy strategy is to simply pay attention! ▶

# Top 5 Cyber Crimes in India



## 1. Hacking

Hacking is a systematic process used to identify vulnerabilities in a system and access nearly all the administrative controls in the system. This can lead to a hacker getting control of how the system functions, what information is encrypted, and even the outputs of specific processes.

## 2. XSS: Cross-Site Scripting

Such attacks try to use the URL of an existing and otherwise reliable website to perform a targeted attack. The attacker will try to insert JavaScript, HTML, or Flash-based code onto the third-party site.

## 3. Denial-of-Service Attack

Suppose you are a System Administrator for a large enterprise and looking after the IT Infrastructure at the premises. Your job is to ensure maximum uptime and hence contribute to the enterprise productivity levels. While you monitor the performance of systems on your platform, you suddenly see a spike in the cloud data consumption of a few systems from the Customer Support team. At first, you believe that they are simply

running too many processes, which will settle in a while. Then you see some systems from the HR Team consuming more cloud resources than usual. Before you can react, a whole set of systems from the operations teams uses your cloud resources in excess. Within minutes, these systems have eaten into the threshold of your cloud platform. And now – you will have to stop regular business processes for fixing the issue.

## 4. Phishing Scam

Generally, when people are asked the top 5 cybercrimes, their list invariably includes phishing scams. With this method of attacking enterprises and individuals, the attacker tries to masquerade as a known enterprise or an authoritative body.

## 5. Spamming

While spamming is not considered a criminal act in many jurisdictions, it can be discomforting for the recipient. If you are using a compromised corporate email ID, your inbox may get flooded with unsolicited messages that divert you from having a productive day and consume your firm's resources. ►

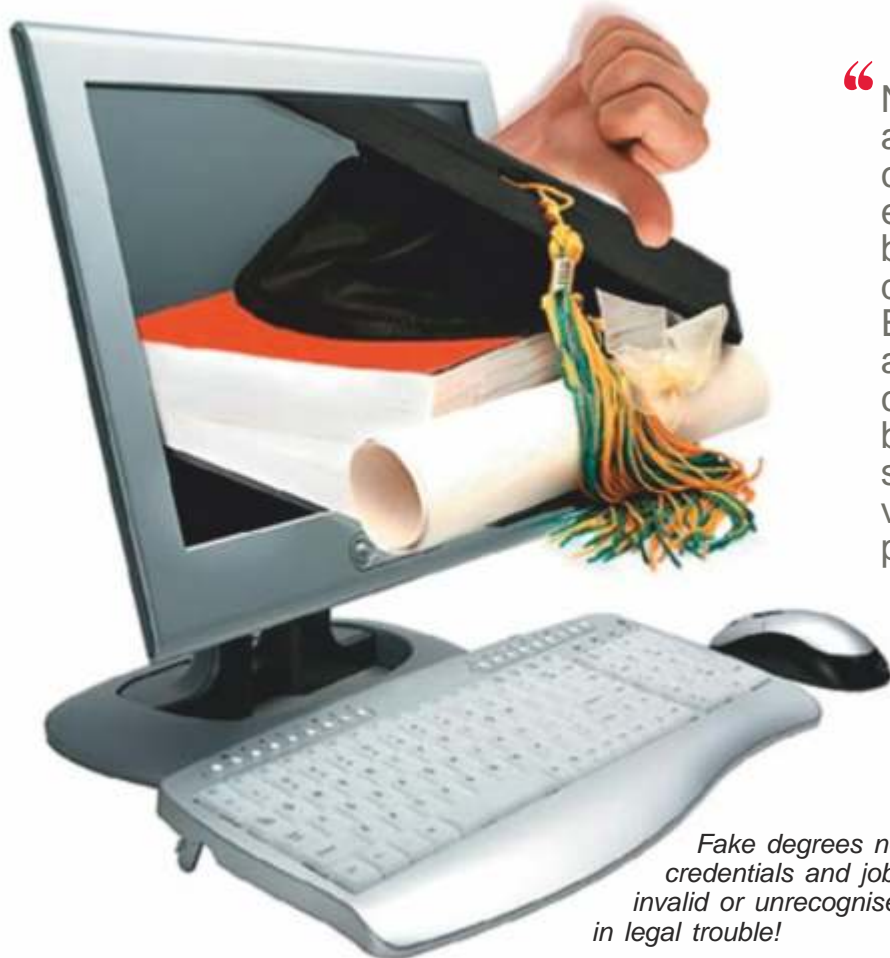


**Dr. Alka Mukne**

Ph.D. (Tech.)  
Board Member-PSAIF



## Could Your Online Degree Be Fake?



“Nothing is sacred anymore for cyber-criminals – not even education! E-learning has been tarnished with fake degree programmes. Even as the authorities are trying their best to clamp down on the bogus universities, students need to be vigilant to avoid falling prey to these scams.”

– Dr. Alka Mukne

*Fake degrees not only undermine your credentials and job prospects as they are invalid or unrecognised; they can also land you in legal trouble!*

**THERE IS LITERALLY** no limit when it comes to cybercrime. From unauthorised access to our digital devices to mobile banking frauds to tech support scams to sextortion – cyber offenders have infiltrated every aspect of cyberspace and rendered it unsafe for netizens. We are digitally vulnerable in every sphere and education is no stranger to cyber duping either!

We are seeing that students across the world are turning to distance education programmes and online university degrees to improve their qualifications, skills and job prospects. E-learning has increased over the last couple of years with online higher learning institutions sprouting up across the globe. The next best thing for an Indian student who cannot afford to go to USA to complete his Masters is to get the degree from an American university that offers online courses. The COVID-19 pandemic has boosted the demand for online education programmes and is indirectly driving the internet education scam industry as well.

### What is the E-Learning Con?

Online university degrees/certificates/diplomas have a lot going for them –



A recent research has estimated that the fake degree industry is worth over **Rs. 12,000 crores** worldwide. In case of India, the UGC maintains a list of fake universities, but it does not provide the list of online fakes.

not only is it cost-effective, but brings flexible schedules, better quality of learning, access to experienced tutors and more. However, like any good thing, this is also attracting bad elements who do more than just besmirch the experience.

Welcome to the world of diploma mills – the pseudonym for fake online

university websites that either openly sell degrees for cash or pose as legitimate ones to award 'degrees' to their 'students'. The latter try every trick – setting up elaborate websites, offering a roster of courses and even listing an impressive faculty - to create the illusion that everything is legitimate and certified. But fact of the matter is that it is all bogus – the university does not exist at all and the degrees it churns out are not even worth the paper they are printed on! This is more worrying as they not only dupe the unsuspecting students who shell out lakhs of rupees for a worthless degree, but the 'illegal' academic credentials can also spoil their career prospects – you will not get hired and can even be prosecuted by law.

### Pay Attention to the Red Flags

Fortunately, there are some tell-tale signs that can help you avoid the common online education scams:

#### ■ Lack of accreditation –

Accreditation denotes that the school or programme has been reviewed and validated by a recognised group and meets an acceptable standard of quality. While they can still make up an accreditor or lie about being

The next best thing for an Indian student who cannot afford to go to USA to complete his Masters is to get the degree from an American university that offers online courses.





accredited by a real one, a good place to start is to check with the accrediting agency or scan online databases of accredited programs. Keep in mind that many programs are not accredited and may have alternative credentials too.

■ **Using prestigious and familiar names** – Another common tactic is to modify the name of a bonafide and prestigious university – like Columbia State University in place of Columbia University or Cambridge International University to replicate the real University of Cambridge. As it sounds familiar, students either mistake it for the original one or assume that it is associated with the established university.

■ **Sketchy/missing faculty details:** Any university is just about as good as its faculty. Therefore, missing or even sketchy information about the faculty on the website will definitely raise questions about the genuineness of the institute. While some of them may resort to fake names or wrong attributions, students should go the extra mile by crosschecking the credentials of the

faculty from professional networking sites like LinkedIn.

■ **Admission criteria is too good to be true** – Genuine colleges and universities will require specific education background and other requirements. A quick and easy admission policy riding only on a resume or work experience is fishy for sure.

■ **Graduating at super speed** – Every qualification will involve coursework with classes, interaction with professors, assignments or assessments. While experience can help you earn some credits, it cannot become the basis for getting a diploma or degree. Similarly, the possibility of completing a course within a few months or just a year instead of three should ring some loud warning bells.

■ **Shady contact details** – Official website URLs will always end in .edu and not .com, .net or other domain extensions. Even the email address will not be generic like @gmail.com. While at it, also check the physical location, address and other contact information – watch out for a post

box number or address that is difficult to locate.

■ **No student services** – Which established university does not offer student services like counselling, technology support and library facilities? Proceed with caution if these are missing.

■ **Pressure to enrol** – While education has definitely become all about marketing and sales pitches, pay special attention if the recruiter avoids discussing the academics and outcomes of the program and only pushes for enrolment. Requirements to pay the full tuition fee upfront without any instalments or semester/year structure is another glaring warning that something is amiss.

## Conclusion

The University Grants Commission (UGC) declared 20 universities as bogus in 2020 itself. Investing some time and effort in researching the authenticity and reliability of an online education programme will pay off in terms of securing a genuine and valuable education. ■





## MR. MAHESH PATEL

was President and Group Chief Technology Officer (CTO) at AGS Transact Technologies Limited - one of the largest integrated omni-channel payment solutions providers in India – and is now Director at Hitachi Payment Services Pvt. Ltd.

# Rise of Digital Payments and Growing Threat of Cyber Frauds

Banks, e-wallets, UPI IDs are generally prone to cyberattacks to cash in on the treasure-trove of personal and financial data! Mr. Mahesh Patel opines about how the COVID-19 pandemic has become a watershed moment for digital transactions with the swift adoption further giving a fillip to cyberattacks while stressing on the need for safe digital practices.

**TODAY, THERE ARE** two aspects of safety that are of paramount importance. First relates to physical safety from the coronavirus and second is 'payment safety' from the increasing number of cyber frauds. To mitigate the risk of spread by shared surfaces like cash or cards, the Government and other regulatory bodies like NPCI are encouraging citizens to make digital payments. While this move has brought many customers under the ambit of digital India, it has also given a significant rise to cyber frauds. Cyber criminals are using fear, lack of knowledge and various deceptive means like lucrative emails to cheat vulnerable customers such as first time or not-so-tech-savvy users.

## The Growth Of Digital Payments

The pandemic has pushed most Indians to embrace digital payments as cash was perceived as a potential carrier of the virus. According to the latest National Payments Corporation of India (NPCI) data, UPI recorded 2.23 billion transactions amounting to INR 4,16,176.21 crore or INR 4.16 trillion in December 2020. Additionally, according to an estimation made by RBI in 2020, digital payments are expected to jump to 1.5 billion transactions, worth Rs. 15 trillion a day in five years.

Most citizens are now making their grocery, electricity bill and essential purchases using digital modes. We can see a paradigm shift in preferences and purchasing habits. According to a recent survey done by India Transact Services Ltd, a merchant payment solutions company, 57 per cent of respondents used digital payments 5 to 6 times a week in July 2020 while 21 per cent of them claimed to use it thrice. About 20 per cent of respondents used digital payments less than three times a week. These numbers define the quantum of usage and hence the possible impact that it will have in case of frauds.

### THERE ARE FOUR MEGATRENDS THAT ARE DRIVING THE DIGITAL PAYMENTS REVOLUTION



**1. Continued innovation and increasing performance in digital technology**



**2. Consumer demand and rising expectations of one-touch transactions**



**3. The policy push towards financial inclusion and the desire to marginalize cash transactions**



**4. An explosion of essential consumer services ranging from e-commerce to app-based taxi hailing that necessitates digital transactions, and the scale-up of these services to mass adoption.**

## The Growing Risk Of Frauds

Growing concern of customers and lack of digital literacy has put many digital users at risk.

As citizens across the world are trying to source information related to the pandemic, fraudsters are now tampering the official websites and also acting as imposters of official sources to deceive users. Hence, customers must be extra cautious while sharing details or downloading attachments from unfamiliar emails.

According to Mumbai Police's cyber cell, there has been a 70 per cent rise in e-wallet fraud and related digital payment crimes during January to May 2020 as compared to the same months in 2019. Since the imposition of the lockdown, the police have received 12 cybercrime complaints a day on an average. In this period, cybercrimes, including credit and debit card fraud, rose by 19 per cent in Mumbai and 51 per cent in Maharashtra. Recently, India's cybersecurity chief Rajesh Pant said that India was hit by around 375 cyber-attacks each day in 2020. Additionally, it is estimated that there has been a loss of loss of US\$ 6 trillion to organisations and individuals as a result of cybercrime in the first nine months of 2020.

Fortunately, banks and financial institutions can proactively manage the fraud related threats to the digital payment ecosystem through innovative and secure solutions.

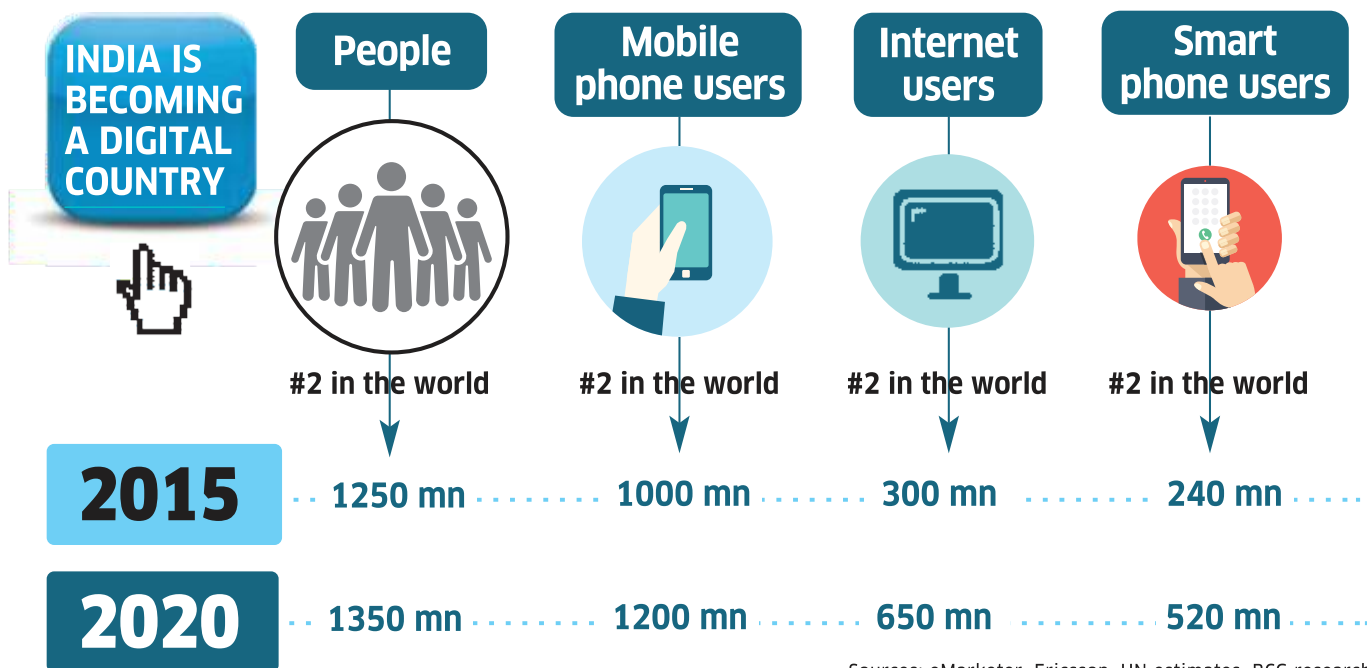
### Two-factor Authentication

**(2FA):** When a user logs into a portal with the help of a password, he/she receives a dynamic OTP via text message on a registered mobile number to authenticate the transaction. Since the hacker would require

both the cardholder's login password and phone to access the account, this measure can be fairly effective in circumventing fraud.

**Tokenisation:** It is a secure measure to prevent digital fraud as it primarily precludes the need for the user to share payment credentials for each online transaction. In





Sources: eMarketer, Ericsson, UN estimates, BCG research.

this method, a token is created for the card number which issuer can authenticate; therefore, there is no need to transmit the actual card number. Since the credit card number is tokenised with secure key each time the transaction is performed, the digital payment is secure and the potential for data breach and fraud decreases.

**3-Domain Secure (3DS) layers:** These are real-time authentication services in transaction communication that allow issuer banks and merchants to interchange the data provided by customers for authentication. In this case, transactions are initiated and authorised after checkout through a password or dynamic one-time password (OTP) received as a text message on the user's mobile and e-mail account.

**Address Verification Service (AVS):** Even though slightly archaic, this mechanism can be effective in limiting fraud. At the time of transacting, the AVS verifies the information provided by a cardholder with that available with the issuing bank, along with other factors (such as card number and expiry date). Once the information is verified, the issuing bank sends an AVS code to the merchant's payment gateway.

## An Eye On Security

As we migrate into the digital realm, digital payments are likely to become a bigger part of our future. The proliferation of digital payments will inevitably amplify the risk of cyber thefts and frauds. In such an environment

the early detection and prevention of fraud should become a hygiene factor for banks and financial institutions.

Regulatory bodies such as RBI and NPCI as well as banks, take timely initiatives to ensure customers are educated about security concerns and ways of tackling them. These bodies often share e-mails and SMSs with their customers to keep them abreast. However, many times customers turn a blind eye to these communications and become vulnerable to frauds. Therefore, endconsumers can follow simple steps like reading important communications from their banks/payment apps with regards to possible digital frauds and SMS related to transactions. In case of a suspicious activity, they should immediately inform the concerned banks.

Furthermore, each passing day fraudsters are preying on gullible customers and evolving their ways of deception. Such risks can be mitigated if banks integrate their systems with online real time fraud monitoring systems. In these challenging times, solutions like these can prevent security breaches and ensure financial safety.

In a nutshell, while the banks, regulatory bodies, cybersecurity agencies and payment providers ensure we get best and secure payment platforms, its success largely depends on how safe our digital practices are. Vigilance and digital literacy are our strongest defence to fight cyber frauds. ■

You can read the full article at

<https://www.expresscomputer.in/guest-blogs/rise-of-digital-payments-and-growing-threat-of-cyber-frauds/72217/>





**Aditi Malhotra**

Advisor, QCI

## PARENTS BEWARE!

# Is Your Child Being Bullied in Cyberspace?

The internet has been an enabler for all of us in the pandemic world of today, but the lack of digital literacy and online safety measures has exposed our children to increased incidents of cyberbullying.



*The internet opens the door to immense knowledge, learning and socializing;  
but this can be a double-edged sword for the students*

**BULLYING AMONG KIDS** and youth has been an issue for generations. For the last two decades, bullies have been using technology to expand their reach and the extent of their harm and increased digital activity since the start of the pandemic has only enhanced this problem. Cyberbullying is a broad term used to describe different kinds of online abuse including but not limited to harassment, doxing, trolling, swatting, shaming and reputation attacks.

Victims of cyberbullying, even adults, often don't know the identity of their abuser and even if the victim is able to suspect or identify the bully, in most cases they are unable to prove it because trolling and bullying accounts often take advantage of the right to anonymity.

The perpetrator uses technology such as computers, consoles, tablets and any device with access to the internet or social media to abuse, threaten, humiliate, stalk or otherwise harass another person by instigating and/or participating in online hate campaigns. Cyberbullying is not exclusive to social media and specially in the context of children, it is extremely problematic within the online gaming community.

Cyberbullying occurs across multiple venues and mediums in cyberspace and most often where kids and adolescents congregate online. It started with internet chatrooms in the early 2000s where most online harassment took place. As social media (Instagram, Snapchat, Twitter) expanded and now includes voice/text chat in popular games (Roblox, Fortnite) and video sharing, streaming and community sites (YouTube, Discord, Twitch), it has led to increased reports of cyberbullying occurring in those environments, although their frequency, type and context varies greatly. Now we are seeing this happen in Augmented Reality (AR) and Virtual Reality (VR) environments, in online classrooms, in social gaming sites and in various anonymous apps.

## Traditional Bullying v/s Online Bullying

While often similar in terms of form and technique to physical bullying, cyberbullying is different and has a more devastating impact on the victim. Firstly, the aggressors can cloak their identity using anonymous accounts and pseudonymous screen names. Secondly, it is easier for the cyberbully's actions to go viral-everyone's right to anonymity allows for mob mentality online where complete strangers join in the cyberbullying taking place by contributing and amplifying the bullying rather than helping the victim. Therefore, the pool of potential targets, aggressors, witnesses and bystanders is limitless.

Also cyberbullying can be done from a physically distant location where the aggressor is unable to see the response and impact on their target. Because they are in a sense sheltered from the target's response, kids and teens might not even realise the serious harm their actions are causing the victim.

Given the ever-evolving online world and its enhanced reach in the post-pandemic world, many parents and caregivers do not have the technological know-how to keep track of what kids and teens are up to online. As a result, an aggressor's actions may be left unchecked and a target's experience may be missed. Even when the

bully is identified, the adults often find themselves unprepared to adequately respond to the situation. Therefore, many feel that there are little to no consequences for their actions, causing cyberbullying to become a major issue for children.

Given the ubiquitous and essential nature of online communication tools for all children in today's world, preventing cyberbullying should be a priority for parents, caregivers and educators. Adults can no longer afford to be dismissive of cyberbullying and should accept that this is a problem that will only get worse if it is ignored.

## Parents' Role

Unfortunately, many kids don't tell their parents that they are being cyberbullied. It may be because they may not know exactly what counts as bullying online, especially children with learning and thinking differences and those with poor social skills. Even when kids do realise what is happening, they may stay silent while they try to figure out the situation. They may be worried, that if they complain, like in traditional bullying, it will get worse. Or the bullied child may feel that some attention from their peers, even if it is negative, is better than none.

In the post-pandemic world, where kids have lived almost their entire life online for the last two years, they may be afraid of losing their online privileges. They might be nervous that their parents will address the problem by taking away their computer and devices.

Parents need to be aware of possible signs that their kids are being bullied online. Most child experts agree that there are some common signs that parents and caregivers can look out for to identify if your child is being cyberbullied - like your child becoming suddenly withdrawn.

One of the major signals of cyberbullying is when your child suddenly stops using their computer, gaming device, tablet, etc. even though they have enjoyed it before. Another usual marker is if your child does not want to use their electronic device in a place where you can see it or they may turn off the computer monitor or change screens every time you or anyone else walks by.

Other tell-tale signs include your child seeming nervous or jumpy every time they get an instant message, text or email or if your child alludes to bullying indirectly by saying things like 'There is a lot of drama at school' or 'I have no friends' and may not want to attend classes online or appears uneasy to go to school physically when that is an option.

If it doesn't stop, cyberbullying can put your child at risk for anxiety, depression and other behavioural and health issues. They may also have difficulty concentrating in school. Therefore, parents must prepare their child for going online and talk to them about online and digital behaviour.

## Causes of Cyberbullying

There are multiple reasons that someone might choose to cyberbully another person.

They might have been cyberbullied themselves and may feel that it is fine to treat others the same way or find that it is the only way to express their own pain.

Sometimes, a group of friends may be targeting and bullying another child and they feel that by participating they will 'fit in' or develop a new group of friends themselves.

Like traditional bullying, the perpetrator may be experiencing a difficult home life and misplace their anger and frustrations onto the victim. Sometimes insecurity, especially in adolescents, as they compare themselves to their peers, usually with regard to their appearance, can result in envy and jealousy based cyberbullying and abuse. The aggressor may choose to cyberbully in order to feel powerful and in control of a situation. Online gaming chatrooms have boomed and some children take advantage of this technology to abuse and bully.

### What can parents do?

There are several steps that parents can take if they think that their child is a target of cyberbullying. They can start a conversation with their child by either describing a bullying incident from their own childhood or an example of cyberbullying that may have been in the news. If the child still isn't forthcoming, the parent must calmly tell them that they will be the administrator of their computer, phone and online device. The parent and caregivers need to see where they have been online and the browsing history that they may have deleted.

If the parents confirm that their child is being bullied online and can identify the bully, there are things they can do to put a stop to it. Begin by suggesting to the child that they let the bully know that the parents have access to the child's devices. They must also encourage the child to reach out to friends for support. Research indicates that peers sticking up for each other is an effective defence against bullies, even online. Bullies work by isolating their victims. When kids rally around the kid being targeted, these upstanders thwart the bully.

If the bullying still does not stop, and is intense and frequent, the parent may need to take one or all of the following steps. They will need to talk to the parents of the bullying child and let them know what is going on and how it is affecting their child. The parents may also reach out to their child's teacher, school counsellor or principal. Some schools have begun to set up anti-cyberbullying policies and protocols to help. In most cases if bullying is happening online, it might be happening offline too. If none of these strategies work, especially if there is a physical threat involved, the parents may consider getting law enforcement involved. They may printout, take screenshots and save digital evidence of the bullying in case that is needed.

In cases where the parents are unable to identify the bully and the child is bullied on a website or in an app, the parents can visit the company's site and look for the section offering support, such as 'community guidelines', 'safety center', 'parent info', 'safety tips' or something similar. It may make recommendations such as blocking the bully or changing the setting for who can contact you.

If your child is bullied on text messages, parents can call their mobile network provider to report the number.



*Bullying of children no longer ends when the school bell rings. It can easily spill over into the online world.*

They may be able to block it or change their number. Some carriers may offer additional anti-bullying features for a fee.

### The Other Side

If a parent discovers that their child is cyberbullying others, they should first communicate to their child, how that behaviour inflicts harm and causes pain in the real world.

We must remember that kids are not sociopaths, they sometimes lack empathy and make mistakes. Parents must give them an opportunity to address their behaviour. That said, consequences should be firmly applied depending on the seriousness and intentionality, and escalated if the behaviour continues.

Moving forward, you as a parent, need to pay an even greater attention to your child's technology use to make sure that they have internalised the lesson and are continually acting in responsible ways. Parallely, work to cultivate empathy by intentionally putting them in situations that make them uncomfortable and can soften their hearts. Such activities may include age-appropriate community service projects and the like that help them to take alternative perspectives and begin to understand that everyone is fighting a hard battle.

### Conclusion

We need to get all stakeholders involved – children, youth, parents, caregivers, educators, counsellors, youth leaders, social media companies, law enforcement agencies and the community at large to create an environment where all children feel comfortable talking with adults about the problem of cyberbullying and feel confident that meaningful steps will be taken to resolve their situation.

It will take a concerted and comprehensive effort from all involved to make a meaningful difference in reducing cyberbullying. ▀





## Stop Operating on Autopilot!

We are spending more time online and exchanging more data than ever before. However, this has also made us more digitally vulnerable than ever before. Indeed, the more connected we get, the more important it is to safeguard ourselves from the threats that are abounding in cyberspace. Consumers across India share their opinions/experiences of cybercrime.

**THE VIRTUAL WORLD** is dominating our lives and our digital footprint is growing every minute. The most dangerous thing here is that a cyber threat cannot be detected until after it has happened! Think about it – we can still catch a person stalking us on the road or become suspicious when someone is lurking near an ATM. But can we actually perceive a cyber stalker or a phishing scam for that matter?

The virtual threat is metaphorically staring us in the face and we have no choice but to become extremely cautious about what we are doing online.

– **Stephen Baker, Karnataka**



The ways and means of using the internet is bound to grow beyond our wildest imagination. But it is not only technology, even the cyber risks are continuously evolving. The heavier dependence on technology fuelled by the onset of the pandemic has become a

**Technology and its benefits are ever-growing; so are the avenues to misuse it**

goldmine for bad actors. Cyber security is now an essential service, just like police stations, fire engines and ambulances.

– **Hiral Baldev, Mumbai**

Cyber scammers are coming at us from every which where – phone call, SMS, email, social media, apps and more. Last year, my father fell prey to a fraudulent email that was supposedly from his bank asking him to update his details and ended up sharing sensitive credentials including his Aadhaar card number. The perpetrator used the information to apply for loans in micro-banks before wiping out his bank account completely! We reported it to the Cyber Crime desk but alas, the damage was done and the money cannot be traced till date!

– **Rasanpreet Sodhi, Agartala**

The line between our online and offline lives is almost indistinguishable. This can be due to convenience or out of compulsion. But the fact remains that it is making us susceptible to not only losing money to frauds and embezzlement but also damage and destruction of data, theft of intellectual property, lost productivity and even loss of reputation. There are so many gullible folks like you and me around the world....

– **Krishnan Kumar, Kolkata**

The internet is the lifeline of the entire universe. But how safe are we in this alternate realm? Always keep in mind that technology is a double-edged sword and can cost you more than you can think. It is our duty to not only be mindful in cyberspace but also keep it free of trouble!

– **Ziven Shah, Surat**

Everyone around me, myself included, is using apps like Google Pay, Paytm, BHIM, Phonepe for making payments. The government is pushing for digitization and almost everyone is banking online and has a UPI ID now. But why are we not talking about cyber security? Who is responsible for keeping customer financial data safe? Why aren't businesses prioritising digital security and allocating higher budgets for investment in anti-fraud technologies? Does anybody even think about risk assessment? We have to join hands to keep ourselves secure and fight against cybercrime.

– **Girish Kanodia, Hyderabad**

UPDATE ...



Moving a Step Ahead

*Update on the October edition on World Food Day 2021 -  
Dealing with the Grave Threat of Food Insecurity*

# Combatting the Assaults on Food Security

Food Safety & Standards Authority of India (FSSAI) on Twitter:

## On this World Food Day

Let's join hands to make our Future more Nutritious and Healthy. Our actions are our future – Better production, better nutrition, a better environment and a better life.

#EatSafeEatHealthyEatSustainable

**THE INTERNATIONAL CELEBRATIONS** for World Food Day kicked off with the very first Food Systems Summit organised by the United Nations in September to discuss ways to transform the production and consumption of food. The emphasis was on building awareness and participation of every actor in the food systems.

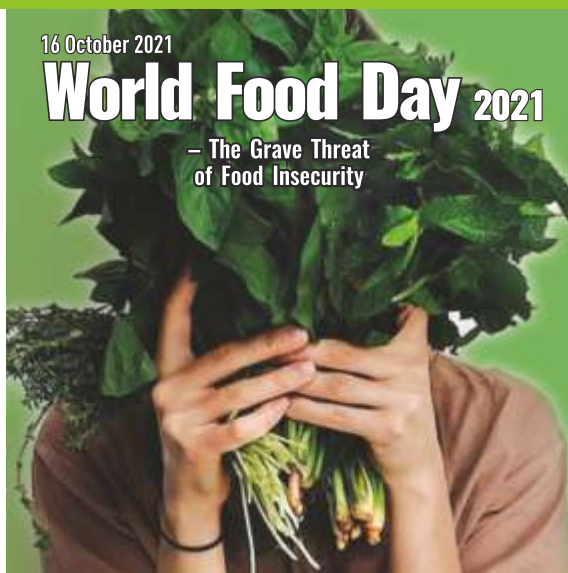
Prior to this, the Indian government organised Food Systems Summits at the national and sub-national levels to generate wider participation, ideas and suggestions from key players across the country. We presented our achievements on Action Track 4: Advance Equitable Livelihoods at the international summit and will continue to learn from the experiences and successes to bring about positive and tangible changes in the food systems.

World Food Day was celebrated across the globe on 16th October with the theme 'Our Actions are our Future'. This was a rallying call to inspire everyone to contribute to the transformation of the agri-food systems. Yet, FAO

16 October 2021

## World Food Day 2021

– The Grave Threat  
of Food Insecurity



Director General, Qu Dongyu noted that world hunger levels are continuing to rise.

It is particularly disheartening that India ranked 101 out of 116 countries in the Global Hunger Index 2021 (released in October) that tracks hunger and malnutrition across the world. India holds the dubious distinction of being the country with the highest child wasting rate worldwide and is one among the 31 nations where hunger has been classified as 'serious'. We stand behind Pakistan, Bangladesh and Nepal with our ranking being on the downward trend since 2016,

falling from 94 out of 107 countries in 2020.

The government is vehemently questioning the report and the FAO estimate on India's undernourished population stating that it is 'devoid of ground reality and facts and suffers from serious methodological issues'.

Still the fact remains that the situation is grim indeed. We need to fight hunger and not the Global Hunger report! ▶

## SOURCES / REFERENCES

<https://en.wikipedia.org/>  
<https://www.meity.gov.in/>  
<https://www.mha.gov.in/>  
<https://pib.gov.in/>  
<https://www.ncbi.nlm.nih.gov/>  
<https://www.interpol.int/>  
<https://www.who.int/>  
<https://unctad.org/>  
<https://www.unodc.org/>  
<https://www.hrw.org/>  
<https://unbumf.com/>

<https://www.moneycontrol.com/>  
<https://www.reuters.com/>  
<https://www.mondaq.com/>  
<https://www.appknox.com/>  
<https://www.latestlaws.com/>  
<https://www.legalserviceindia.com/>  
<https://www.thehindu.com/>  
<https://thehindubusinessline.com>  
<https://economictimes.indiatimes.com/>  
<https://www.hindustantimes.com/>

<https://www.indiatvnews.com/>  
<https://www.firstpost.com/>  
<https://citizenmatters.in/>  
<https://www.barandbench.com/>  
<https://infosecawareness.in/>  
<https://staysafeonline.org/>  
<https://www.medrxiv.org/>  
<https://online.maryville.edu/>  
<https://cloudian.com/>  
<https://www.expresscomputer.in> ▶

## YOUR OPINION MATTERS

## Letters to the



## editor

(October issue -  
World Food Day 2021 - The Grave  
Threat of Food Insecurity)

We are truly humbled by the praise and acknowledgment that is flowing in from varied sources. Please feel free to send in your comments, views or feedback on The Aware Consumer magazine at [bejonmisra@theawareconsumer.in](mailto:bejonmisra@theawareconsumer.in) – we will publish your opinions and implement your feedback while ensuring that your voice is heard on the right platforms.



Bejon Da,

We congratulate you and your team for bringing such educative articles in this issue on the eve of World Food Day. Its contents are highly informative and useful for all of us when we are still facing challenges of malnutrition in some parts of our society.

– **Shovan Ganguli, Bengaluru**



Dear Editor,

Thank you so much for the October edition of The Aware Consumer dedicated to Food on the occasion of World Food Day where it has covered very interesting and valuable articles related to the global food scenario.

The articles namely Committing To End World Hunger; Hunger Amidst Abundant Production; India Can Take A Front Seat In Driving Global Food Security and Tackling Food Insecurity For Hunger From India are worthy for applaud in highlighting the challenges & solutions. Do keep covering such informative & research based stories in the upcoming TAC issues.

– **H Wadhwa, Delhi**



This issue is very visual and that helps readers like me to browse through the pages quickly and pick what interests us most. They also encouraged me to read the article in detail. Reliable stats/data references shared allowed me to size the problem/impact and gave a clear perspective. Now I have a clear vision on how the production and consumption of food can be transformed. It also gives a good visibility of the initiatives and programs undertaken in different parts of the world and promotes a global perspective of the efforts. Including messages from key personalities promoted the cause and severity of the crisis, which is well presented.

Also, the emphasis on the importance of healthy eating and tips that everyone should follow, is a crucial awareness during these challenging pandemic phases. The suggestions for improvement around the e-PDS are apt. The consequences of poor micronutrients are well depicted.

On a whole, I would say this magazine is a "Power House" of information and awareness that's much needed to be spread across the world, for the cause of transforming the way we eat, what we eat, food wastage and food poverty/exposure of the under privileged community. Hope many more people come forward and contribute towards actioning the vision and recommendations shared here.

– **Aarti Yadav, London**



When I need to understand something in all its depth, complete with facts and figures, I would most definitely pick 'The Aware Consumer' magazine. This month the factual writeups on the extent of food insecurity in the world with the pictorial representation of data answered most of the questions that

I have. What is most appealing, is the way it was designed with crisp information that inspires me to take those well informed decisions towards lifestyle changes.

Especially, the magazine gives us a great insight into how by simply watching what we eat, can indirectly transform the world... How cool is that! The very basics, of how and when, answered with respect to nutrition and global impact is simply outstanding. Even the simple facts of meals at school and the impact of that on the growth of our future generation.

I would like to direct attention to the fact that the consumer affairs department is still tied up with the food and public distribution department. A dedicated consumer affairs ministry will help the authorities to better safeguard consumer rights and interests!

– **Dilys Dias, Goa**

**THE NATIONAL CONSUMER DAY** - observed on 24th December every year - was primarily invoked to highlight the importance of the consumer movement in the country. It pays tribute to the historic date - December 24th, 1986 when the President of India gave his assent to the Consumer Protection Act. This is a subtle reminder to the government that protecting the interests of the consumers should always be one of their core activities. It is really sad to note that the authorities fail to plan out such momentous events in advance – even the theme is announced at the last minute. This year we again vow to keep persevering to protect consumer interests and also make them aware of their rights!



**WATCH  
OUT!**

for the next issue in January dedicated to  
Medical Diagnostic Testing



## **NABH AYUSH ENTRY LEVEL CERTIFICATION PROGRAM**

### **TAKING QUALITY TO OUR ROOTS**



#### **NABH**

is a constituent board of Quality Council of India (QCI).

It is playing a pivotal role at the National level in propagation, adoption and adherence to healthcare quality standards in AYUSH healthcare delivery systems.

With an objective to bring more light to AYUSH related treatments, the Government of India in 2014, formed the Ministry of AYUSH and consequently brought in the National Accreditation Board for Hospitals & Healthcare Providers (NABH) to start implementing quality healthcare standards for hospitals providing AYUSH treatments as well.

In the recent years, there has been a paradigm shift from allopathy system to traditional healthcare. To support this trend, health insurers have started offering AYUSH treatment covers as part of their health insurance policies. NABH Ayush Entry Level Certification Standards provide an objective system of empanelment by insurance and other third parties. These standards also address the need for quality control and quality monitoring in AYUSH healthcare as required by the Pradhan Mantri Jan Arogya Yojana (PM-JAY) under the Ayushman Bharat Scheme.

**NABH AYUSH Entry Level Certification standards are easily downloadable from NABH website.**



**[www.nabh.co](http://www.nabh.co)**



**[nabh@nabh.co](mailto:nabh@nabh.co)**

# THE AWARE CONSUMER

India's Most Credible  
**Consumer Monthly**

Save upto

**50%**

on subscription



## Subscribe **today!**

{ Save **₹3,600/-**  
FOR 36 ISSUES }

Please accept my subscription of **THE AWARE CONSUMER**

NAME \_\_\_\_\_

ADDRESS \_\_\_\_\_

PH. NO. \_\_\_\_\_ E-MAIL \_\_\_\_\_

PAYMENT ☐ CASH ☐ CHEQUE CHEQUE/DD NO. \_\_\_\_\_

DRAWN ON \_\_\_\_\_

DATE \_\_\_\_\_ SIGNATURE \_\_\_\_\_

No. of Issues	News Stand Price	Discount	You Pay	You Save
12	₹ 2,400/-	20%	₹ 1,920/-	₹ 480/-
24	₹ 4,800/-	30%	₹ 3,360/-	₹ 1,440/-
36	₹ 7,200/-	50%	₹ 3,600/-	₹ 3,600/-

Cheque / DDs should be drawn in favour of **HAMARA CONSUMER DOST PVT. LTD.**

Send your subscription to: The AWARE CONSUMER, F-9, 2nd Floor, Kailash Colony, New Delhi-110048

Contact: 9311044424 • E-mail: bejonmisra@theawareconsumer.in

Posted at Lodi Road HPO, New Delhi on 9-10<sup>th</sup> of every month  
Published on 6<sup>th</sup> of every month

RNI No. DELENG/2015/67140  
REG. NO. DL (S)-17/3523/2017-19