# WHAT ABOUT FINANCIAL SAFETY?

## Poor More Often Victims of Fraud

**Jayalakshmi Chittoor and Janice Verghese***



*School students and locals at a Digital Literacy and Online Safety campaign workshop, conducted by the Cyber Peace Foundation in Tura, Meghalaya.*

Ever wondered how many electronic devices have invaded most middle class homes and impacted our lives? Have you wondered if the same access to electronic devices exists among the poor? One common answer is that most people will now have access to at least a mobile phone, television and FM Radio. The phones have almost become ubiquitous with a potential to reach nearly 100 per cent of the population. Just around 2015, only 18.5% of the population owned smart phones, but the meteoric rise of these phones was evident as prices dropped, and a major disruptive mobile service provider was able to penetrate the bottom of the pyramid population with an impossible to put down commercial offer. This led to the penetration zooming up to 25% by 2017. The rural internet growth that breached the half a billion mark at 566 million would reach 627 million by the year end (2019), according to a research study published in March 2019 by market research and consumer consulting organisation Kantar IMRB. In the same study it was observed that 97% of the users accessed Internet using the mobiles as their access device.

Government of India's Digital India Programme has been a major initiative since 2014. Pegged as a mission mode programme, it takes off from the core infrastructure impetus given by previous government initiatives under the umbrella of National e-Governance Programme. One of the key initiatives here is the Common Service Centres (CSC) programme, which under its first tranche established 1,10,000 public access centres across the rural and urban fringes.

These were designed as a public private partnership model to enable each citizen of India to access government services. While several e-governance initiatives moved ahead at a rapid pace, the services were often accessed or availed. Cost of computers and Internet was a major stumbling block for citizens to avail these services. However, several services matured well to create a user interest. Topping this list were Passport Services, Income Tax online, Service Tax online, Railway reservation and allied services of IRCTC as well as banking and other financial products like insurances. The list of excellent government online services, including the establishment of payment gateways through banking links, enabled services like bill payments very easy.

When the common man's need to interact with government agents or officials reduced, and ipso facto led to more transparent and efficient services, the value created by this massive

* *Jayalakshmi Chittoor is an independent KM4Dev and ICT4D specialist associated with Cyber Peace Foundation, an NGO; Janice Verghese leads the Training Division at Cyber Peace Foundation. She is a techno legal expert on cyber safety with extensive pan India community outreach experience.*

government initiative was much appreciated.

Even when the ambitious Digital India programme was launched it sought to further reduce the bureaucratic bottle necks and create an atmosphere of accessible government.

Towards this end, the CSC programme was expanded to cover 650000 panchayats across the country, again through the village level entrepreneur. He/she was provided and facilitated with newer business opportunities, while fulfilling the mandate of reaching all citizens. With banking getting online and government policy focusing on direct benefit transfers, especially of subsidies and scholarships, it was no longer an option for people not to use online services, but the need of the hour.

Aadhaar enrolment became the foundation stone for transitioning to a digital economy. The access question has been debated globally, and especially by organisations like Centre for Internet and Society as well as IT for Change which work on the intersection of development and digital technologies. Digital citizenship, democratic rights and social justice questions have been consistently raised not only from the Indian perspective but from a global third world perspective. Internet content, access to Internet content in local languages (including Indic language computing challenges) and gender bias on the Internet

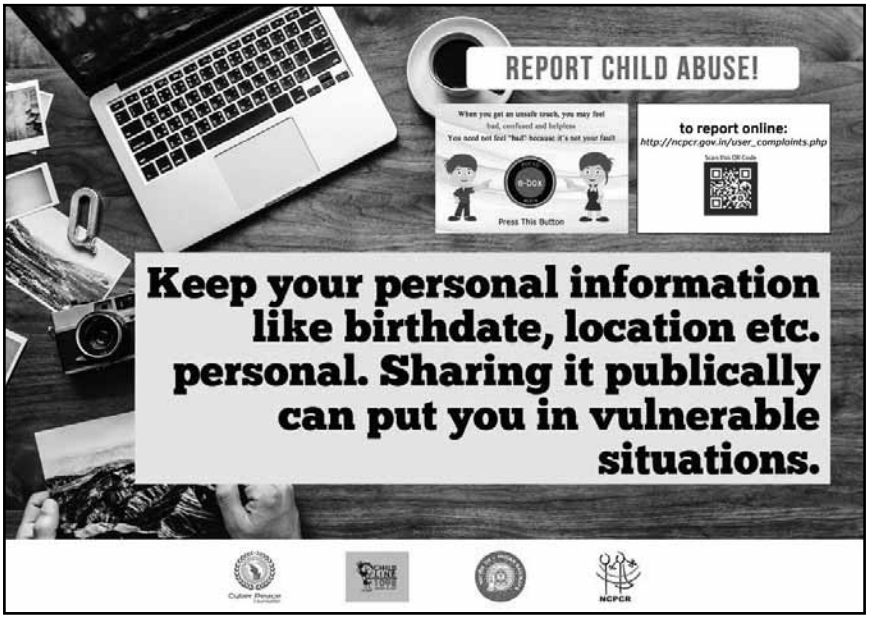



*The Cyber Peace Foundation and National Commission for Protection of Child Rights created posters to spread awareness about the rise in cybercrime against children.*

are key areas in which Anita Gurumurthy, Executive Director of IT for Change has been working for the last 20 years. Policy narratives often, she argues in a recent article in the *Economic & Political Weekly*, keep women out, because they tend to ignore issues like fear of technologies that constrain women's freedom to use digital spaces. She also spoke on the violence on women in cyberspace, backed by a research undertaken by IT for Change in three states of south India, featuring a survey of over a 1000 young persons (born in an Internet age, between 19 to 23) as well as several focus group discussions covering both male and female respondents.[1]

The world of opportunities for knowledge sharing and livelihood enhancement, along with a flood of other educational or economic opportunities that are now accessible to many, have still evaded a large chunk of the Indian population. Constraints of age, education levels, economic prosperity, discriminatory social practices, abilities, and rural/urban divides are challenges that continue to confront citizens keen to address the issue of social justice to all.

While the millennial males and females celebrate the world of social networks and other online spaces, their experiences differ. There is a noticeable increase in violence against women, and reinforcement of patriarchal and oppressive behaviour among males in these spaces. Abuse, trolling, sextortion, revenge porn, cyberbullying, cyberstalking, identity theft/impersonation, hacking/cracking of accounts etc. are terms that have become commonplace.




*Posters were used to familiarise school children with provisions of POCSO and on ways to register complaints.*

The underlying challenges stem from three key constraints: 1. Lack of knowledge about safety: Not all who can afford a phone, for example, know how to keep themselves and their data safe. 2. Technology intrusion in daily lives: Hacking is a reality, and is only the tip of the iceberg. 3. Insufficient number of cyber professionals to assist even large scale institutions, let alone common citizens: Many face the challenge of finding experts who can rescue them at the time of a crisis. It is even harsher for the poor and marginalised facing financial frauds.

Financial fraudsters operate without any geographical borders. The infamous Jamtara in Jharkhand has moved from being a locality of extremely poor people trying to eke out a living to a community of expert financial fraudsters turned millionaires adept at foxing the hell out of law enforcement agencies. Even when they get caught, they are quick to bounce back to repeat their offences, finding newer ways to target gullible citizens. There are shocking cases reported in the media about how these fraudsters wiped out the savings of digital neo-literate users and siphoned out their money by cloning electronic wallets or cards, ATMs, or even devices remotely. This digital divide, one could argue, is the single biggest challenge faced by the digital economy.

This is accentuated by the fact that mobiles are easy to clone and misuse, and cyber criminals are on the prowl to attack the most vulnerable. Mobile devices, once attacked, like terrible virus strikes, cannot be fixed easily. Nor do the citizens care to secure themselves and their devices. The problem is worsened by a severe lack of cybercrime experts and investigating agencies, with the first respondents not yet trained to collect evidence acceptable under the courts of law.

Even the existing laws have only provisions to penalise scammers. There is still a huge need to invest in research and innovation, especially in the domain of expertise in nabbing prowlers in the dark web. It would not be wrong to say that even the most educated and aware segment of the population would not know what to do in the face of a crisis, barring a few who would resort to blocking their cards or deleting their accounts. They are not aware that for over a year (since august 2018), a dedicated portal has been set up to report cybercrimes, ranging from cases of photos/videos being shared non consensually, to rape videos, and even lesser crimes.

One can simply click on http://cybercrime.gov.in, verify his/her credentials and report the incident. In the backend, the government has created a link through the CCTNS, which will forward the complaint to the cyber thana of the state, building another level of accountability and access to law enforcement agencies. This addresses the issue of not knowing who to approach when a cybercrime is committed. It also helps identify and locate the fraudsters who

may seem untraceable owing to the anonymity that the internet allegedly guarantees. This misconception has been busted through active investigation and redressal of a large number of cases that have been reported on the portal. Undeniably, more awareness is needed among citizens about these welcome developments, and volunteers from every spectrum of society and across different professions can help reach more people.

The digital divide has aggressively denied the participation of many in the modern economy that has seen dramatic disruptions by way of technology. Let us take the example of businesses that have cropped up in the last decade or so. Take Ola and Uber as the disruptor of taxi services. While they have given many a new job/ enterprise opportunity, within a span of 10 years, these start ups have changed their agreements with the driver partners, often locking them up in a series of loan instalments that they need to pay off. Sometimes their situation is aggravated by losses, owing to money being stolen from mobile wallets, even as their lack of awareness on digital security keeps becoming pronounced.

To tackle the need for digital literacy and awareness, the Ministry of Electronics and Information Technology ran a large scale Information Security Education and Awareness Programme (ISEA), reaching over a lakh people, through workshops, short courses etc. It has reached out to government officers, the CSC personnel, citizens, educational institutions, and developed numerous safety awareness materials. Another nationwide campaign is the PMGDisha, wherein at least one person per household is to be trained on digital services, including basics of using computers, other electronic devices and transacting with/ using government services. The programme has been targeting common citizens and is being delivered through the CSCs, covering all the 6.5 lakh panchayats.




*This poster tells children about inappropriate behaviour by known/unknown adults.*

Other civil society initiatives, like the Digital Shakti programme, by the award winning NGO Cyber Peace Foundation (CPF), have reached out to over 60,000 women and girls. A public private partnership, with support by a technology provider major, government and civil society organisations, this initiative's focus was to enable women access online spaces safely and adopt practices that prevent them from being harmed online. It also aimed to help women make the most of what the internet has to offer and create their digital identities. Another initiative has been to train law enforcement officers in eight states on investigating cybercrimes against children, with the support of UNICEF.

Since the difference between online and offline behaviour is blurring, it increases the vulnerability of the affected persons. It could create economic, mental or psychological losses with indescribable and unfathomable consequences. The cyber criminals have neither spared the children nor the innocent elderly. The world of online scams was alive and thriving way back in the 90s, when scam mails from Nigeria or other countries asked recipients to share lottery/ inheritance or other gains, and subsequently demanded the bank details of innocent victims.

| | |
|---|---|
| Damage to computer/computer system, This includes hacking, introducing malware, denying or causing denial of any service. | Section 43, IT Act |
| Receiving stolen computer resource | Section 66B, IT Act |
| Identity theft | Section 66C, IT Act |
| Cheating by impersonation | Section 66D, IT Act |
| Violation of privacy | Section 66E, IT Act |
| Cyber terrorism | Section 66F, IT Act |
| Child sexual abuse material | Section 67B, IT Act |

The next type of frauds are identity thefts, phishing and vishing attacks, as well as ransomware attacks, especially on large scale computers, leaving a trail of huge financial losses. These were limited not only to ransomware, but also other kinds of malware including spyware, key loggers, adware, bots, bugs, Trojan horses, worms and viruses. The presence of agencies like Indian Computer Emergency Response Team (CERT-IN) is a help, but not enough. In a study by NASSCOM, it was estimated that there is a deficiency of nearly half a million cybersecurity experts in the country. Also, our educational institutions offering engineering degrees with specialisation in cyber security, laws and forensics are not creating enough professionals qualified to comprehend, let alone deal, with this complex environment of fraudsters. So, individuals can hardly expect recourse through systemic experts/agencies for their woes.

It will be unfair to not give due credit to the existing legislations that have helped prosecute criminals. The IT Act, enacted in 2000, and amended twice in later years, has covered most of the common crimes. However, the legislations make cybercrime offences bailable and provide for punishment lasting less than three years. Therefore, there is a need for more stringent laws to ensure deterrence and also to set a precedent that cybercrimes are to be taken as seriously as traditional crimes and will hence be dealt with accordingly.

The Indian Penal Code, enacted in 1860, has been used for a much longer time and in most cases. The precedence of the IT Act over other laws was established in *Sharat Babu Digumarti v. Govt. of NCT* in 2016. In this case, an ecommerce platform was prosecuted for selling and distributing obscene material. Initially, the director of the company was booked u/s 292 of the IPC for obscenity.

When the case was presented before the Supreme Court, it was said that there is difference in laws pertaining to similar crimes. Section 292 of the IPC pertains to the transmission of obscene material through conventional print media, including books, pamphlets, paintings and drawing. On the other hand, Section 67 of the IT Act, also criminalises the publication and transmission of obscene material in the electronic form. It is important to note that there may be several laws dealing with the same crime, but only when the law is correctly interpreted that we understand the nuances. The Supreme Court established the difference, and henceforth, the IT Act has been read in all cases of cybercrime primarily, along with other Sections.

There are many more Sections in the IT Act, criminalising various activities, including identity theft, cheating by impersonating, hacking, theft of data, etc.

These laws can be used in most of the cases, and certain activities, although not defined or criminalised explicitly, may be taken within the ambit of others for redressal. However, there are grey areas lacking specific laws, where most criminals operate.

A very good example would be Section 66E, which deals with violation of privacy. On examining the law, one understands that under Indian laws, violation of privacy occurs only when the private parts of an individual are captured. But violation of privacy is much more than just this. Trying to access an individual's device or simply capturing their images is also a violation of their privacy.

Laws are either way too specific or very vague, which we see in Section 67. This provision of this IT Act deals with obscenity. The context of obscenity is set by using the words "lascivious" and "appeals to the prurient interest." The definition of lascivious can be found in a dictionary. But in real life, what is obscene for one may not be obscene for another. Herein lies the problem of interpretation of statutes and clarity is gained only through case laws and precedents.

It is the same problem on social media platforms. Most platforms have no tolerance for inappropriate behaviour, but again, the community guidelines and user policies that cover all these aspects, right from creation of accounts, to what is construed as acceptable behaviour, are not uniform.

Instagram, for example, allows users to share images of breastfeeding, since it is a natural process. Facebook, on the other hand, does not allow such pictures to be posted as they are considered obscene. Here we see two widely-used platforms having different takes on obscenity. These platforms tend to follow community norms for their fraternity. However, the norms undergo reviews with user feedback.

This further creates problems for users, when they report content based on their perception of obscenity or inappropriate behaviour. However, the content is not removed. Nor are accounts blocked as they do not fit the definition of inappropriate as set by the platform.

Therefore, when on one end, we need more laws, on the other, we also need a deeper understanding of existing laws and reporting mechanisms. This ensures that cases are dealt with proactively and swiftly both by users and law enforcement agencies.

The government has been actively spreading awareness through messages to the masses. These include tips to keep in mind when banking and staying wary of fraud messages, mails and call. It is also trying to disseminate information through posters and ads, posted both physically in public places and on various online platforms. Campaigns have been initiated by stakeholders in both the private and public sector, but owing to the huge population of our country, it may not reach the masses as much as we would like. Therefore, the responsibility lies not only on the shoulders of the stakeholders at the top level, but also on the end users, to use the digital platform with caution.

It is heartening to note that the cybercrime issues are being tackled with better infrastructure, forensic labs and stronger laws. More needs to be done. In India there are only seven central cyber forensic labs. This is not enough for the rising number of cybercrime cases. There is a need for more volunteers and experts to join hands to keep the country safe from cybercriminals.




*Reporting child abuse: These posters are aimed at encouraging children to open up and talk to their parents and teachers about both online and offline abuse.*

*(PHOTOGRAPHS COURTESY: Cyber Peace Foundation)*

## (Endnotes)


1. Gurumurthy, Anita (2019, March 8), How the online space for women is in a crisis and what needs to be done about it. *TECH2*, Retrieved on November 20, 2019 from https://bit.ly/2E2zKPV